Concept 3

1

Inhoudsopgave

5

Voorwoord

Voor u ligt het rapport 'Het lek onder de loep' dat gaat over de voortijdige verspreiding van het Eurochamprapport in de periode dat er een geheimhouding gold. Dat was nodig vanwege de privacygevoelige gegevens die er in stonden in combinatie met een aangifte door de provincie bij Justitie vanwege vermeende frauduleuze handelingen.

Toen medio november 2008 duidelijk werd dat het Eurochamprapport in handen was geraakt van de pers, heeft het college van gedeputeerde staten naar de toedracht een onderzoek laten uitvoeren door het adviesbureau KPMG. De uitkomsten van dat rapport waren voor Provinciale Staten onbevredigend en op 18 maart 2009 hebben zij besloten een eigen onderzoek te verrichten.
Vertrekpunt van het statenonderzoek was het KPMG-rapport. De onderzoeksperiode liep van het verschijnen van het definitieve Eurochamprapport (10 november 2008) tot aan de openbaarmaking ervan (27 november 2008). Het onderzoekskader had betrekking op een drietal onderzoeksvragen. Die komen kort gezegd neer op: wie heeft er gelekt en hoe is dat gebeurd, welke bestuurlijk/culturele factoren hebben hieraan bijgedragen en wat kan er worden geleerd van de onderzoeksbevindingen.

De navolgende Statenleden werden op 8 april 2009 benoemd in de onderzoekscommissie:

1. Leo Bomhof (VVD; voorzitter)
2. Renée Westerhof (SP; vice-voorzitter); vanaf 28 april wegens ziekte vervangen door Ko Vester (SP)
3. Herman Beerda (PvdA; na 28 april 2009 vice-voorzitter)
4. Sietze de Jong (CDA)
5. Margriet Stijkel-Kuijpers (ChristenUnie)
6. Gea Smith-Bults (Groen Links)

Het onderzoek is binnen drie maanden afgerond, waarbij het onderzoeksrapport binnen tien dagen na de laatste hoorzitting (18 juni 2009) gereed kwam. Dat heeft een forse inspanning gevraagd van de commissieleden, de statengriffier (mevrouw I. Rozema), het adviesbureau BING (de heren C. Kooman en P. Werkman) en van onze notuliste mevrouw G. Bol. Echter, daardoor kon wel aan de wens van provinciale staten worden voldaan om het politieke debat nog voor het zomerreces te voeren.

De onderzoekscommissie heeft niet kunnen achterhalen wie het Eurochamprapport heeft laten uitlekken naar de media. Wel is zij erin geslaagd om de gebeurtenissen in de onderzoeksperiode nauwkeuriger aan te geven en de betrokkenheid van de verschillende actoren beter in beeld te brengen. Daarbij zijn van verschillende personen opmerkelijke gedragingen geconstateerd, die mede door de aanwezige politiek-bestuurlijke cultuur in de provinciale organisatie konden ontstaan. In het rapport wordt hier uitgebreider op ingegaan.

Rest mij de leden van de onderzoekscommissie, de secretaris, de notuliste en de adviseurs te bedanken voor hun enthousiasme, kennis en grote inzet tijdens de afgelopen maanden. Zonder deze kwaliteiten was het de commissie niet gelukt om het onderzoek in zo'n korte tijd gereed te hebben.

Leo Bomhof
Voorzitter van de Onderzoekscommissie Eurochamprapport
Assen, 29 juni 2009

1 Inleiding

1.1 Leeswijzer

Het rapport van de onderzoekscommissie is opgebouwd uit zes hoofdstukken. In hoofdstuk 1 wordt de doelstelling van het onderzoek beschreven. Hoofdstuk 2 bevat het toetsingskader. Dit kader vormt de beleidsmatige en juridisch context waarin het handelen van bestuurders en ambtenaren in deze casus dient te worden bezien. In hoofdstuk 3 wordt antwoord gegeven op de eerste onderzoeksvraag, in hoofdstuk 4 op de tweede onderzoeksvraag en in hoofdstuk 5 op de derde onderzoeksvraag. Het rapport wordt afgesloten met conclusies en aanbevelingen (hoofdstuk 6).

1.2 Onderzoeksvragen

De drie centrale vragen van het onderzoek zijn[1]:

1. wie is verantwoordelijk voor de voortijdige verspreiding van het rapport van Deloitte en op welke wijze is dat geschied?
2. waren er bij de provincie Drenthe organisatorische en/of 'bestuurlijk-culturele' factoren die de voortijdige verspreiding hebben bevorderd?
3. in hoeverre moet het gevoerde bestuur worden aangepast om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen?

De commissie heeft deze onderzoeksvragen in haar plan van aanpak geoperationaliseerd, waarbij een aantal subvragen/deelaspecten zijn geformuleerd die bij het beantwoorden van de centrale vragen aan de orde konden komen. De commissie heeft ervoor gekozen om deze subvragen niet in dit rapport op te nemen. Wel hebben deze subvragen een rol gespeeld bij het opstellen van de interviewvragen die aan betrokkenen zijn gesteld in de interviews en de hoorzittingen.

1.3 Onderzoeksfasen

De commissie heeft naar aanleiding van de onderzoeksopdracht (bijlage 2) een plan van aanpak voor haar eigen onderzoek geschreven. Dit plan is als bijlage bij het rapport gevoegd (bijlage 3). Tevens heeft de commissie haar werkwijze vastgelegd in een huishoudelijk reglement (zie bijlage 4).
In het plan van aanpak van de commissie wordt een drietal onderzoeksfasen onderscheiden. In de eerste fase, de fase van deskresearch, heeft de commissie relevante informatie verzameld en geanalyseerd. Deze informatieverzameling en analyse is uiteindelijk de gehele onderzoeksperiode voortgezet. Dit had te maken met de vertraagde aanlevering door Gedeputeerde Staten van diverse documenten/gegevens, onder meer vanwege een voorafgaande toets aan privacy- en andere regelgeving en tekortschietende interne

[1] Deze onderzoeksvragen zijn mede tot stand gekomen naar aanleiding van een advies van professor dr. D.J. Elzenga d.d. 5 april 2009

communicatie en vanwege de tijd die nodig was voor het beschikbaar maken (restoren) van digitale gegevens. Enig gebrek aan gevoel voor urgentie speelde hier naar de mening van de commissie ook een rol.
Onderdeel van deze eerste onderzoeksfase was ook een digitaal onderzoek, dat de commissie heeft laten uitvoeren in het kader van de bewijsvergaring om (met name) de eerste onderzoeksvraag te kunnen beantwoorden.
In de tweede fase van het onderzoek heeft de commissie interviews (informatieve voorgesprekken) gehouden met betrokken ambtenaren, bestuurders en overige personen. Naast interviews heeft de commissie ook een aantal mensen gehoord in een openbare of besloten hoorzitting (zie bijlage 6). Deze hoorzittingen hebben plaatsgevonden op 16 en 18 juni 2009. Twee journalisten van het Dagblad van het Noorden die waren uitgenodigd voor zowel de interviews als voor de hoorzittingen, zijn niet ingegaan op deze uitnodigingen en hebben zich hiervoor afgemeld.
De derde fase van het onderzoek betrof de fase van het rapporteren van de bevindingen en conclusies volgend uit het onderzoek van de commissie. Deze fase heeft geresulteerd in onderhavig rapport.

1.4 Juridisch kader onderzoek

Het wettelijk kader van het onderzoeksrecht van Provinciale Staten is geregeld in de artikelen 151a tot en met 151f van de Provinciewet.
Conform artikel 151a lid 8 dienen PS, alvorens tot een onderzoek te besluiten, bij verordening nadere regels te stellen met betrekking tot deze onderzoeken. In elk geval moeten daarin regels worden opgenomen over de wijze waarop ambtelijke bijstand wordt verleend aan de commissie.
De provincie Drenthe beschikt sinds 2003 over een dergelijke verordening. Deze 'Verordening Onderzoekscommissie' (met kenmerk BJCA/A1/200300611 2) is door PS vastgesteld op 25 juni 2003 en door GS bekend gemaakt op 30 juni 2003. De verordening is als bijlage bij het rapport gevoegd (bijlage 5).

2 Toetsingskader

2.1 Inleiding

In dit hoofdstuk wordt kort het toetsingskader geschetst dat relevant is voor de beantwoording van de onderzoeksvragen. Dit kader vormt de beleidsmatige en juridisch context waarin het handelen van bestuurders en ambtenaren in deze casus dient te worden bezien.
Het toetsingskader bestaat uit een juridisch kader; de relevante wet- en regelgeving, en een beleidskader, waartoe diverse documenten behoren die door de provincie ten aanzien van het onderwerp informatie en informatiebeveiliging zijn opgesteld.

2.2 Juridisch kader

2.2.1 Enkele relevante wetsartikelen

De commissie vermeldt hier de wettelijke artikelen die - gelet op de casus - het meest relevant zijn.
Op basis van artikel 125a lid 3 van de Ambtenarenwet is een ambtenaar verplicht tot geheimhouding van hetgeen hem in verband met zijn functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt. Een breder kader wordt geschetst door artikel 125ter: 'Het bevoegd gezag en de ambtenaar zijn verplicht zich als een goed werkgever en een goed ambtenaar te gedragen.'

Op basis van artikel 55 van de Provinciewet kunnen Gedeputeerde Staten geheimhouding opleggen omtrent de inhoud van stukken die aan hen worden overgelegd.
Op grond van artikel 25 van de Provinciewet kunnen Provinciale Staten geheimhouding opleggen omtrent het in vergadering behandelde en omtrent de inhoud van de stukken die aan PS worden overlegd.
Een schending van de geheimhouding kan een strafbaar feit opleveren. In artikel 272 van het Wetboek van Strafrecht is de schending van de geheimhouding geregeld. De tekst van het artikel luidt als volgt:

Artikel 272

1. *Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.*
2. *Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.*

2.2.2 Bestuurlijke gedragscode

De provincie Drenthe beschikt over zowel een ambtelijke gedragscode (Gedragscode ambtelijke integriteit) als een code voor de bestuurders; de Drentse gedragscode integriteit Commissaris van de Koningin, Gedeputeerde Staten en Provinciale staten.

Laatstgenoemde code voor bestuurders is vastgesteld door PS op 3 september 2003.
In de gedragscode wordt een aantal kernbegrippen van integriteit genoemd. Dit zijn: dienstbaarheid, functionaliteit, onafhankelijkheid, openheid, betrouwbaarheid en zorgvuldigheid.
Deze kernbegrippen worden in de integriteitcode gezien als toetssteen voor de in de code opgenomen gedragsafspraken. De leden van het college van GS en PS worden geacht de regels na te leven. Wanneer

zij zich er niet aan houden, kan dat - blijkens de tekst van de code - gevolgen hebben voor hun functioneren en voor hun positie.

Voor deze casus is met name artikel 4 van de code van belang. In dit artikel, getiteld 'Informatie', staat het volgende:

Artikel 4.1 Een bestuurder gaat zorgvuldig en correct om met informatie waarover hij uit hoofde van zijn ambt beschikt. Hij verstrekt geen geheime informatie.

Artikel 4.2 Een bestuurder verstrekt informatie, tenzij deze geheim of vertrouwelijk is en het geven van informatie niet mogelijk is op grond van de Wet openbaarheid van bestuur.

Artikel 4.3 Een bestuurder maakt niet ten eigen bate of ten bate van zijn persoonlijke betrekkingen gebruik van in de uitoefening van het ambt verkregen informatie.

In de inleiding van de bestuurlijke gedragscode staat dat er voor ambtenaren tevens een beroepscode is opgesteld, waar integriteit een belangrijk deel van uitmaakt. De voorliggende code en de beroepscode voor ambtenaren zijn op elkaar afgestemd. Er staan geen tegenstrijdige bepalingen in, zo staat er geschreven.

2.2.3 Ambtelijke gedragscode

De Gedragscode ambtelijke integriteit is vastgesteld bij besluit van GS van 18 maart 2003. In de code worden de volgende zes kernbegrippen van ambtelijke integriteit onderscheiden: dienstbaarheid, professionaliteit, onafhankelijkheid, verantwoordelijkheid, betrouwbaarheid en zorgvuldigheid.
In de code zelf komt het onderwerp omgaan met informatie niet terug. Wel bestaat er bij de provincie een niet-gedateerd document getiteld 'Omgaan met provinciale informatie'. Hierin wordt gesteld dat zorgvuldig moet worden omgegaan met informatie. Voor vertrouwelijke stukken geldt dit – volgens de tekst van het document – nog eens extra. Tevens staat in het document letterlijk: 'Lekt informatie bijvoorbeeld via de pers uit, dan kun je hier als medewerker persoonlijk op worden aangesproken.'

2.2.4 Reglement gebruik bedrijfsmiddelen (2006)

In het Reglement gebruik bedrijfsmiddelen staat de procedure omschreven omtrent beschikbaarheid, gebruik, controle en bewaring van bedrijfsmiddelen. De artikel 2 t/m 6 van dit reglement worden als relevant beschouwd voor het onderzoek en zullen hieronder worden toegelicht.

In artikel 2 van het reglement staat dat gedragingen worden toegerekend aan diegene die op de computer is ingelogd. De tekst van het artikel luidt als volgt:

Artikel 2.

1. *De directie kan de beschikbaarheid van bedrijfsmiddelen beëindigen of beperken wanneer een medewerker de bedrijfsmiddelen gebruikt op een wijze die in strijd is met dit reglement.*
2. *Een medewerker die de beschikking heeft over e-mailfaciliteiten is verplicht zijn postbus regelmatig te controleren of te doen controleren. De directie kan hiervoor nog nadere aanwijzingen geven.*
3. *Gedragingen worden toegerekend aan degene die op de computer is ingelogd.*
4. *Het installeren van software en applicaties is niet toegestaan, tenzij vooraf toestemming is verleend door de directie. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en eventuele licenties worden betaald.*

In artikel 4 van het reglement staat dat het een medewerker niet is toegestaan om door het gebruik van bedrijfsmiddelen, schade te berokkenen aan de provincie Drenthe als instantie, haar werknemers en/of aan derden. De tekst van het artikel luidt als volgt:

Artikel 4.

1. *De gebruiker mag alleen gebruikmaken van de bedrijfsmiddelen die beschikbaar worden gesteld door de provincie Drenthe. Uitzonderingen op deze bepaling zijn slechts mogelijk met schriftelijke toestemming van de directie. Aan deze toestemming kunnen voorwaarden worden verbonden.*
2. *Het is de gebruiker niet toegestaan om door middel van het gebruik van bedrijfsmiddelen zich zodanig te gedragen dat:*
    a. *de goede naam van de provincie kan worden geschaad;*
    b. *het ongestoord functioneren van de technische infrastructuur van de provincie in gevaar wordt gebracht;*
    c. *de vertrouwelijkheid van gegevens kan worden geschaad;*
    d. *het strijdig is met geaccepteerde omgangsvormen of goede zeden, belastend is voor de goede werksfeer dan wel beledigend is voor medewerkers en/of derden;*
    e. *het onrechtmatig is of een strafbaar feit oplevert;*
    f. *het strijdig is met de CAP;*
    g. *de provincie op enigerlei andere wijze dan op vorenstaande genoemde wijzen kan worden geschaad, hetzij in financiële zin, hetzij anderszins.*
3. *Het gebruik van middelen gericht op het verhinderen van kennisname binnen de provinciale organisatie van de inhoud van berichten en bijlagen door anderen dan de opsteller is niet geoorloofd. Van deze bepaling kan door de directie ontheffing worden verleend. Aan de ontheffing kunnen voorwaarden worden verbonden.*
4. *Gebruik van bedrijfsmiddelen voor privé-doeleinden wordt toegestaan mits met mate, uitgedrukt in zowel tijd en kosten, en niet in strijd met dit reglement. Voor het privé-gebruik van bedrijfsmiddelen kan de directie een financiële vergoeding vragen.*

In artikel 5 van het reglement staat omschreven hoe de observatie en controle van gebruiksmiddelen plaatsvindt en welk doel het dient. Er staat onder meer in dat de directie te allen tijde opdracht kan geven tot observatie. In artikel 6 wordt nader ingegaan op de regels omtrent het bewaren van gegevens. In dit artikel staat onder andere vermeld dat e-mails bewaard worden overeenkomstig de termijnen van de Archiefwet.

2.3 Beleidskader

Tot het beleidskader behoort een aantal documenten. De meest relevante documenten worden hieronder besproken.

2.3.1 Uitvoeringsprogramma Drenthe (2006-2007)

In dit uitvoeringsprogramma (getiteld: Welkom in digitaal Drenthe) staat omschreven welke stappen de provincie onderneemt om de inzet van IT te verbeteren. Hoofdstuk 2 van dit document is het Informatiestatuut. In dit statuut wordt specifiek ingegaan op het onderwerp informatiebeveiliging. Hierin wordt gesteld dat de provincie werkt op basis van de Code voor Informatiebeveiliging en dat in de planperiode wordt gestreefd naar een volledige invulling daarvan. Daarnaast staat beschreven dat medewerkers als gebruikers van de IT-hulpmiddelen geen misbruik mogen maken van de aan hen

toevertrouwde middelen en gegevens. Zij mogen deze middelen slechts gebruiken voor hun werkzaamheden voor de provincie.

2.3.2 Beleidskader informatiebeveiliging provincie Drenthe (februari 2009)

In het Beleidskader informatiebeveiliging provincie Drenthe (getiteld: *Veilig, integer en vertrouwd: hoe is onze informatie beveiligd?*) wordt beschreven hoe ambtenaren (en bestuurders) van de provincie Drenthe dienen om te gaan met informatiebeveiliging.
In het beleidskader worden de volgende definities gehanteerd:

*'**Informatie** is een bedrijfsmiddel dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor de organisatie en voortdurend op een passende manier beveiligd dient te zijn.*
Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden of in gesproken vorm). Welke vorm de informatie ook heeft of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn.

***Informatiebeveiliging** bestaat uit het treffen van maatregelen die beogen te voorkomen dat onbevoegden vertrouwelijke gegevens kunnen bezitten, raadplegen of beschadigen.*
Informatiebeveiliging wordt gekarakteriseerd als het waarborgen van:
Veilige beschikbaarheid: geautoriseerde gebruikers hebben op de juiste momenten tijdig toegang tot informatie en aanverwante bedrijfsmiddelen;
Integriteit: correctheid en volledigheid van informatie en de verwerking daarvan;
Vertrouwelijkheid: informatie is alleen toegankelijk voor degenen, die hiertoe geautoriseerd zijn en daarmee op de juiste wijze omgaan'.

Als uitgangspunt voor het informatiebeveiligingsbeleid wordt door de Provincie Drenthe de Code voor Informatiebeveiliging (NEN/ISO 270001 en 270002) gehanteerd. In deze code worden de volgende tien categorieën noodzakelijke beveiligingsmaatregelen onderscheiden:

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie en beheer van bedrijfsmiddelen
4. Beveiligingseisen ten aanzien van personeel.
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatie- en bedieningsprocessen
7. Toegangsbeveiliging
8. Aanschaf, ontwikkeling en onderhoud van systemen
9. Continuïteitsmanagement
10. Naleving

In het handboek Informatiebeveiliging worden bovenstaande onderwerpen en de regelingen omtrent naleving meer in detail behandeld.

2.3.3 Handboek Informatiebeveiliging (2005)

Dit document geldt als uitwerking van het Informatiestatuut. De tien beveiligingsmaatregelen, zoals in de vorige paragraaf beschreven, worden hierin uitgebreid behandeld. Met name wordt ingegaan op de richtlijnen, procedures en werkwijzen van de beveiligingsmaatregelen. Deze maatregelen gelden als

basisnorm waaraan de provincie Drenthe zich minimaal wil houden om veilig, integer en vertrouwd met informatie om te gaan. Hieronder worden kort een aantal aspecten uit dit handboek belicht.
In hoofdstuk 5 van het Handboek wordt gesproken over classificatie en beheer van bedrijfsmiddelen. Hier wordt beschreven op welke wijze informatie geclassificeerd kan worden en welke typen er bestaan. Op deze manier wordt het duidelijk welke toegangsrechten er verbonden zijn aan een bepaalde classificatie,zoals vertrouwelijkheid. De volgende typen classificaties worden onderscheiden:

- ***Openbaar***
  Informatie die voor derden toegankelijk is (lezen). Wijzigen van deze informatie kan uitsluitend door medewerkers van de Provincie (eigenaar) plaats vinden.

- ***Niet Openbaar,*** *onderverdeeld in:*
  - *Intern gebruik:*
    Alle interne informatie die uitsluitend voor medewerkers van de provincie Drenthe toegankelijk is. Op basis van functie worden toegangsrechten tot deze informatie toegekend.
  - *Vertrouwelijk:*
    Informatie die uitsluitend voor een beperkte groep medewerkers van de provincie toegankelijk is. Bij de informatie dient aangegeven te worden wie toegang heeft tot de informatie.
  - *Persoonlijk:*
    Informatie uitsluitend bestemd voor de geadresseerde.

Tevens staat in dit hoofdstuk beschreven hoe informatie gelabeld dient te worden:
- *Voor alle informatiesystemen wordt de geldende classificatie van informatie vastgesteld.*
- *Informatie zonder label wordt als "Intern gebruik" behandeld.*
- *Documenten met vertrouwelijke en persoonlijke informatie dienen op de voorpagina en in de koptekst voorzien te zijn van het label.'*

In hoofdstuk 8 van het Handboek wordt het beleid rondom het gebruik van e-mail beschreven. Hier wordt onder meer gesteld dat het niet toegestaan is om vertrouwelijke informatie te verzenden via de e-mail. Daarnaast wordt gesteld dat de provincie de e-mail alleen voor informele communicatie mag gebruiken.
In hoofdstuk 12 van het Handboek wordt onder meer ingegaan op welke wijze bedrijfsdocumenten dienen te worden beschermd tegen verlies, diefstal, vernietiging en vervalsing. Naast de classificatie en labelling van informatie zoals beschreven in hoofdstuk 5, worden er extra maatregelen ondernomen om informatie optimaal te beveiligen. Zo staat er onder meer geschreven:

- *'Vertrouwelijke informatie dient in afgesloten kasten te worden bewaard na werktijd en bij het verlaten van de werkruimte*
- *Belangrijke systeeminformatie (systeemtoegang) dient centraal in een afgesloten ruimte bewaard te worden'.*

3 De eerste onderzoeksvraag: Verantwoordelijkheid voor voortijdige verspreiding

3.1 Inleiding

De eerste onderzoeksvraag van de commissie luidt:

Wie is verantwoordelijk voor de voortijdige verspreiding van het rapport van Deloitte inzake Eurochamp en op welke wijze is dat geschied?

In dit hoofdstuk zal eerst worden stilgestaan bij het onderzoeksrapport van KPMG. Dit rapport heeft voor de commissie gediend als vertrekpunt/basisdocument voor haar eigen onderzoek. Tevens zal in dit hoofdstuk een reconstructie van de feiten worden gepresenteerd. Dit onder meer op basis van het eigen onderzoek van de commissie.

3.2 Onderzoek KPMG

De onderzoeksvraag voor het onderzoek van KPMG luidde als volgt:

'Is het definitieve rapport van Deloitte Forensic Services inzake Stichting Eurochamp Foundation voortijdig verspreid vanuit het Provinciehuis? Zo ja, op welke wijze, wanneer en door wie?'

KPMG heeft haar bevindingen gerapporteerd in een rapport d.d. 10 maart 2009 met als titel '*Onderzoek naar mogelijke voortijdige verspreiding rapport Eurochamp*'. Dit KPMG-rapport is als bijlage 7 bij onderhavig rapport gevoegd.
De conclusie van KPMG is dat het definitieve rapport van Deloitte buiten het Provinciehuis terecht is gekomen, voordat het openbaar is gemaakt op 27 november 2009. KPMG heeft niet kunnen vaststellen op welke wijze dit is gebeurd, waar en door wie.

KMPG heeft in haar rapport de belangrijkste feiten samengevat en op een rijtje gezet. Deze luiden als volgt[2]:

- 'De versie van het rapport die is verspreid voordat het rapport openbaar is gemaakt op 27 november 2008 betreft het definitieve *'Rapport inzake onderzoek naar de Stichting Eurochamp Foundation'*. Het rapport heeft het referentienummer 3112182270/2111.
- De versie die de heer Klaver in zijn bezit heeft vanaf 21 november 2008, betreft de digitale (pdf-) versie van voornoemde rapportage.
- De digitale (pdf-) versie van de rapportage is in de periode tussen 10 en 16 november niet verder per e-mail verspreid.

---

[2] KPMG rapport d.d. 10 maart 2009, 'Onderzoek naar mogelijke voortijdige verspreiding rapport Eurochamp', bladzijde 16.

- De informant heeft verklaard dat hij de wetenschap heeft dat een exemplaar van het rapport in ieder geval op de ochtend van 13 november in het bezit is van Dagblad van het Noorden.
- Het Dagblad van het Noorden heeft aangegeven inzage te hebben gehad in de rapportage. Dit is in een redactioneel commentaar in Dagblad van het Noorden bevestigd. Niet is aangegeven welke versie van het rapport door Dagblad van het Noorden is ingezien.'

De commissie onderschrijft op basis van haar eigen onderzoek bovenstaande bevindingen, met uitzondering van de derde bullit, omdat niet kan worden uitgesloten dat dit wel is gebeurd (zie bevindingen digitaal onderzoek, paragraaf 3.5, hierna). Wel tekent de commissie nog het volgende aan.
Uit het onderzoek van de commissie is gebleken dat KPMG een aantal feiten en omstandigheden niet in haar rapport heeft meegenomen. Dit is gedeeltelijk te verklaren uit het feit dat KPMG gesproken heeft met een informant. Daardoor heeft KPGM bepaalde informatie niet willen en/of kunnen meenemen in haar rapport, om zo te voorkomen dat de identiteit van de informant onthuld zou worden. De commissie heeft niet gesproken met deze informant. De informant heeft in eerste instantie het verzoek afgewezen om met de commissie te praten. Na afloop van de hoorzittingen wilde de informant alsnog een verklaring afleggen, maar alleen op zijn voorwaarden. Dat verzoek is door de commissie afgewezen. Dit was mede ingegeven door het feit, dat de daaruit verkregen informatie niet zou kunnen worden gebruikt in het onderzoek.
De commissie is tevens van mening dat het onderzoek van KPMG een te beperkte reikwijdte heeft gekregen. Zo heeft KPMG slechts één computer onderzocht, heeft er geen analyse van telefoonverkeer plaatsgevonden en is er geen zogeheten 'restore' van de mailomgeving gemaakt (zie verder paragraaf 3.5).

In de volgende paragraaf zal eerst een reconstructie worden weergegeven van de belangrijkste feiten, zoals die uit het onderzoek van de commissie[3] naar voren zijn gekomen. Deze bevindingen van de commissie worden in de reconstructie gecombineerd met de bevindingen van KPMG. Als vertrekpunt voor deze reconstructie is gekozen voor maandag 10 november 2008, de dag dat het (later uitgelekte) definitieve rapport van Deloitte binnen is gekomen bij de provincie Drenthe. De reconstructie loopt gedetailleerd tot 14 november 2008, de dag nadat het rapport volgens verklaringen van de informant in het bezit zou zijn van het Dagblad van het Noorden. De relevante gebeurtenissen van na 14 november 2008 worden tevens beschreven, zij het wat minder uitgebreid. Maar de commissie vindt deze feiten en/of omstandigheden relevant genoeg om deze in het rapport op te nemen.

3.3 Reconstructie

3.3.1 Maandag 10 november 2008

Op maandagochtend 10 november 2008 wordt de secretaresse van de directie van de provincie door een medewerkster van Deloitte gebeld met de mededeling dat het definitieve Eurochamprapport aan het einde van de dag, rond 18.30 uur, per koerier zal worden bezorgd. De secretaresse, die weet dat de directie dringend zit te wachten op de ontvangst van het rapport, vraagt daarom uit eigen initiatief of het rapport dan mogelijk ook digitaal verstuurd kan worden, zodat de directie het rapport eerder tot haar beschikking heeft.

[3] interviews, digitaal en ander technisch onderzoek en analyse documenten.

De secretaresse van de directie verklaart de gang van zaken als volgt:

'Deloitte belde om te zeggen dat de koerier niet op de afgesproken tijd zou komen, maar dat de rapporten pas 's avonds tussen half zeven en zeven uur zouden worden afgeleverd. Toen heb ik in dat telefoongesprek gevraagd of het rapport dan per e-mail naar het provinciehuis verstuurd zou kunnen worden, opdat men met dit rapport aan het werk kon.'

De directie van de provincie wil dat het rapport die dag binnenkomt in verband met de besluitvorming die de volgende dag in Gedeputeerde Staten zal plaatsvinden. Daarvoor is een op 10 november 2008 (of eerder) gedateerd rapport nodig.
De beleidsmedewerker Sport zegt daarover (zie ook paragraaf 3.3.3):

'Het heeft een beetje te maken met de termijnen waarmee wij te maken hadden. Wij hadden het bestuur van EuroChamp in augustus meegedeeld dat wij voornemens waren de subsidie te wijzigen en daarna volgde een periode waarin zowel de andere partij als de provincie zich konden beraden. Om en nabij de week van 10 november liep die termijn af. We hadden het dus redelijk druk. We moesten het rapport hebben.'

Het verzoek van de secretaresse van de directie wordt binnen Deloitte besproken, waarna later toestemming wordt gegeven om het document per email te versturen. Het rapport wordt vervolgens om 14.14 uur digitaal per email verzonden aan de secretaresse van de directie van de provincie. Het rapport bestaat uit drie PDF-bestanden, die als bijlagen bij een (begeleidende) email worden gevoegd. De secretaresse bewaart de email met bijlagen in haar mailaccount. De secretaresse meldt vervolgens aan de directeur / plaatsvervangend secretaris (hierna te noemen DpS) dat het rapport digitaal is binnengekomen. Die vertelt haar dat inmiddels al is besloten dat GS haar besluiten over het Eurochamprapport zal baseren op het concept Eurochamprapport, waardoor de digitale versie van het rapport niet meer van belang is.

De secretaresse van de directie verklaart hierover het volgende tijdens de hoorzittingen:

'Mevrouw Stijkel: Wij hebben begrepen uit het vorige gesprek dat wij met u hebben gehad, dat u, normaal gesproken, alle binnenkomende e-mails en documenten voor de directie uitprint. Is dat ook met dit rapport gebeurd?

De secretaresse: Nee, voor zover ik mij dat kan herinneren, is dat niet gebeurd. Voor zover ik mij kan herinneren heb ik niets met die mail gedaan.

Mevrouw Stijkel: Waarom is dan in dit geval van die regel afgeweken?

De secretaresse: Ik heb 's middag even na twee uur een telefoontje gekregen van de secretaresse van Deloitte dat het rapport verstuurd kon worden. Dat heb ik eigenlijk meteen aan de DpS gemeld en zij zei toen, dat het niet meer nodig was, omdat inmiddels vanwege de tijdsdruk was besloten op basis van het conceptrapport de oplegnotitie voor GS te maken.
Op het moment dat ik het meldde aan de DpS, was de e-mail al onderweg naar mij. Dat was toen niet meer terug te draaien.'
(...)
Mevrouw Stijkel: Het e-mailverkeer met Deloitte over dit dossier verliep, voor zover wij hebben kunnen nagaan, vrijwel uitsluitend via het mailaccount van de DpS. Wij vragen ons daarom af waarom het definitieve rapport niet via haar mailaccount is binnengekomen. In dit geval kreeg u het immers in uw eigen mailbox.
Waarom is van de gebruikelijke gang van zaken afgeweken?

De secretaresse: Alle contacten waren die tussen de heer Vriend met de DpS. Die ochtend belde een secretaresse van Deloitte naar het secretariaat van de DpS, dus naar mij. En ik denk dat dat ook de reden is waarom die mevrouw om twee uur 's middags vroeg naar mijn e-mailadres. Dat heb ik gegeven.

Mevrouw Stijkel: Dus in plaats van dat ..

De secretaresse: Ja, als ze had gevraagd naar het e-mailadres van de DpS zou ik dat hebben genoemd.

Mevrouw Stijkel: Maar dat zouden ze toch wel geweten hebben, neem ik aan.

De secretaresse: Ja. Het blijft allemaal heel raar.

De heer Bomhof: Wij zijn in het bezit van een mailtje van de heer Vriend aan de DpS. Dat mailtje is van 14.21 uur. In dat mailtje schrijft de heer Vriend: "U ontvangt het rapport digitaal in pdf." Maar zij kreeg het niet, u kreeg het.

De secretaresse: Ja.

De heer Bomhof: Dat is heel bijzonder.

De secretaresse: Ja. Ik denk dat u die vraag bij de secretaresse van Deloitte neer moet leggen.

De DpS verklaart hierover tijdens de hoorzitting:

De heer Bomhof: Ja, dan ga ik nog even met u terug naar het vorige. U zegt dat u voor de 17e geen toegang hebt gehad tot het bestand van uw secretaresse. Nu is het rapport van Deloitte rechtstreeks naar uw secretaresse gestuurd. Dat is een beetje bijzonder, hebben wij gemerkt vanuit het onderzoek, omdat alle eerdere conceptrapporten rechtstreeks naar u zijn gegaan. Als wij dan kijken naar een e-mail die door het bureau Deloitte is verstuurd waarin wordt aangekondigd dat het rapport op de 10e digitaal zou worden doorgestuurd, dan is dat een mail aan u. Vervolgens zien wij dat het rapport zelf niet bij u komt, maar in afwijking daarvan bij uw secretaresse. Hebt u er een verklaring voor hoe dat kan?

De DpS: Ja, ik denk dat het van belang is dat Deloitte daar antwoord op geeft. Ik heb daar natuurlijk geen directe verklaring voor, behalve dan dat ik in algemene zin kan zeggen dat het contact dat er is met interne en externe instanties soms direct gebeurt, maar ook regelmatig via het secretariaat. Wat dat betreft is dit voor mij niet verwonderlijk.

De heer Bomhof: Het zegt u verder niets. Het is niet ongerijmd, dat de definitieve versie van het rapport bij uw secretaresse terecht komt en alle voorgaande concepten en versies rechtstreeks bij u binnen komen. Dat dit wat ongerijmd is, zegt u verder niets?

De DpS: Nou, u hebt de mail gezien denk ik?

De heer Bomhof: Ja, ja, daar heb ik het ook over.

De DpS: Nou, daarin ziet u dat Deloitte ook vraagt waar de rapporten heen moeten. Het contact dat daarover is geweest, is met mijn secretaresse geweest.

De heer Bomhof: Ik zal u voorlezen wat er in die mail staat. De mail is aan u gericht en er staat: "U ontvangt het rapport digitaal in pdf-formaat via mijn personal assistant" en de mail is aan u gericht en niet aan uw secretaresse.

De DpS: Ik zie mijn secretaresse als een verlengde arm en wat dat betreft zijn wij een goede twee-eenheid. Dit soort dingen gebeurt wel vaker.

Uit het onderzoek van de commissie is niet duidelijk geworden of er die dag nog andere personen op de hoogte waren van het feit dat het rapport eveneens digitaal is binnengekomen. Gedeputeerde mevrouw

Haarsma is die middag samen met de DpS op werkbezoek bij de NAM. Zij kan zich echter niet herinneren of zij die dag (of op welk ander moment dan ook) door de DpS hiervan op de hoogte is gesteld. Wel is zij ervan op de hoogte dat het rapport die dag per koerier wordt bezorgd.

Mevrouw Smith: Wist u ook dat het rapport op 10 november digitaal is verzonden aan de secretaresse van de directie?

Mevrouw Haarsma: Dat wist ik niet.

Mevrouw Smith: Wanneer heeft u dan gehoord dat het digitaal verzonden was aan de secretaresse?

Mevrouw Haarsma: Dat heb ik gehoord op 19 november.

Mevrouw Smith: Waarom op 19 november?

Mevrouw Haarsma: Tijdens het gesprek met de landsadvocaat ving ik terloops op dat er een digitale versie aanwezig was.

Mevrouw Smith: U was de middag van 10 november samen met de DpS op pad. Is toen de digitale ontvangst van het rapport niet ter sprake gekomen?

Mevrouw Haarsma: Voor zover ik mij kan herinneren, niet.

Mevrouw Smith: Heeft u toen wel met haar gesproken over het binnenkomen van de hardcopy van het rapport?

Mevrouw Haarsma: Ook hier geldt: voor zover ik mij kan herinneren, niet.
(...)
Mevrouw Haarsma: U heeft gevraagd of wij daarover gesproken hebben en ik kan mij niet herinneren dat wij daarover gesproken hebben. Dat het binnengekomen was, heb ik toen ik terug kwam van het werkbezoek aan de NAM in ieder geval wel begrepen.

De heer Bomhof: En wat heeft u toen begrepen, wat was er dan binnengekomen?

Mevrouw Haarsma: Ik heb begrepen dat het definitieve rapport was binnengekomen.

De heer Bomhof: En dan gaat het over de digitale versie en over de printversie?

Mevrouw Haarsma: Als ik spreek over het definitieve rapport dan heb ik het over het rapport met de hardcopy.

In de hoorzitting met de DpS is hierover het volgende naar voren gekomen:

'De heer Bomhof: De maandagmiddag dat dit rapport binnen kwam, was u er niet. U bent op stap geweest voor een werkbezoek met mevrouw Haarsma naar een instantie buiten het huis. Hebt u ook met mevrouw Haarsma gesproken over het feit dat de digitale versie van het rapport was binnengekomen?

De DpS: Ik sluit het niet uit, maar ik weet het echt niet meer, dus kan u er geen zekerheid over geven.

De heer Bomhof: Waarom sluit u dat niet uit?

De DpS: Als je met een gedeputeerde samen ergens naar toe bent en er speelt een belangrijk dossier, dan lijkt het voor de hand te liggen dat je ook daarover spreekt. Vandaar dat ik het niet uitsluit.'

Bij terugkomst op het provinciehuis neemt de DpS een afgesloten doos in ontvangst. In de doos zitten de rapporten (tien exemplaren) van Deloitte die door de koerier zijn afgegeven bij de beveiliging van de provincie. De DpS verklaart dat ze deze doos vervolgens in een afgesloten kast op haar kamer heeft geplaatst.

Aan het eind van de middag vindt er een overleg plaats van de ambtenaren die bij het Eurochampdossier zijn betrokken. Bij dit overleg van de zogeheten 'kerngroep Eurochamp' zijn onder meer aanwezig mevrouw Haarsma, haar communicatieadviseur, de DpS en een tweetal andere ambtenaren. Ondertussen wordt er door de aanwezigen gezamenlijk gegeten, waarna betrokkenen het provinciehuis verlaten. Alle bij dit overleg aanwezige personen zijn ervan op de hoogte dat het definitieve rapport die dag is binnengekomen. Eén van de afspraken die is gemaakt na ontvangst van het rapport, is dat het rapport als vertrouwelijk zal worden behandeld. Alle bij het dossier betrokken ambtenaren zijn daarvan op de hoogte.
De communicatieadviseur van mevrouw Haarsma merkt hierover op:

'De definitieve versie van het rapport is in slechts zeer beperkte aantallen beschikbaar gesteld. Verder is binnen de directie, het college en het ambtelijk apparaat, bij alle ambtenaren die erbij betrokken waren, bekend gemaakt dat dit een vertrouwelijk dossier betrof.'

De DpS verklaart het volgende over het overleg:

'De heer Bomhof: Diezelfde maandag is er, toen u terugkwam van het werkbezoek, een overleg geweest met ambtenaren. Dat was een reguliere werkgroep die ook al in de voorfase met het conceptrapport bezig was. Hebben die ambtenaren ook over dit rapport gesproken? Hebt u na terugkomst van het werkbezoek ook deel uitgemaakt van het overleg van die werkgroep? Is daar ook gesproken over de digitale versie en de uitgeprinte versie die waren binnengekomen?

De DpS: Ik was daarbij aanwezig en ik kan mij absoluut niet herinneren dat daarover is gesproken. Misschien kan ik dat nog toelichten? Dat was op dat moment helemaal geen belangrijk feit, want belangrijk was vooral de besluitvorming van de volgende dag in het college.

De heer Bomhof: U zegt dat het geen belangrijk feit was, maar uit het onderzoek is gebleken dat het vooral belangrijk werd geacht dat het definitieve rapport op tijd binnen kwam om aangifte te kunnen doen bij Justitie. Daarvoor was het belangrijk dat het definitieve rapport op maandag 10 november 2009 tijdig zou binnenkomen. Dan zou ik mij kunnen voorstellen dat er in de werkgroep gezegd wordt: "Nou het definitieve rapport is nu echt binnen en dat is heel belangrijk, want nu kunnen wij ook met een gerust gevoel aangifte doen bij Justitie over de zaken die zijn gebleken in het EuroChamp-rapport". Is daar niet over gesproken in de werkgroep?

De DpS: Die kans is heel groot dat zij het daarover hebben gehad.

De heer Bomhof: Dat sluit u ook niet uit?

De DpS: Dat klopt.'

De heer Van Luyn, de advocaat van een van de directeuren (de heer Leijssenaar) van Eurochamp, is eveneens op de hoogte van het feit dat het definitieve rapport van Deloitte die dag bij de provincie zal binnenkomen. Hij probeert die dag contact te leggen met gedeputeerde mevrouw Haarsma en de directeur-secretaris van de provincie. Dat contact komt echter niet tot stand. Wel heeft hij telefonisch contact met een tweetal ambtenaren (waaronder de communicatieadviseur van mevrouw Haarsma), ook behorend tot de

kerngroep Eurochamp. De advocaat stelt in dat gesprek voor om eventueel gezamenlijk op te trekken in de communicatie naar buiten toe. Dat voorstel wordt door de ambtenaren afgewezen.

Tijdens de hoorzitting met de heer Van Luyn komt het volgende naar voren:

De heer De Jong: We gaan even terug in de tijd, op 10 november, volgens ons onderzoek, hebt u contact opgenomen met de provincie, dat is op een maandag geweest, ook de dag waarop het definitieve rapport hier vanuit de provincie is binnengekomen en de vraag is: kunt u toelichten waarom dat was op die 10e november en waarom precies op die dag en hoe die contacten liepen?

De heer Van Luyn: Die 10e november en waarom het precies die dag was: omdat ik wist dat op dat moment, tenminste ik had dat vernomen, het rapport bij de provincie zou zijn. Ik denk dat ik dat van cliënt heb vernomen. Op 10 november heb ik gebeld, verschillende keren, in ieder geval met een betrokken ambtenaar en ik heb gevraagd naar mevrouw Haarsma en in een volgend telefoongesprek naar de directeur-secretaris. Aan beide dames heb ik e-mails gestuurd met de mededeling dat ik probeer tot hen door te dringen en dat ik graag met hen overleg wilde. Met één van hen. Doel daarbij was tweeledig. In de eerste plaats: mijn taak op dat moment was de extreem negatieve berichtgeving proberen een draai ten goede te geven en ik hoopte dat te doen door het Dagblad van het Noorden te bewegen om enige objectiviteit te betrachten in de berichtgeving. Dat was één methode. De andere methode was dat ik graag in contact wilde treden met de belanghebbende mensen binnen de provincie, t.w. mevrouw Haarsma om te bezien hoe nu verder met het naar buiten brengen van het rapport tegen de tijd dat het het levenslicht zou zien. Via in ieder geval een betrokken ambtenaar, maar waarschijnlijk ook nog wel iemand anders van.....

Volgens de betrokken ambtenaar, de communicatieadviseur van mevrouw Haarsma, zou de heer Van Luyn tijdens het gesprek hebben opgemerkt dat de provincie er nog wel eens spijt van zou kunnen krijgen dat ze niet op zijn verzoek ingaan.

Gedeputeerde mevrouw Klip belt op 10 november in de middag twee keer met de journalist de heer Gerard de Kleine van het Dagblad van het Noorden (zie paragraaf 3.6 voor haar verklaringen hieromtrent).

3.3.2 Dinsdag 11 november 2008

Op dinsdagochtend 11 november 2008 heeft mevrouw Haarsma 's ochtends een overleg met een directeur van Deloitte over het rapport. Bij dat overleg zijn ook haar communicatieadviseur en de DpS aanwezig. Tijdens dat gesprek licht de directeur van Deloitte het rapport inhoudelijk nog eens toe. Na dat gesprek vindt de wekelijkse vergadering van GS plaats, waarbij mevrouw Haarsma het rapport van Deloitte toelicht. Op dat moment beschikken de GS leden nog niet over een definitieve versie van het rapport.
Door GS wordt tijdens die vergadering onder meer besloten om op basis van de oplegnotitie en hun kennis van de inhoud van het conceptrapport, dat op 3 november 2008 is verzonden aan de provincie, aangifte te doen bij het Openbaar Ministerie. Tijdens de vergadering ligt er een aantal exemplaren van het concept rapport op tafel. De secretaris van GS heeft verklaard dat geen enkel lid van GS een exemplaar heeft meegenomen.

Na deze GS vergadering, belt mevrouw Haarsma met de journalist de heer De Bruin van het Dagblad van het Noorden. Mevrouw Haarsma verklaart hierover:

'Het gebeurt met enige regelmaat dat wanneer er een persconferentie is geweest, een journalist achteraf nog weer contact opneemt om te vragen of hij nog wat verder mag doorvragen. Dat zou toen ook gebeurd kunnen zijn, dat hij mij heeft gebeld en dat ik hem later heb teruggebeld. Dat gebeurt met enige regelmaat.'

Uit onderzoek van de commissie (analyse toegangsgegevens) is gebleken dat de heer De Bruin die dag niet in het provinciehuis is geweest.

Diezelfde dag wordt door advocaat Van Luyn een persbericht uitgebracht met als titel '*Onderzoeksrapport pleit Leijssenaar vrij*'. De strekking van dit bericht is dat de heer Leijssenaar door het onderzoeksrapport van Deloitte zou worden vrijgepleit en dat Gedeputeerde Staten van de provincie Drenthe het voorstel voor de constructie zouden hebben bedacht aan de hand waarvan de heer Leijssenaar de aanbestedingsregels zou hebben omzeild.
De advocaat belt eveneens met de heer De Bruin, de journalist van het Dagblad van het Noorden. Naar aanleiding van dit telefoongesprek vindt er de volgende dag een gesprek plaats op het advocatenkantoor[4] van de heer Van Luyn in Almere.

Mevrouw Klip belt op 11 november 's ochtends kort met de heer De Kleine van het Dagblad van het Noorden.

3.3.3 Woensdag 12 november 2008

In het Dagblad van het Noorden verschijnt die dag een artikel getiteld '*Directeur van EuroChamp bijt van zich af*'. Het artikel is geschreven door de heer De Bruin. In het artikel worden de heer Van Luyn,de heer Leijssenaar en mevrouw Haarsma geciteerd of aangehaald. Bij het 'citaat' van mevrouw Haarsma wordt aangetekend dat zij zich baseert op bevindingen van het onderzoeksbureau Deloitte.

Die middag vindt er een Statenvergadering plaats. Tijdens die Statenvergadering wordt door mevrouw Haarsma, blijkens het verslag van die vergadering, onder meer het volgende over de vertrouwelijkheid van het rapport gezegd.

'Er is een feitenonderzoek geweest naar het handelen van het management van de Stichting Euro-Champ. De uitkomsten van het rapport zijn zeer privacy gevoelig en natuurlijk speelt het rapport eenbelangrijke rol in de aangifte die de provincie bij het Openbaar Ministerie gaat doen, omdat wij redelijke vermoedens hebben van strafbare feiten. Omdat de privacy in het geding is, kunnen en mogen wij het rapport niet openbaar maken. Dit was overigens ook een voorwaarde van Deloitte. Maar na alle berichtgeving over EuroChamp, ook van de advocaat van het management, meen ik het rapport in ieder geval voor de fractievoorzitters ter inzage te kunnen geven, opdat zij zelf een oordeel kunnen vellen over de inhoud ervan.'
(...)
'Ik ben tot heel veel zaken bereid, maar het gaat nu om een zeer gevoelige materie.
Ik kan het niet en ik wil ook niet dit rapport op de een of andere manier in de openbaarheid brengen.
Dit is ook een strikte voorwaarde van Deloitte en Touche. Wij hebben met die voorwaarde ingestemd en daaraan hebben wij ons dus ook te houden.'
(...)
'Het college wil het rapport gebruiken als onderligger voor de aangifte en in die situatie is het - de heer Van de Boer zei het al - heel dom om al in het openbaar over het rapport te spreken. Zolang een zaak

[4] De heer Van Luyn is werkzaam bij het kantoor Cleerdin & Hamer Advocaten

onder de rechter is, spreken wij er niet over. Ik ga niet op de stoel van de rechter zitten. Zodra de kwestie eenmaal is afgehandeld, zullen wij bekijken hoe het rapport in de staten besproken kan worden.'

Voorafgaand aan de vergadering is er door een verslaggever van RTV Drenthe een email uit het Eurochampdossier van de advocaat Van Luyn verspreid onder de fractievoorzitters van PS. In die email wordt gesproken over de rol van voormalig gedeputeerde de heer Weggemans en de rol van mevrouw Haarsma in het Eurochampdossier. Uit deze email wordt de volgende dag in een krantenartikel van de heer De Bruin geciteerd.

Aansluitend aan de Statenvergadering, vindt er een diner voor Statenleden plaats. Tijdens dat diner wordt mevrouw Haarsma naar eigen zeggen aangesproken door de heer De Bruin die haar het een en ander vraagt over het Eurochampdossier. Mevrouw Haarsma verklaart dat zij hierdoor het gevoel krijgt dat de heer De Bruin reeds over veel informatie beschikt en mogelijk de beschikking heeft over het rapport van Deloitte. Zij deelt dit vermoeden op de avond van het diner met gedeputeerde mevrouw Klip. Mevrouw Klip verklaart hierover later dat zij toen tegen mevrouw Haarsma heeft gezegd dat zij hieraan iets moet doen. Mevrouw Haarsma wist op dat moment al dat de heer De Bruin bij advocaat de heer Van Luyn was geweest:

'... Bij het scheiden van de markt, voor wij rechtstreeks doorgingen naar het begrotingsdiner, heeft mijn communicatieadviseur mij een persbericht in de hand gedrukt en heeft daarbij gezegd: "De Bruin is bij Van Luyn geweest." Meer woorden hebben wij bijna niet gewisseld, want u weet hoe wij daar zitten en na de vergadering zijn wij direct richting begrotingsdiner gewandeld. Dus details heb ik daarover niet gehoord.'

Die avond, na het diner heeft mevrouw Haarsma telefonisch contact met haar communicatieadviseur en met de heer De Bruin. Mevrouw Haarsma verklaart later over dat telefoongesprek:

'Ik heb eerst nog in het provinciehuis gebeld met Martin de Bruin. Ik heb hem aan de lijn gehad, hij was nog in het provinciehuis en was in gesprek met iemand anders. Toen heeft hij gezegd dat ik hem later terug moest bellen. Ik heb hem toen vanuit huis weer gebeld, toen kreeg ik zijn partner aan de telefoon en die vertelde dat hij er even niet was. Zij heeft gezegd dat hij mij terug zou bellen. Dat heeft hij gedaan en toen heb ik hem uiteraard bevraagd op wat hij allemaal wist en hoe hij dat wist. Hij heeft mij toen uitgelegd dat hij 's ochtends bij de advocaat Van Luyn was geweest. Hij heeft mij tevens gevraagd of ik de dag daarop een interview met hem wilde hebben en ik heb daarop gezegd dat ik dat eerst met mijn communicatieadviseur wilde bespreken.'

De communicatieadviseur van mevrouw Haarsma verklaart dat hij die middag, dus nog voor het Statendiner, heeft gesproken met de heer De Bruin die hem toen zou hebben verklaard dat hij inzage in het Deloitte rapport zou hebben gehad op het kantoor van advocaat Van Luyn. Tijdens de Statenvergadering heeft de adviseur dan al een kopie van het persbericht van advocaat Van Luyn overhandigd aan mevrouw Haarsma.

'Ik heb tijdens de Statenvergadering een kopie van dat persbericht gemaakt en met dat persbericht ben ik tijdens de vergadering naar Anneke Haarsma gelopen. Ik heb het persbericht toen aan haar overhandigd en er heel kort met haar over gesproken, omdat het op dat moment niet de plek was om er uitgebreid over in gesprek te gaan'.

'Anneke Haarsma heeft mij op het eind van de avond gebeld. Er waren meerdere dingen. Een punt was dat ik 's middags in de Statenvergadering aanwezig was en bij de pers zat. Mijnheer De Bruin vertelde mij daar dat hij inzage had gehad in het rapport bij de advocaat van de heer Leijssenaar. Hij heeft mij ook een persbericht overhandigd die vanuit de heer Van Luyn richting de media was verspreid. Dat was in ieder geval voor mij een belangrijk punt. Daarnaast hebben wij het gehad over een mogelijk gesprek met de krant'.

Het gesprek tussen de advocaat de heer Van Luyn en de heer De Bruin vindt die middag plaats op het kantoor van de advocaat in Almere. Bij dat gesprek is de cliënt van de advocaat, de heer Leijssenaar, aanwezig. Het gesprek heeft volgens de advocaat ongeveer anderhalf uur geduurd.
De heer De Bruin heeft, behalve tegen bovengenoemde personen, vermoedelijk (blijkens het KPMG rapport) ook tegenover KPMG verklaard dat hij tijdens dat gesprek inzage zou hebben gehad in het dossier/rapport van de heer Van Luyn. Door advocaat Van Luyn wordt dat tijdens de hoorzitting onder ede ontkend:

'Dat klopt niet. In de eerste plaats niet omdat het niet waar is. Ik heb ook geen enkele reden om daarover iets anders te verklaren. Want als nu iemand mij een rapport geeft waar hij zelf 'geheim' op heeft gestempeld ben ik er niet aan gehouden. Dus ik had ook geen enkele moeite gehad om het rapport te verspreiden als dat in het belang van cliënt was geweest. Dus alleen al het feit dat hij mij verwijt van lekken, let wel dit is de man die publiekelijk overal de afgelopen week te kennen heeft gegeven dat hij het rapport bij mij heeft ingezien en nu hier niet is om zijn bron te beschermen. Deze man die zegt dat hij op mijn kantoor bladzij voor bladzij (de heer Van Luyn toont het rapport) dit rapport heeft doorgenomen.'

'De heer De Jong: het zijn 90 pagina's voor zover wij weten.

De heer Van Luyn: ja, één minuut per pagina, waarbij hij ook nog aantekeningen maakte en een interview afnam, vind ik een hele prestatie. Dus kortom, nee hij heeft niet bij mij op mijn kantoor het rapport ingezien.'

Mevrouw Klip belt op 12 november drie keer met de heer De Kleine van het Dagblad van het Noorden. Dit betreft een telefoongesprek in de vroege ochtend, een gesprek in het begin van de middag en een telefoongesprek in de loop van de avond, vermoedelijk na het Statendiner (zie paragraaf 3.6 voor haar verklaringen hieromtrent).

22

3.3.4 Donderdag 13 november 2008

Dit is de dag, waarop volgens de informant, waarmee zowel KPMG als het Statenlid de heer Klaver hebben gesproken, het Dagblad van het Noorden in de ochtend reeds in het bezit zou zijn van een kopie van het definitieve Eurochamprapport.

In het Dagblad van het Noorden verschijnt het artikel '*Provincie hielp bij omzeilen van regels*'. Het artikel is geschreven door de heer De Bruin. In het artikel worden verklaringen van de heer Leijssenaar, oud gedeputeerde de heer Weggemans en mevrouw Haarsma opgetekend.

Op het provinciehuis wordt de doos met rapporten geopend en wordt er een begin gemaakt met de verspreiding van het rapport (zie paragraaf 3.4.2)

Op de ochtend van 13 november 2008 is er een aantal malen telefonisch contact tussen de gedeputeerde mevrouw Haarsma, haar communicatieadviseur en de heer De Bruin. Daarover verklaart de communicatieadviseur:

'Op de 12e 's avonds hebben wij het er even over gehad en op 13 november heb ik 's ochtends contact gehad met Anneke Haarsma. Toen hebben wij gezegd dat wij met Martin de Bruin moesten gaan praten, want op dat moment werden bij de omroep en bij de krant allerlei verhalen gepresenteerd over de manier waarop de provincie een dubieuze rol zou hebben gespeeld bij de aanbesteding. Voor mij was dat het belangrijkste argument om een gesprek met de journalist aan te gaan.

'...Ik heb ook verschillende keren met Martin de Bruin gebeld om het tijdstip te verzetten en uiteindelijk is afgesproken om in Haren het gesprek te hebben.'

Als reden voor het gesprek verklaart mevrouw Haarsma:

'Er werd in de media behoorlijk over het aanbestedingsbeleid van de provincie gesproken en wij hadden de behoefte om uit te leggen hoe dat in elkaar stak.'
(...)
'Dat het natuurlijk niet alleen om het aanbestedingsbeleid ging, maar met name om de inhoud van het rapport, en dat het aanbestedingsbeleid niet de hoofdmoot was van het rapport. Het ging om een andere zaak'.

De communicatieadviseur van mevrouw Haarsma verklaart dat mevrouw Haarsma tijdens dit gesprek opnieuw aan de heer De Bruin heeft gevraagd hoe hij aan zijn gedetailleerde kennis komt van het rapport en/of hij mogelijk inzage heeft gehad in een rapport:

'Wat ik mij kan herinneren is dat al vrij snel in dat gesprek Martin de Bruin met details uit dat rapport kwam. Toen heeft Anneke Haarsma gevraagd hoe hij aan die informatie kwam en toen heeft de heer De Bruin andermaal bevestigd dat hij inzage had gehad bij de advocaat van de heer Leijssenaar.'

Die avond belt mevrouw Haarsma wederom met de heer De Bruin. Uit het onderzoek is niet duidelijk geworden wat er toen is besproken.

Mevrouw Klip belt drie keer met de heer De Kleine van het Dagblad van het Noorden. Dit betreft een telefoongesprek in de vroege ochtend, een gesprek laat in de middag en een telefoongesprek in de loop van de avond.

De heer Van Luyn schrijft op deze dag een brief aan mevrouw Haarsma, waarin hij dreigt met een kort geding als hij niet uiterlijk 17 november 2008 een kopie van het definitieve rapport tot zijn beschikking krijgt.

23

3.3.5 Vrijdag 14 november 2008

In het Dagblad van het Noorden verschijnt het artikel *'EuroChamp deed slechts melding van fraude'*. Het artikel is geschreven door de journalisten Gerard de Kleine en Martin de Bruin. In het artikel wordt mevrouw Haarsma geciteerd:

'..."Op basis van een redelijk vermoeden van strafbare feiten" zegt PvdA – gedeputeerde Anneke Haarsma. Ze verwijst naar een rapport van Deloitte die constateerde dat EuroChamp werkzaamheden niet volgens de richtlijnen aanbesteedde.'

Mevrouw Haarsma belt die dag in ieder geval twee keer met de heer De Bruin. Ook hiervan is tijdens het onderzoek niet duidelijk geworden wat er is besproken tijdens deze gesprekken.
Mevrouw Klip belt drie keer met de heer De Kleine van het Dagblad van het Noorden. Dit betreft een telefoongesprek in de vroege ochtend en twee gesprekken in de middag.

24

3.3.6 Zaterdag 15 november 2008

Op deze dag verschijnen in het Dagblad van het Noorden twee artikelen over het Eurochampdossier. Het eerste artikel is genaamd *'Het rapport over opkomst en ondergang van EuroChamp'* en is geschreven door Gerard de Kleine en Martin de Bruin. In het artikel wordt gemeld dat de krant inzage heeft gehad in het rapport van Deloitte. Het tweede artikel is getiteld *'Advocaat: Jan heeft geen strafbare feiten gepleegd'*. Dit artikel is grotendeels gebaseerd op het interview van de heer De Bruin met de heer Van Luyn en zijn cliënt de heer Leijssenaar. Beide personen komen in het artikel aan het woord.

3.3.7 Maandag 17 november 2008

Er wordt een vervolg gemaakt met de verspreiding van kopieën van het Deloitte rapport.

De DpS belt die avond met haar secretaresse, die op dat moment al thuis is, en vraagt haar om haar inloggegevens (wachtwoord van haar computer), zodat zij de digitale versie van het definitieve rapport van Deloitte kan doorsturen naar de landsadvocaat.
De DpS verklaart hierover als volgt:

De heer Bomhof: Goed, wij gaan naar de 17e. U zegt dat u toen wel het wachtwoord had van uw secretaresse. Dat was voor het eerst en toen heeft u dat gebruikt. Kunt u zeggen waarvoor u dat gebruikt heeft?

De DpS: Er was contact met de landsadvocaat en die wilde voor zijn advies het rapport hebben. Daar heb ik het voor gebruikt, want ik heb het doorgestuurd naar de landsadvocaat.

De heer Bomhof: Dat is 's avonds gebeurd?

De DpS: Dat klopt.

De heer Bomhof: Nu vraagt de commissie zich af waarom u dat nu gaat doorsturen naar de landsadvocaat als normaliter uw secretaresse dat doet en zeker op een tijdstip dat ik mij kan voorstellen dat de landsadvocaat andere dingen te doen heeft dan zakelijke post te bekijken. Het had ook de dag daarna gekund. Waarom moest u zo nodig zelf die avond dat rapport nog versturen?

De DpS: Voor zover mijn herinnering strekt was er steeds veel druk op wat er speelde. Er was natuurlijk ook veel commotie in de pers, dus dat betekende dat wij snel de zaken wilden regelen. De juridisch medewerker had contact met de landsadvocaat en gevraagd of hij advies zou kunnen geven en er was veel belang bij om dat snel te doen. De secretaresse was weg en vandaar dat ik als dienstverlenend ambtenaar het op mij heb genomen om ervoor te zorgen dat het ook snel voor elkaar was.'

De secretaresse verklaart, dat zij niet verbaasd was over het verzoek van de DpS:

De heer Bomhof: (...) Op 17 november vraagt de DpS uw wachtwoord om het rapport van Deloitte door te kunnen mailen naar de landsadvocaat. Ik neem aan dat het u verbaasde dat dit gebeurde, want normaliter zendt u de stukken door en niet de DpS.

De secretaresse: Het heeft mij niet verbaasd.

De heer Bomhof: Vroeg zij dan wel eens vaker om uw wachtwoord?

De secretaresse: Nee.

De heer Bomhof: Ik spreek over verbazing omdat zij het a. niet eerder deed en b. omdat zij het rapport 's avonds naar de landsadvocaat wilde doorzenden, terwijl die er die avond waarschijnlijk ook helemaal niets mee zou doen. Het rapport zou de dag daarna dus ook wel verzonden kunnen worden en dan zou u weer op kantoor zijn.

De secretaresse: Nee, ik heb geen vraagtekens gezet bij de noodzaak van het doorsturen. Ik heb tot dit jaar – verleden jaar heb ik helemaal geen last gehad van het rapport van Deloitte – ook helemaal niet begrepen wat er aan de hand was.'

3.3.8 Woensdag 19 november 2008

Advocaat de heer Van Luyn heeft opnieuw een gesprek met de heer De Bruin. Daarbij is ook de journalist de heer De Kleine aanwezig.
Over dit gesprek verklaart de heer Van Luyn het volgende:

'Dat was op initiatief van De Bruin. Die heeft mij gebeld en ze wilden de zaak nog een keer bespreken. Ik heb toen overleg gehad met cliënt en gevraagd wat hij daarvan vond en gezamenlijk hebben wij besloten dat er nog best het één en ander bij te sturen viel en daarom hebben we ze nog een keer uitgenodigd en nog een keer te woord gestaan. Bij dat gesprek lag deze map wel op tafel. Deze zelfde map. Ik heb daar af en toe naar gekeken. Maar ik heb een fors formaat bureau, dat mag u gerust weten, hij kan niet ondersteboven dat rapport hebben gelezen en zeker niet iedere bladzijde.'

De heer Van Luyn meent dat de journalisten de beschikking hadden over het rapport:

'Ja, op twee manieren. Simpelweg door de kennis die ze bezaten en het andere punt is dat ze bepaalde kennis hadden die alleen in het definitieve rapport naar voren kwam zoals ik zo-even noemde het voorbeeld van Ludgert Management. Dat staat alleen in de definitieve versie van het rapport.'

3.3.9 Vrijdag 21 november 2008

Het Statenlid de heer Klaver wordt thuis opgezocht door een informant. Volgens de heer Klaver vertelt deze informant hem onder meer dat het Dagblad van het Noorden al op de ochtend van 13 november 2008 in het bezit is van het Eurochamprapport van Deloitte. Later die dag maakt de heer Klaver een kopie van het rapport dat de informant in zijn bezit heeft.
De heer Klaver verklaart later tegenover de commissie dat de versie die hij heeft gekopieerd van de informant, volgens de informant dezelfde versie is als de versie die de krant tot zijn beschikking heeft.

Diezelfde dag belt de heer Klaver met de directie van de provincie en doet navraag naar het mogelijk uitlekken van het Eurochamprapport.
Tijdens de hoorzitting komt dit als volgt ter sprake:

De heer Vester: Waarom heeft u er dan voor gekozen de weg te bewandelen die u heeft bewandeld? Het gaat dan om de manier waarop u dit alles naar buiten heeft gebracht. Waarom heeft u uw informatie niet meteen aan GS of aan de directie overhandigd?

De heer Klaver: Zo simpel was het niet. Het lijkt simpel, maar dat was het niet.
Ik zal nu toch iets over mijn beweegredenen vertellen. Toen er op enig moment – ik meen dat het ook op vrijdag 21 november was - in het Dagblad van het Noorden op pagina 3 een redactioneel stukje stond, waarin werd gemeld dat de advocaat de heer Van Luyn in een zodanig daglicht stond dat hij mogelijk de oorzaak van het lek was en had aangekondigd op 4 december een kort geding aan te spannen, hadden wij, zeker na het bezoek van 11 uur, ernstige vermoedens en aanwijzingen dat er uit dit huis gelekt werd. Na mevrouw Rozema, de statengriffier, te hebben geconsulteerd en overleg te hebben gehad met mijn fractiegenoten, zijn er in de loop van die middag een drietal vragen aan GS opgesteld, waarin wij antwoord wilden op de vraag of ons vermoeden correct of niet correct was.
Dat was voor ons de vraag en die vraag is nog steeds aan de orde. De fractie van het CDA heeft het ernstige vermoeden dat er op ongeoorloofde wijze vroegtijdig informatie naar buiten is gegaan.
En wat er allemaal omheen komt, zullen wij straks wel in het rapport van deze commissie lezen.

De directeur-secretaris (hierna te noemen DS) van de provincie verklaart hierover:

' Meneer Klaver heeft op vrijdagochtend gebeld met de vraag. Hij heeft ook gevraagd of ik wist hoeveel exemplaren er binnen waren gekomen. Ik heb gezegd een handjevol en dat die achter slot en grendel lagen. Ik heb dat ook eerlijk verklaard in het interview met u. Vervolgens heeft hij zijn vermoedens uitgesproken, dat heb ik voor kennisgeving aangenomen en ik heb onmiddellijk de waarnemend commissaris van de Koningin gebeld, mevrouw Haarsma. Ze was op weg naar een vergadering in Leeuwarden en is ter plekke omgekeerd naar het provinciehuis. Daar hebben wij verder over de zaak gesproken. 's Middags kwamen er vragen binnen van het CDA over het vermeende lek. Daar hebben wij een brief over doen uitgaan en wij hebben er dinsdag ook over gesproken in het college en dat is de aanleiding geweest om een vraag neer te leggen bij het Openbaar Ministerie om eventueel een strafrechtelijk onderzoek in te stellen.'

(...)

De heer De Jong: Twee dingen: u refereerde net aan het telefoontje met de heer Klaver waarin hij vermoedens uitsprak. Kunt u wat meer over die vermoedens zeggen, wat u toen gehoord hebt?

De DS: Dat hij dacht dat er een lek zou zijn en dat hij een document in handen had waarvan hij dacht dat het niet in zijn handen zou moeten zijn.

De heer De Jong: Heeft hij toen verklaard dat hij het document had dat beslist niet bij hem mocht zijn? Dan is het niet meer denken, dan heb je feiten zou ik zeggen. Mijn vraag daaraan gekoppeld is, wij weten ondertussen dat voor die datum van 21 november al in dit huis gesproken is over een lek. Maar dat was voor u het eerste moment dat u het hoorde?

De DS: Wel van een vermeend lek vanuit het provinciehuis. Voor die tijd is er wel gesproken, maar daar hadden wij onze vermoedens over, en dat staat ook in het KPMG-rapport, dat de heer Van Luyn ook een aantal berichtgevingen in de krant heeft neergezet. Dus er was nooit aanleiding voor ons in eerste instantie dat het een lek van het provinciehuis zou zijn.

De heer Bomhof: Wat ik nog graag zou willen weten is: u heeft natuurlijk ook wel zich er van vergewist of er in dit huis niet zou zijn gelekt, een soort check, iedereen kan het altijd beweren, maar stel je nou voor dat het echt zo is. Wat heeft u nou intern naar de ambtenaren gedaan om u er van te vergewissen of er al dan niet gelekt is. Kunt u dat vertellen?

De DS: Alle ambtenaren die in het kerngroepje zaten, waarover u ook vanochtend wat gehoord heeft, plus alle bestuurders zijn bij mij op de kamer geweest. Ik heb hen expliciet gevraagd of ze de eed of belofte hebben afgelegd en stuk voor stuk of ze gelekt hadden, of op een andere wijze het document verspreid hadden. Daar heeft iedereen 'nee' op geantwoord.'

3.3.10 Maandag 24 november 2008

De digitale versie van het rapport wordt uitgeprint, waarna ambtenaren van de provincie een begin maken met het verwijderen van namen uit het rapport, zodat er een 'geschoonde' versie ontstaat die voor verdere verspreiding geschikt is.

Advocaat de heer Van Luyn ontvangt een fax van de journalist de heer De Kleine. Deze fax bevat een kopie van bladzijde 17 van het definitieve rapport van Deloitte. Volgens advocaat Van Luyn heeft de heer De Kleine hem die fax gestuurd als bewijs van het feit dat de krant de beschikking heeft over het definitieve rapport van Deloitte. Over deze fax, waarvan de onderzoekscommissie een kopie heeft ontvangen, zegt de heer van Luyn het volgende:

'Ik werd door De Kleine gebeld en die liet mij weten dat het rommelde op de redactie. Er was sprake van enige animositeit tussen de beide heren journalisten. Hij zei mij, wij hebben inzage gehad in de definitieve versie van het rapport en ten bewijze daarvan zal ik je één pagina daarvan faxen. Hij heeft die naar mij gefaxt, hij verzocht mij om de kopregel er af te knippen. Dat heb ik gedaan. Vervolgens belde hij nog een keer en zei: maar laat de datum en de tijd er alsjeblieft aanzitten, dat lijkt me wel zo handig. Ik zei daarop: oh ja, da's waar ook. Dus die heb ik er weer bijgedaan en ik heb die fax hier in mijn dossier zitten.

De heer De Jong: Kunt u die datum nog noemen, wanneer dat was?

De heer Van Luyn:Jazeker, dat was 24 november 2008.

De heer De Jong: En uit die fax bleek u .....

De heer Van Luyn: Het was een willekeurige bladzijde uit het rapport, het is bladzijde 17 van 91, 10 november 2008 en er staat een nummer boven wat eindigt op 2111.

De heer De Jong: Dat hebben wij ook gecontroleerd, dat is de definitieve versie van het rapport. Wat is de reden dat hij u dat gefaxt heeft?

De heer Van Luyn: De reden was dat hij meende dat we tot op zekere hoogte door de heer De Bruin in de maling genomen werden. Daarom wilde hij mij een bewijs in handen geven dat zij wel de definitieve versie van het rapport hadden. Het kwam hem namelijk voor dat De Bruin mij aanwees als degene die het rapport zou hebben gelekt. Het enige rapport wat ik had, zo wist ook De Kleine, was de conceptversie, de definitieve versie was nog niet beschikbaar behalve bij het Dagblad dat kennelijk inzage had gehad. Met die fax bewees hij dat.'

Vermoedelijk op 24 november 2008 (of om en nabij deze datum) stuurt de heer Westera, chef redactie Drenthe van het Dagblad van het Noorden een email aan zijn hoofdredactie en in cc aan de heer De Bruin en de heer De Kleine. Deze email is later in het bezit gekomen van de heer Klaver. Tijdens de hoorzitting heeft de heer Klaver deze email voorgelezen:

"Collega's,
we staan voor een dilemma. Hoe nu verder met EuroChamp nu de zaak zich dreigt toe te spitsen op de vraag wie er heeft gelekt naar het Dagblad van het Noorden. Ik denk te weten dat het goede antwoord op die vraag tot politieke beroering en wellicht gevolgen zal leiden. Juist omdat wij min of meer betrokken zijn bij deze zaak – wij zijn de ontvangers van het lek – is alles wat wij doen ook in zekere zin verdacht.
Het verstandigste is nu, denk ik, stilzitten en ons houden bij en aan de feiten. In mijn optiek is het beschermen van de bron nu van groter belang dan het aanzwengelen van de op zich terechte discussie of door het hoogste bestuurlijke orgaan wellicht een politieke doodzonde is begaan door het lekken. Als krant verspelen we enorm veel gezag, invloed en betrouwbaarheid als wij nu mede aankoersen op de onthulling van de bron."

De commissie meent dat deze email met name relevant is voor het onderzoek, omdat de krant er op zinspeelt dat de onthulling van hun eigen bron tot politieke beroering en wellicht gevolgen zou kunnen leiden. Volgens de commissie volgt hieruit dat de bron van het Dagblad van het Noorden dus kennelijk niet (of niet alleen) de heer Van Luyn is, maar iemand, wiens onthulling tot politieke beroering en gevolgen zal kunnen leiden.
De communicatieadviseur van mevrouw Haarsma is door de heer Westera gebeld over deze email. Hij verklaart hierover:

'Met de heer Westera heb ik contact gehad. Dat is de chef-redactie voor Drenthe. Hij belde mij naar aanleiding van de Statenvergadering van 18 maart jongstleden.' (...) *'Hij belde mij omdat hij wilde weten of de mail waaruit werd geciteerd, zijn mail was.'*

3.3.11 Woensdag 26 november 2008

De journalist de heer De Kleine van het Dagblad van het Noorden stuurt een e-mail aan de communicatieadviseur van mevrouw Haarsma. De adviseur heeft deze e-mail voorgelezen tijdens de hoorzitting op 16 juni 2008:

'Paul, dank. Zoals je ongetwijfeld weet ben ik van het dossier gehaald. Dat is gisteren gebeurd. Aangezien ik deze vragen eerder had uitstaan (dus voor de beslissing van de hoofdredactie), wilde ik toch graag het antwoord. Het was een korte, heftige samenwerking en ik heb niets dan lof voor de wijze waarop jij mij van informatie over het wespennest van EuroChamp hebt voorzien. Tot slot, let op uw saeck. Hartelijke groet, Gerard de Kleine'.

De communicatieadviseur verklaart dat het hem niet duidelijk was wat de heer De Kleine met deze email heeft bedoeld:

'De kwalificatie 'let op uw saeck' was voor mij de reden dat ik eerst Gerard de Kleine heb gebeld. Die vertelde mij dat hij geen mededelingen meer kon doen over deze zaak. Dit was op een woensdag en Martin de Bruin was hier in huis. Ik heb toen hem ook gevraagd hoe het zat, want jullie werken toch samen aan dit dossier. Martin de Bruin vertelde dat er andere werkafspraken waren gemaakt. Ik ben hiermee naar mijn teamleider gegaan, naar de directie en naar de gedeputeerde.'

Mevrouw Haarsma, die deze email onder ogen krijgt van haar adviseur, verklaart hierover tijdens de hoorzitting:

'Ik heb tegen hem gezegd: Dit moet je bewaren.'

De heer Bomhof: Maar ik kan mij ook voorstellen dat u hebt gezegd: "Wat is dat een rare mail. Ik heb geen contact gehad met de heer De Kleine en jij kennelijk wel. Wat heeft zich tussen jullie afgespeeld?" En dat zal hij u dan vast wel verteld hebben.

Mevrouw Haarsma: Ik wist dat de heer De Kleine samen met de heer De Bruin aan het EuroChamp-rapport werkte, dus dat vond ik niet zo vreemd. Mijn communicatieadviseur heeft mij ook gezegd dat hij gebeld werd door De Kleine, die hem informatie vroeg. Dus dat is helemaal niet vreemd.

De heer Bomhof: Dus de kwalificaties "korte, heftige samenwerking" en "wespennest" vindt u, gelet op die samenwerking, helemaal niet vreemd?

Mevrouw Haarsma: Ik geef daar geen kwalificatie aan, want ik heb de mail niet geschreven.

Mevrouw Smith: Waarom heeft u tegen de heer Van den Bosch gezegd dat hij die mail goed moest bewaren?

Mevrouw Haarsma: Dat was gezien alles wat op dat moment aan de orde was.'

3.3.12 Donderdag 27 november 2008

Een geschoonde versie van het rapport wordt openbaar gemaakt en verzonden naar Statenleden en personen die op basis van de Wet openbaarheid van bestuur het rapport hebben opgevraagd.
De heer Van Luyn ontvangt die dag van de provincie ook een kopie van het definitieve rapport. Dit betreft een niet-geschoonde versie.

3.3.13 Zaterdag 29 november 2008

In het Dagblad van het Noorden staat een hoofdredactioneel commentaar, getiteld *'De heilige bronnen'* waarin de hoofdredacteur van de krant ingaat op het lekken van het Eurochamprapport. In het stuk schrijft de hoofdredacteur onder meer:

'Het rapport was gemaakt in opdracht van de provincie. Die wilde dat niet openbaar maken, omdat dat de privébelangen van particulieren zou kunnen schaden. Toch heeft de krant er de hand op weten te leggen. We hebben er uitvoerig uit geput in onze verslaggeving over de zaak.'
(...)
'Als het tot een officieel onderzoek naar het lek komt, bestaat de kans dat ook bij de krant wordt aangeklopt. Zou de redactie haar bron dan onthullen? In geen geval.'
(...)
'Nu die wet onderweg is naar de Kamer, is de kans gering dat onze verslaggever of ondergetekende in het gevang belanden als zij weigeren te vertellen hoe de krant aan het rapport van Deloitte is gekomen. Gelukkig maar. Hoewel we het er gerust op hadden laten aankomen. Want de bron is heilig in het krantenvak.'

Deze lijn wordt nogmaals bevestigd in een hoofdredactioneel commentaar op 20 juni 2009.

3.4 Overige feiten en omstandigheden

In deze paragraaf worden een aantal bevindingen besproken die in de reconstructie niet of slechts gedeeltelijk aan de orde zijn gekomen, maar die de commissie wel relevant vindt om te vermelden.

3.4.1 Gelekte versie

Door KPMG is vastgesteld dat er een aantal versies van het Deloitte rapport in omloop zijn geweest. Dit betreffen de volgende vier versies[5]:

1. Een concept versie d.d. 7 oktober 2008 die in het kader van hoor en wederhoor aan betrokkenen in het Eurochamponderzoek is voorgelegd.
2. Een concept versie met nummer 3112182270/2135 die op 3 november 2008 per e-mail is verstuurd naar de provincie en op basis waarvan op 4 november 2008 overleg tussen de provincie Drenthe en Deloitte heeft plaatsgevonden.
3. De digitale versie van het definitieve rapport met nummer 311218227/2111 die op 10 november 2008 door Deloitte per email is verstuurd aan de secretaresse van de directie van de provincie.
4. De ingebonden versie van het definitieve rapport met nummer 311218227/2111 die op 10 november 2008 door Deloitte per koerier aan de provincie is verzonden.

[5] KPMG rapport d.d. 10 maart 2009, 'Onderzoek naar mogelijke voortijdige verspreiding rapport Eurochamp'

Door KPMG is geconcludeerd dat het de onder nummer 3 genoemde versie betreft, die voortijdig buiten het provinciehuis terecht is gekomen. De commissie heeft kennis genomen van de verschillende versies en de verschillen hiertussen eveneens vastgesteld.
Het verschil tussen de digitaal verzonden versie van het definitieve rapport en de per koerier verzonden versie betreft een pagina uit de bijlage die in de digitale versie van het rapport wel voorkomt, maar niet in de 'papieren' versie. Daarnaast is er een lay-out verschil tussen de beide versies. De commissie komt daarmee tot dezelfde conclusie als KPMG.
Overigens heeft de commissie nog een extra bevinding gedaan in de versie die de heer Klaver in handen heeft gekregen, te weten een blanco pagina na pagina 45. De digitaal verzonden definitieve versie van het rapport bestond uit drie PDF-bestanden. Het eerste deel beslaat pagina 1 tot en met 45. Het tweede deel begint op pagina 46.
De commissie heeft geconstateerd dat de versie die de heer Klaver in handen heeft, een blanco pagina bevat ná pagina 45 en vóór pagina 46. Als het eerste deel van de digitale versie dubbelzijdig wordt uitgeprint of wordt gekopieerd, dan is deze blanco pagina na bladzijde 45 goed te verklaren. De commissie meent dat dit een extra aanwijzing is voor het feit dat het de digitale versie van het definitieve rapport betreft, welke is uitgelekt.

3.4.2 Verspreiding rapporten

Het rapport voor hoor en wederhoor is op 7 oktober 2008 door Deloitte verstrekt aan de heer Leijssenaar. Het conceptrapport met nummer 3112182270/2135 is op 3 november 2008 door Deloitte per email aan de DpS en aan de directeur SEO van de provincie verzonden.
Deze conceptversie is vervolgens door beide personen doorgestuurd per email aan een viertal ambtenaren en aan gedeputeerde mevrouw Haarsma.

Op 10 november 2008 is de definitieve versie van het rapport per email verzonden door Deloitte aan de secretaresse van de directie. Volgens de verklaringen van betrokkenen zou deze versie verder niet verspreid zijn, behalve op 17 november 2008, toen deze versie is doorgestuurd per email door de DpS aan de landsadvocaat.

De doos met de tien definitieve versies van de rapporten, die op 10 november 2008 bij de provincie werd bezorgd, is pas op 13 november 2008 geopend. Op die dag krijgt de DpS een versie, de communicatieadviseur van mevrouw Haarsma en een ambtenaar uit de kerngroep Eurochamp. Op 17 november 2008 zijn zes rapporten verspreid. Twee rapporten zijn afgegeven bij de politie. Twee rapporten zijn aan de griffie overhandigd, voor inzage voor de fractievoorzitters van PS. Een exemplaar is aan mevrouw Haarsma overhandigd en er is een exemplaar gegeven aan een van de ambtenaren uit de kerngroep. Op 20 november 2008 is er een exemplaar aan SNN gegeven. Tevens is er vanaf 17 november 2008 een aantal kopieën gemaakt en intern verspreid.

3.4.3 GS vergadering 11 november 2008

Op 11 november 2008 heeft er een vergadering van GS plaatsgevonden. Tijdens de vergadering is een aantal besluiten genomen ten aanzien van het Eurochampdossier.
Deze besluiten zijn genomen op basis van een oplegnotitie die op 7 november 2008 door een ambtenaar van de provincie is opgesteld.
In deze oplegnotitie was een risicoparagraaf opgenomen waarin onder meer wordt gesproken over het risico van negatieve beeldvorming. Er wordt gesteld dat door de relatie die de provincie heeft met de stichting Eurochamp het beeld kan ontstaan dat de provincie haar toezichthoudende rol onvoldoende heeft ingevuld. Ook wordt gesteld dat de schuldvraag voor het faillissement van Eurochamp bij de provincie zou

kunnen worden gelegd. Volgens de opsteller van de notitie, kunnen op basis van de analyses van Deloitte deze beweringen worden weerlegd.'

De beleidsmedewerker Sport die de oplegnotitie heeft geschreven, zegt hierover het volgende:

'Eurochamp is van begin af aan een organisatie geweest, die door heel veel mensen als positief werd gezien. Toen bij ons de mogelijke misstanden werden gemeld en wij het voornemen kenbaar hadden gemaakt de subsidie stop te zetten, was de reactie van de buitenwereld er een van: hoe kan je dat nu doen, want het is zo'n goede organisatie.
De beeldvorming zou daarom kunnen ontstaan dat wij heel snel subsidies zomaar stopzetten met de kans dat een organisatie failliet gaat. Zou dit gebeuren dan zou, als wij geen goede argumenten hadden waarom wij de subsidie hadden stopgezet, de schuld bij de provincie worden gelegd. Dat was de achterliggende gedachte van de paragraaf risico's beeldvorming. Daarnaast was er nog het feit dat de advocaat de heer Van Luyn de eerste week van november een persbericht had verspreid waarin werd gesteld dat de rapportage van Deloitte de heer Leijssenaar vrijpleitte. Daarbij heeft hij quotes uit de rapportage naar voren gehaald, waarin met name werd gezinspeeld op de betrokkenheid van onze bestuurders bij aanbestedingen die mogelijk niet conform de regels zouden zijn.
Maar wij hadden ook het rapport en uit dat rapport blijkt iets anders.
Met het oog op die twee aspecten: negatieve beeldvorming en de al in de media circulerende gedachte dat de provincie ook enige schuld had, is de risicoparagraaf geschreven.

De heer Beerda: Dat betekent dat de provincie uit een oogpunt van mediastrategie op dat moment ook belang had bij het rapport.

De beleidsmedewerker Sport: Ja.

De heer Beerda: En ook bij het wereldkundig maken van het rapport.

De beleidsmedewerker Sport: Wij hebben uitvoerig overleg met Deloitte gehad over de vraag welke gegevens wij zouden mogen gebruiken en welke niet. Het was immers een vertrouwelijk rapport, ook vertrouwelijk voor ons. Die afspraak was gemaakt toen Deloitte het onderzoek ging starten. Er gelden gewoon bepaalde normen als je een forensisch accountantsonderzoek laat doen.
Er zat dus wel enige spanning tussen wat wij wel en wat wij niet zouden mogen vertellen, maar wij hebben altijd heel zorgvuldig met onze juristen bekeken wat wij wel zouden mogen vertellen. Wij hebben Deloitte ook gevraagd om een openbare samenvatting te schrijven omdat wij het rapport niet konden en niet wilden openbaar maken. Pas later werd het rapport wel openbaar.'

Voor zover de commissie heeft kunnen vaststellen, is de hier door de beleidsmedewerker Sport genoemde samenvatting niet openbaar gemaakt.

Gedeputeerde mevrouw Haarsma kan zich de betreffende risicoparagraaf uit de oplegnotitie niet meer zo goed herinneren:

'Ik heb net gezegd dat ik het mij niet meer kan herinneren. Maar, nogmaals, bij ieder stuk voor PS of GS wordt een risicoparagraaf geschreven. En daarbij ga je van het ene uiterste naar het andere uiterste. Er wordt dus gewezen op zowel de positieve als de negatieve kanten. Dat was hier ook aan de orde, maar ik ken die paragraaf niet meer uit het hoofd.'

Tijdens de GS vergadering is er waarschijnlijk niet expliciet over de risicoparagraaf gesproken, in ieder geval kan geen van de leden van GS die zijn gehoord door de commissie zich daar iets van herinneren.

Door GS wordt, blijkens de besluitenlijst, tijdens de vergadering onder meer besloten tot het doen van aangifte bij het Openbaar Ministerie in verband met mogelijke strafbare feiten, het voornemen kenbaar te maken aan Stichting Eurochamp om subsidiebeschikkingen van in totaal € 360.000 in te trekken, het kenbaar maken van het voornemen tot terugvordering uitbetaalde voorschotten, het afwijzen van verzoeken van derden om een exemplaar van het rapport te mogen inzien op grond van de Wet openbaarheid van bestuur en het informeren van PS middels een brief.

3.4.4 Sms'je

Naast de hiervoor genoemde email, heeft de heer Klaver tijdens zijn gesprekken met de commissie ook gerefereerd aan een sms'je dat hij op 19 december 2008 van gedeputeerde mevrouw Klip heeft ontvangen. De tekst van dit sms'je luidt:

'Dag Henk,
ik ben alweer op weg naar Utrecht. Dank voor je bericht. Martin de Bruin onderhoudt nauwe contacten met de afdeling communicatie en is behulpzaam bij het bedenken van scenario's. Vreemd op zijn zachtst gezegd.'

Tijdens de hoorzitting zegt de heer Klaver desgevraagd dat hij verder niet veel contacten heeft gehad met mevrouw Klip over het vroegtijdig uitgelekte rapport:

'Ja, daar kan ik wel iets meer over zeggen. Nee, er is geen intensiever contact geweest. Het ging met name over, de een noemt het helpen en de ander bemoeizucht van de krant met de mensen van de afdeling communicatie in dit huis over en weer. Dat is een van de zorgpunten die wij al aan het begin van dit hele dossier aan de orde hebben gesteld toen het in dit politieke domein op tafel kwam.'

Mevrouw Klip zegt het volgende over het verstuurde sms'je:

'Ik heb af en toe telefonisch of sms-contact met de heer Klaver, maar dat is sporadisch. En, ik moet u zeggen dat ik nou niet specifiek iets kan herinneren waar dat over gaat.'
(...)
'Dat kan ik, zoals u ook al in uw inleiding zei of uw vraagstelling formuleerde: dat is een reactie op een sms van hem. Ik reageer op iets wat hij zegt. Dat weet ik niet meer want ik bewaar die sms'jes niet. De strekking van mijn opmerking van dat sms'je is dat het mij bevreemdde, dat staat ook in dat sms'je, dat een journalist die hoofdscribent was van, zeg maar, de artikelen over het onderwerp waar ook uw onderzoek over gaat, samen met de afdeling communicatie, zoals ik het begrepen heb via de tam-tam in het provinciehuis, nadenkt over een, ik weet niet meer precies hoe het er letterlijk staat, welk woord ik daar in gebruik, scenario's, hoe de informatie dan wel bij de krant gekomen kan zijn. Dat vond ik een beetje vreemde combinatie.'

3.5 Bevindingen digitaal onderzoek

De commissie heeft een uitgebreid digitaal onderzoek uitgevoerd.[6] Hiervan is een afzonderlijke rapportage gemaakt. Deze rapportage is om privacyredenen niet als bijlage bij het rapport van de commissie gevoegd.[7] In deze paragraaf zijn de belangrijkste bevindingen vermeld.

3.5.1 Onderzoek werkplek/computers

De commissie heeft een digitaal onderzoek uitgevoerd op de werkplek (lees: computer) van de secretaresse van de directie, de werkplek van mevrouw Haarsma, die van haar communicatieadviseur en de werkplek van de DpS. Bij dit onderzoek is onder meer met behulp van steekwoorden gezocht naar mogelijke aanwezigheid van, of verwijzingen naar het Eurochamprapport, specifiek in de periode van 10 tot en met 13 november 2008.

Computer/werkplek van de secretaresse van de directie
Op basis van analyse van de Microsoft Windows systeem logbestanden is het waarschijnlijk dat het computersysteem van de secretaresse van de directie niet aan heeft gestaan in de avonduren van 10, 11, 12 en 13 november 2008. Op deze computer zijn geen sporen aangetroffen op basis waarvan vastgesteld kan worden of het rapport in de onderzoeksperiode is uitgeprint.
De commissie heeft digitale sporen aangetroffen van het gebruik van externe opslagmedia, echter niet van het gebruik van externe opslagmedia in november 2008. Wel van het gebruik hiervan vóór en ná november 2008.
De commissie heeft tevens onderzoek gedaan naar het gebruik van externe webmail diensten alsook chat services. Dit om uit te sluiten dat dergelijke diensten gebruikt zijn om het onderzoeksrapport naar de buitenwereld te zenden. Hierbij zijn geen digitale sporen aangetroffen die er op duiden dat gebruik is gemaakt van webmail (Google, Hotmail, etc.) of chat services in de genoemde onderzoeksperiode.
Het steekwoordenonderzoek heeft geen voor het onderzoek relevante resultaten opgeleverd.

Computer/werkplek van de DpS
De commissie heeft digitale sporen aangetroffen die zeer aannemelijk maken dat op 17 november 2008 in de avond omstreeks 18:24 uur is ingelogd onder het gebruikersaccount van de secretaresse van de directie. Op basis van deze sporen is ook zeer waarschijnlijk dat slechts eenmaal is ingelogd op deze computer onder dit account.
De commissie heeft sporen aangetroffen op basis waarvan het zeer waarschijnlijk is dat tijdens die login actie op 17 november 2008 de Deloitte documenten op het provincie netwerk zijn geplaatst. Deze sporen maken zeer aannemelijk dat de Deloitte rapportage documenten zijn geopend en opgeslagen op 17 november 2008. Deze bevindingen komen overeen met de verklaring van de DpS omtrent het doorzenden van het rapport aan de landsadvocaat op 17 november 2008.

---

[6] Het digitale onderzoek is uitgevoerd door specialisten van het onderzoeksbureau dat de commissie heeft ondersteund.
[7] De rapportage ligt voor statenleden vertrouwelijk ter inzage bij de Statengriffie.

Het steekwoordenonderzoek op de betreffende computer heeft verder geen voor het onderzoek relevante resultaten opgeleverd.

Computer/werkplek van mevrouw Haarsma
Op basis van analyse van de Microsoft Windows systeem logbestanden is het zeer waarschijnlijk dat het computersysteem van mevrouw Haarsma niet aan heeft gestaan in de periode van 6 tot en met 28 november 2008. Om die reden heeft de commissie verder geen digitaal onderzoek gedaan op dit systeem.

Computer/werkplek van communicatieadviseur van mevrouw Haarsma
Het steekwoordenonderzoek op deze computer heeft geen voor het onderzoek relevante resultaten opgeleverd.

3.5.2 Onderzoek mailomgeving

De commissie heeft onderzoek gedaan op zowel de logbestanden van de e-mail omgeving alsook een restore van diezelfde e-mail omgeving gedateerd op 14 november 2008.
Het onderzoek op de logbestanden is gedeeltelijk dezelfde stap die het onderzoeksteam van KPMG destijds heeft uitgevoerd. Zij hebben destijds de grootte van het bericht van Deloitte gebruikt als gegeven voor een zoekslag in die logbestanden, om daarmee vast te stellen of het bericht na ontvangst is doorgestuurd. Het originele bericht inclusief bijlagen heeft als grootte 9,5 Megabytes.

De commissie heeft daarenboven de mailbox van een 16-tal personen geëxporteerd uit de restore van de Groupwise omgeving. Deze mailboxen zijn onderzocht op aanwezigheid van een e-mail bericht met één of meerdere bijlagen zoals aangeleverd door Deloitte. Daarbij is alleen het oorspronkelijke bericht aangetroffen in de inbox van de mailbox van de secretaresse van de directie. De commissie heeft in deze export geen sporen aangetroffen die er op wijzen dat het bericht is doorgestuurd.
Daarbij dient wel opgemerkt te worden dat wanneer het bericht op 10, 11, 12 of 13 november 2008 zou zijn doorgestuurd en vervolgens meteen verwijderd is, dat niet zichtbaar zal zijn in de back-up van 14 november 2008. Om die reden kan de commissie niet uitsluiten dat het bericht intern is doorgestuurd. Andere back-ups dan de gebruikte 'week back-up' van 14 november 2008 zijn niet beschikbaar.

3.5.3 Intern doorsturen e-mail

De commissie heeft bij aanvang van het onderzoek het vermoeden dat het intern doorsturen van een extern e-mail bericht binnen de Groupwise omgeving niet zonder meer resulteert in een nieuw bericht met de gelijke omvang van 9,5 Megabytes, in ieder geval niet als zodanig weergegeven in de logbestanden. Het Groupwise mailsysteem probeert zo efficiënt mogelijk om te gaan met de benodigde opslagruimte voor onder andere bijlagen. Indien meerdere gebruikers dezelfde bijlage(n) ontvangen zal deze slechts eenmaal binnen het systeem worden opgeslagen. In de e-mailberichten staat slechts een verwijzing naar dat ene (fysieke) exemplaar. Dit gebeurt geheel 'onder water', elke eindgebruiker ziet de bijlage(n) gewoon als document in het e-mailbericht staan. Bij het intern doorsturen van een extern e-mailbericht met bijlage(n) zal de omvang van de bijlage in de logbestanden niet meer worden opgeteld bij de grootte van het bericht. Dit is door de commissie geverifieerd in zowel een testomgeving in haar eigen lab, alsook in de Groupwise omgeving van provincie Drenthe.
Daarmee is vastgesteld dat de door KPMG gehanteerde onderzoeksmethodiek nooit heeft kunnen leiden tot de conclusie dat het e-mailbericht van Deloitte niet doorgestuurd kan zijn geweest. Op basis van analyse van *alleen* de e-mail loggegevens kan niet uitgesloten worden dat het bericht is doorgestuurd.

Bij het doorsturen naar een persoon extern zal wel de 9,5 MegaBytes worden vermeld. De commissie heeft de externe mail logbestanden onderzocht naar sporen die er op zouden wijzen dat het bericht na ontvangst op de 10e november 2008 is doorgestuurd naar een externe. Hier zijn geen sporen van aangetroffen.

3.5.4 Delegatie mailbox toegang

Het is mogelijk om in een Groupwise e-mail omgeving andere gebruikers toegang te verlenen tot de eigen mailbox. De aard van toegang kan variëren; bijvoorbeeld toegang tot een agenda, takenlijst of de e-mailberichten. Daarnaast wordt onderscheid gemaakt in lees en/of schrijfrechten. Een gebruiker kan dit zelf instellen vanuit het Groupwise e-mailprogramma.
Het rapport van Deloitte is verzonden naar het e-mailaccount van de secretaresse van de directie. De commissie heeft onderzoek uitgevoerd naar de delegatie instellingen van de mailbox van de secretaresse. Dit onderzoek is uitgevoerd op een restore van de Groupwise e-mail omgeving gedateerd op 14 november 2008.
Hieruit volgt dat op 14 november 2008 alleen de secretaresse van de Commissaris van de Koningin toegang had tot de e-mail omgeving van de secretaresse van de directie. Daarmee is niet zonder meer vastgesteld dat de rechten op 10, 11, 12 en 13 november steeds hetzelfde stonden ingesteld. Het is mogelijk om deze delegatierechten tijdelijk aan te passen en na gebruik weer terug te zetten.

De secretaresse van de directie heeft aangegeven dat zij niet op de hoogte was van het feit dat zij deze andere secretaresse toegang had verleend tot haar mailaccount.
Zij verklaart hierover:

Mevrouw Stijkel: Waren er andere medewerkers die in die week in 2008 toegang hadden tot uw e-mail, hetzij via een machtiging, hetzij via inloggegevens?

De secretaresse: Nee.

Mevrouw Stijkel: Weet u dat heel zeker?

De secretaresse: Ja, volgens mij weet ik dat heel zeker.

Mevrouw Stijkel: Uit ons onderzoek is gebleken dat de secretaresse van de CvdK gemachtigd was voor toegang tot uw e-mail. Daar wist u dus niets van?

De secretaresse: Dat moet ik dan zelf gedaan hebben, mogelijk in de zomer, maar dat wist ik op dat moment niet meer.

Mevrouw Stijkel: Niet in deze periode?

De secretaresse: Nee.

Mevrouw Stijkel: Uit ons onderzoek is gebleken dat het dus wel zo was, dat de secretaresse van de CvdK toegang had. Voor zover wij weten heeft u dit in het vorige interview niet ter sprake gebracht, maar u wist het dus gewoon niet.

De secretaresse: Nee, ik wist het niet.

Mevrouw Stijkel: Is het daarom mogelijk dat zij die week wellicht toch toegang heeft gehad tot uw mailbox en daarin heeft gezocht? Heeft u daarvan iets gemerkt, of heeft u gedacht: "Er is iets bezig?"

De secretaresse: Nee.

De secretaresse van de CvdK stelt eveneens dat zij hiervan niet op de hoogte is geweest.

3.5.5 Onderzoek overname mailbox

Het overnemen (proxy) van een mailbox in een Groupwise wordt wel in het logbestand vermeld. De commissie heeft hier onderzoek naar gedaan om uit te sluiten dat iemand de mailbox van de secretaresse van de directie heeft overgenomen in de genoemde onderzoeksperiode.
Uit dit onderzoek is gebleken dat het zeer onwaarschijnlijk is dat de mailbox van de secretaresse van de directie in de onderzoeksperiode is overgenomen vanuit een ander account.

Uit het onderzoek van de commissie is eveneens gebleken dat het zeer onwaarschijnlijk wordt geacht dat in de genoemde onderzoeksperiode vanaf een andere dan haar eigen werkplek is ingelogd op de mailbox van de secretaresse van de directie.

3.5.6 Conclusies digitaal onderzoek

De commissie heeft geen digitale sporen aangetroffen die inzicht geven in de toedracht van het verstrekken van het onderzoeksrapport van Deloitte aan derden in de genoemde onderzoeksperiode.
De commissie heeft geen digitale sporen aangetroffen die er op wijzen dat de mailbox van de secretaresse van de directie, middels de zogenaamde proxy rechten, door anderen is overgenomen.
De commissie heeft geen digitale sporen aangetroffen dat op de mailbox van de secretaresse van de directie is ingelogd vanaf een andere dan haar eigen werkplek.
Daarbij dient wel opgemerkt te worden dat wanneer het bericht op 10, 11, 12 of 13 november zou zijn doorgestuurd en vervolgens meteen verwijderd is, dat niet zichtbaar zal zijn in de back-up van 14 november 2008. Om die reden kan de commissie niet uitsluiten dat het bericht intern is doorgestuurd.

De commissie constateert dat het digitaal onderzoek uitgevoerd door KPMG initieel beperkt is in scope. De commissie is niet op de hoogte van de overwegingen daarin, maar merkt op dat deze beslissing mogelijk van invloed kan zijn geweest op het eindresultaat. Bij digitaal onderzoek in ICT omgevingen is het van groot belang om snel in kaart te brengen welke systemen mogelijk relevant kunnen zijn voor een onderzoek. Zonder daar meteen onderzoek op te doen, is het altijd raadzaam om deze digitale gegevens preventief veilig te stellen. De praktijk wijst uit dat veel IT systemen in het normale verloop van gebruik gegevens gaan overschrijven.
Ten tijde van het onderzoek van de commissie blijkt onder andere dat meerdere type loggegevens niet meer beschikbaar zijn voor de onderzoekscommissie. Daarnaast zijn de werkplek computersystemen uitgerust met harde schijven met weinig opslagcapaciteit, digitaal sporenmateriaal wordt daardoor sneller overschreven. Ditzelfde geldt voor printserver systemen.

De overweging om alleen de werkplek van de secretaresse van de directie veilig te stellen heeft ook impact op het vervolgonderzoek. De onderzoekscommissie heeft een drietal extra werkplekken veiliggesteld, echter dit heeft pas zes maanden na het uitlekken van het document plaats kunnen vinden. Het kan niet uitgesloten worden dat door het verstrijken van tijd belangrijk digitaal sporenmateriaal is overschreven.

De DS verklaart het volgende over de reikwijdte van het digitale onderzoek van KPMG:

'Ik verwacht van een onafhankelijk bureau dat zij met de onderzoeksvraag in de hand, haar eigen afwegingen maakt hoe het onderzoek uitgevoerd moet worden. Dat hebben zij gedaan, we hebben ook wekelijks contact gehad over de procesgang, of via de telefoon en een keer fysiek. En een keer is het concept eindrapport besproken.'
(...)
'Wij hebben ons gehouden aan de onderzoeksopdracht. Dat waren ook de gesprekken met KPMG. We wilden een lean en mean rapport en in die hoedanigheid heb ik er niet over gesproken. We hebben wel KPMG gevraagd, en dat heb ik ook verteld

in het interview, als wij nader onderzoek zouden doen, zou dan het één en ander dan wel veel duidelijker worden in de uitkomsten van de onderzoeksvraag. Daarbij heeft KPMG aangegeven met betrekking tot IT dat de IT-investeringen waarschijnlijk niet zouden opwegen tegen de baten. En daar hebben wij in het college ook over gesproken en de afweging gemaakt om het bij dit onderzoeksrapport zoals het er nu ligt te laten.'.

(...)

'Ik heb u ook in het interview aangegeven dat als KPMG had gezegd dat ze nog twee of drie computers wilden onderzoeken dan zou dat absoluut geen probleem zijn geweest. Dat is nooit onderwerp van gesprek geweest. En in GS hebben wij gesproken, en volgens mij heeft u die stukken ook, en is op basis van het rapport wat er lag de overweging gemaakt wel of niet doorgaan'.

De voor het KPMG onderzoek verantwoordelijke gedeputeerde mevrouw Klip verklaart hierover:

'Ik denk dat ik niet veel toe te voegen heb aan de verklaring van de directeur zoals ze die in het vorige verhoor gegeven heeft. We hebben de onderzoeksopdracht geformuleerd in het college en vervolgens de suggestie aan KPMG gedaan wie de mensen waren die volgens ons verhoord moesten worden, en dat is gebeurd. Ik weet eerlijk gezegd niet precies, hoe de hele ICT-omgeving door KPMG is onderzocht. U zegt één computer, ik meen mij te herinneren dat in het KPMG-rapport wel staat dat er ook gekeken is of er vanuit welke computer dan ook in ieder geval bestanden zijn verzonden van hetzelfde formaat als het bewuste pdf-bestand. Ik heb zelf de indruk dat er wel iets breder gezocht is dan alleen die ene computer.'

3.6 Bevindingen onderzoek telefoonverkeer

De commissie heeft onderzoek gedaan naar de zogeheten historische telefoongegevens van de bij het Eurochamprapport betrokken ambtenaren en bestuurders. Daarbij is met name onderzocht in hoeverre er telefonisch contact heeft plaatsgevonden tussen journalisten van het Dagblad van het Noorden en ambtenaren en bestuurders van de provincie. De commissie heeft daarbij uitsluitend de uitgaande gesprekken van de mobiele telefoonnummers kunnen onderzoeken, dat wil zeggen de gesprekken waarbij door ambtenaren of bestuurders met hun mobiele telefoon is gebeld en dus niet de telefoontjes die zij hebben ontvangen.
De gegevens van het 'vaste' telefonieverkeer heeft de provincie in een laat stadium aangeleverd en in een formaat dat niet geschikt was voor analyse in het kader van dit onderzoek. Ook langs andere wegen waren de benodigde gegevens niet te achterhalen. Daardoor heeft de commissie deze gegevens niet kunnen onderzoeken/analyseren.

Uit dit onderzoek is vast komen te staan dat er veelvuldig telefonisch contact is geweest tussen de gedeputeerde mevrouw Klip en de heer De Kleine enerzijds en gedeputeerde mevrouw Haarsma en de heer De Bruin anderzijds.
Gedeputeerde mevrouw Klip verklaart over haar (telefonische) contacten met journalisten het volgende:

'Met de heer De Bruin, waar ik zakelijk als statenverslaggever eigenlijk altijd mee te maken heb, los van soms wat andere contacten bij het Dagblad van het Noorden als het hele specifieke onderwerpen betreft, die contacten zijn er. Dat heb ik u, ook qua frequentie, in het interview uitgelegd, dat ligt een beetje aan de politieke actualiteit. Als u doelt op de andere journalist van artikelen over het Deloitte-verhaal, Gerard de Kleine, daar heb ik zeker in die periode heel regelmatig contact mee gehad, maar niet in zijn functie als journalist. Dat waren privé contacten.'

(...)

Dat is zeker in die eerste week niet over dat rapport gegaan, sowieso nooit inhoudelijk over het rapport. Ik sluit niet uit dat in de weken daarna dat wel eens in de slipstream van een gesprek aan de orde is geweest maar nooit inhoudelijk.

(...)

'Ik begrijp dat u daar van opkijkt. Dat zijn privé gesprekken. Ik vind zelfs het feit dat u de frequentie noemt eigenlijk al een privédomein raken. Ik ga daar inhoudelijk niet op in want daarmee raak ik de persoonlijke levenssfeer van iemand anders, dat

ga ik niet doen, ook niet in het onderzoek. Ik kan u wel de context vertellen. Ik ken de heer De Kleine, denk ik, zeven à zevenhalf jaar. In de loop van de laatste paar jaar is daar een vriendschappelijke relatie uit ontstaan. En zoals dat met vriendschap gaat, heb je de ene periode frequenter contact dat de andere periode. Maar nogmaals, misschien ten overvloede, dat had niets met het Deloitte-rapport te maken.'

(...)

'De heer Bomhof: U zegt: het had niets met het Deloitte-rapport te maken maar waar wij hier naar vragen is de voortijdige verspreiding van het Deloitte-rapport. Wij kijken wie dat geweest is en onder welke omstandigheden dat heeft kunnen gebeuren. Nu is het zo dat gesprekken waarover is gerept, u zegt als je alleen al de aantallen noemt beschouwt u dat als een stukje privacy. Het is natuurlijk wel zo dat dat gegevens zijn die in de archieven van de provincie zijn en volledig beschikbaar zijn voor de commissie. Daar kan de commissie ook vragen over stellen. Het is dan over de inhoud verder aan u om te zeggen dat het privé is en het er niet over hebt. Daar treden wij ook niet in, dat moet zeer nadrukkelijk duidelijk worden. Voor zover staat u ook onder ede, dat geen van die gesprekken, en sommige zijn vrij vaak achter elkaar gevoerd, dat geen van die gesprekken te maken heeft gehad met het uitlekken van het rapport dan wel met de omstandigheden waaronder of ander soort wetenschap die een rol kan hebben gespeeld bij het verspreiden van het rapport. Daar zult u dus dan nu duidelijk over moeten zeggen, daar is in geen van die gesprekken sprake van geweest.'

'Mevrouw Klip: Er is in geen van die gesprekken sprake van geweest.'

Mevrouw Haarsma heeft in de betreffende week (10-15 november 2008) in ieder geval vijf keer contact opgenomen met de heer De Bruin. De commissie sluit echter niet uit dat er meerdere gesprekken zijn geweest, aangezien mevrouw Haarsma heeft verklaard dat zij een aantal keren contact heeft opgenomen met de heer De Bruin op bepaalde momenten, terwijl dit niet is gebleken uit de gegevens die de commissie tot haar beschikking heeft.
Mevrouw Haarsma verklaart zelf het volgende over haar telefonische contacten:

'Ik heb al gezegd dat het van de politieke actualiteit afhangt. Ik heb net ook uitgelegd waarom ik op bepaalde momenten met de heer De Bruin heb gebeld. Het heeft dus inderdaad daarmee te maken.'

(...)

'...De ene week kan het tig keer zijn en daarna kan het wel twee weken helemaal nooit zijn.'

Uit onderzoek van de commissie is niet gebleken dat er veel contacten zijn geweest tussen ambtenaren en journalisten van het Dagblad van het Noorden. De commissie heeft slechts één gesprek tussen de communicatieadviseur van mevrouw Haarsma en de heer De Bruin kunnen vaststellen. De commissie sluit echter niet uit dat er meerdere gesprekken zijn geweest, aangezien de adviseur heeft verklaard dat hij een aantal keren contact heeft opgenomen met de heer De Bruin op bepaalde momenten, terwijl dat niet is gebleken uit de gegevens die de commissie tot haar beschikking heeft.

De commissie heeft onderzoek gedaan om te bepalen of in het telefoonverkeer sprake is geweest van een patroon. Zij heeft geconstateerd dat dit voor beide gedeputeerden het geval is, zij het dat mevrouw Haarsma in de week voorafgaand aan het verschijnen van het definitieve rapport geen contacten had met Martin de Bruin. De gesprekken van mevrouw Klip met Gerard de Kleine liggen in die periode per week ongeveer op hetzelfde niveau. In geen van de bekeken weken heeft een significant hoger aantal telefoongesprekken plaatsgevonden met één van de twee journalisten.

3.7 Beantwoording eerste onderzoeksvraag

De eerste onderzoeksvraag betreft de vraag wie verantwoordelijk is voor de voortijdige verspreiding van het rapport van Deloitte inzake Eurochamp en op welke wijze dat is geschied.

De commissie acht het aannemelijk dat de digitale versie van het definitieve Eurochamprapport in de week van 10-15 november 2008 voortijdig vanuit het provinciehuis naar buiten is gebracht en in handen is gekomen van het Dagblad van het Noorden, al dan niet direct of indirect via een tussenpersoon. De commissie heeft niet kunnen vaststellen op welke wijze en in welke vorm het voortijdig is verspreid en door wie.
Daarmee kan niet worden vastgesteld wie er verantwoordelijk is voor de voortijdige verspreiding van het Eurochamprapport. Dit laat onverlet de bestuurlijke verantwoordelijkheid van het college van Gedeputeerde Staten.
De mogelijkheid dat het rapport vanuit Deloitte verzonden is aan mensen buiten het provinciehuis, is volgens de commissie niet meer dan een theoretische mogelijkheid. KPMG heeft hiernaar specifiek onderzoek gedaan en zij hebben daar geen aanwijzingen voor gevonden. Deloitte heeft geen medewerking aan het onderzoek van de onderzoekscommissie verleend, met als reden dat zij alle relevante inlichtingen reeds aan KPMG hadden verstrekt.

De commissie baseert haar antwoord op de eerste onderzoeksvraag op de volgende bevindingen:

a. De inzage die de commissie heeft gehad in het exemplaar van het rapport dat via de informant in handen is gekomen van de heer Klaver. De commissie heeft daarbij vastgesteld dat het hierbij gaat om een uitgeprinte versie van het digitaal verzonden definitieve rapport;
b. De door de informant afgelegde verklaringen tegenover KPMG, welke door KPMG als betrouwbaar zijn bestempeld, maar niet door de commissie konden worden geverifieerd;
c. De verklaring van de informant dat het Dagblad van het Noorden op 13 november 2008 in het bezit is van het Eurochamprapport, blijkens het KPMG-rapport;
d. Het hoofdredactioneel commentaar van 29 november 2008, waarin de hoofdredacteur schrijft dat de krant de hand op het rapport had weten te leggen. De hoofdredacteur stelt daarnaast tevens dat de krant zijn bron in geen geval zal onthullen en dat de bron heilig is. De commissie vraagt zich overigens af hoe zich dit verhoudt tot de verklaringen van de heer De Bruin tegenover de provincie (mevrouw Haarsma en haar communicatieadviseur) en tegenover KPMG dat hij bij advocaat Van Luyn inzage heeft gehad in het Eurochamprapport. Op 19 juni 2009 schrijft de krant zelfs openlijk dat de heer De Bruin inzage heeft gehad bij de heer Van Luyn;
e. Uit het onderzoek volgt dat advocaat Van Luyn tot 27 november 2008 niet de beschikking had over een definitieve versie van het rapport;
f. De uitgelekte email die binnen het Dagblad van het Noorden is verstuurd door de chef redactie Drenthe aan de hoofdredactie (in cc aan de heer De Bruin en de heer De Kleine) en waarin wordt gesteld dat het goede antwoord op de vraag wie er heeft gelekt tot politieke beroering en wellicht gevolgen zal leiden.

4 De tweede onderzoeksvraag: Organisatorische en/of 'bestuurlijk-culturele' factoren

4.1 Inleiding

De tweede onderzoeksvraag van de commissie luidt:
Waren er bij de provincie Drenthe organisatorische en/of 'bestuurlijk-culturele' factoren die de voortijdige verspreiding hebben bevorderd?

Onder bestuurlijke cultuur verstaat de commissie de bestaande manieren van denken en doen in het bestuur van een organisatie.[8] Daarbij gaat het zowel om de wijze waarop bestuurders zich in een organisatie gedragen, als om de waarden en normen, ideeën en opvattingen, sentimenten en emoties die aan dat gedrag ten grondslag liggen.

Uit het onderzoek van de commissie is een aantal organisatorische en/of bestuurlijk-culturele factoren naar voren gekomen die naar de mening van de commissie een rol kunnen hebben gespeeld in de voortijdige verspreiding van het Deloitte rapport. Deze factoren worden in de navolgende paragrafen besproken.

4.2 Aard en frequentie van contacten met media

Zoals reeds in het vorige hoofdstuk naar voren is gekomen, bestaan er intensieve contacten tussen bestuurders van de provincie en journalisten van het Dagblad van het Noorden. Dit betreffen niet alleen zakelijke, maar ook vriendschappelijke contacten.
Gedeputeerde mevrouw Klip heeft aangegeven dat haar frequente telefonische contacten met de heer De Kleine - die zowel tijdens als buiten kantoortijden plaatsvinden - uitsluitend een privé karakter hebben en dat zij daarom hierover verder niets wenst te verklaren. In het vorige hoofdstuk is haar verklaring hieromtrent al belicht.

Het contact tussen gedeputeerde mevrouw Haarsma en de heer De Bruin kent volgens mevrouw Haarsma een zakelijk karakter.
Mevrouw Haarsma heeft aangegeven dat zij regelmatig telefonisch contact heeft met de heer De Bruin. Uit onderzoek van de commissie is gebleken dat deze contacten zowel tijdens als buiten kantoortijden plaatsvinden. Daarbij belt zij de journalist zowel op zijn mobiele telefoonnummer als op zijn huisnummer. Het betreft hier overigens geen eenrichtingsverkeer. Mevrouw Haarsma wordt naar eigen zeggen zelf ook met enige regelmaat gebeld door de heer De Bruin.

Uit onderzoek van de commissie is gebleken dat de communicatieadviseur van mevrouw Haarsma slechts in beperkte mate als intermediair in dit contact optreedt en dat hij kennelijk niet op de hoogte is van de frequentie van die contacten. Dit getuige het volgende fragment uit de hoorzitting met de communicatieadviseur:

---

[8] Gebaseerd op het begrip organisatiecultuur zoals omschreven in Openbaar bestuur, Beleid, organisatie en politiek, U. Rosenthal en anderen, 1996, blz. 164.

'De heer De Jong: Een andere vraag is of mevrouw Haarsma regelmatig contact heeft met de heer De Bruin en andere journalisten.

De communicatieadviseur: Er is zo nu en dan contact met een journalist. Met meerdere.

De heer De Jong: Zou u iets specifieker kunnen zijn over de frequentie van die contacten?

De communicatieadviseur: Het gebeurt in de regel weinig, maar zo nu en dan gebeurt het wel. Laat het eens in de maand zijn? Of eens in de twee maanden? Ik weet het niet precies. Zoiets.

De heer De Jong: Was er naar uw weten rechtstreeks contact tussen de journalist en mevrouw Haarsma?

De communicatieadviseur: Ja, om een voorbeeld te geven. Vorige week stond er een stuk in de krant over het sportgala dat Drenthe en Groningen mogelijk samen doen. Anneke Haarsma heeft verteld dat zij daarover rechtstreeks door een journalist was benaderd en op vragen daarover ook antwoord heeft gegeven. Dat gebeurt dus zo nu en dan.

De heer Bomhof: Nu gaat het over de periode van 10 november 2009 en de dagen daarna. Dan is het ook zo dat Anneke Haarsma weinig contact heeft gehad met journalisten en dat het dan vooral uw rol is geweest om als communicatiedeskundige die contacten te leggen?

De communicatieadviseur: Dat klopt. Op de tapasavond is er contact geweest en verder weet ik niets van contacten tussen bestuurders en journalisten.

De heer Bomhof: Ik begrijp ook dat mevrouw Haarsma daarbij contact heeft gehad, maar u bent haar communicatieadviseur en ik begrijp ook dat er regelmatig overleg is geweest tussen jullie beiden over de contacten van u zelf en mevrouw Haarsma met journalisten en de afspraken die er met hen werden gemaakt. Hadden jullie over en weer vrij goed zicht op het contact dat jullie hadden met journalisten?

De communicatieadviseur: Ja.

De heer Bomhof: Wat u in dat verband over mevrouw Haarsma zegt, is dat met grote mate van zekerheid juist?

De communicatieadviseur: Ik kan alleen maar zeggen wat ik heb meegemaakt en daarbij staat mij, behalve op die avond, niet voor de geest dat er op andere momenten ook contact is geweest.'

Het Eurochamprapport betrof een vertrouwelijk rapport. In de week van 10-15 november 2008, maar ook in de weken daaromheen, is er intensief contact geweest tussen bestuurders en journalisten van het Dagblad van het Noorden. De commissie meent dat hiermee de schijn is gewekt dat er over dit vertrouwelijke rapport zou kunnen zijn gesproken en dat er mogelijk inzage in het rapport heeft kunnen plaatsvinden. Het interview op 13 november 2008 en de citaten van mevrouw Haarsma in artikelen van de krant in de betreffende week, zoals besproken in het vorige hoofdstuk, versterken deze schijn.

De aard en frequentie van het contact met de media is volgens de commissie daarmee een bestuurlijk-culturele factor die het risico van verspreiding van vertrouwelijke informatie vergroot.

Naast telefonische contacten met bestuurders en/of ambtenaren van de provincie, is de journalist de heer De Bruin ook regelmatig op het provinciehuis te vinden. Gezien zijn functie van Statenverslaggever is dit geen bijzonder gegeven. De commissie vindt het wel opmerkelijk dat de heer De Bruin de beschikking heeft

over een vaste toegangspas voor het provinciehuis. De heer De Bruin kan zich daardoor, tijdens kantoortijden, vrijelijk binnen het provinciehuis begeven en desgewenst met iedereen het gesprek aangaan of op enigerlei wijze informatie tot zich nemen, zonder dat iemand daar mogelijk op toeziet. De commissie ziet dit als een organisatorische factor die de voortijdige verspreiding van het rapport heeft kunnen bevorderen.

4.3 Beeldvorming in de media

In het vorige hoofdstuk is de oplegnotitie aan de orde gekomen die is besproken tijdens de GS vergadering van 11 november 2008. In deze notitie wordt gesproken over het risico van negatieve beeldvorming. Concreet wordt daarbij opgemerkt dat het Eurochamprapport bepaalde beweringen over de rol van de provincie zou kunnen weerleggen.

Diverse bij het dossier betrokken personen hebben tegenover de commissie verklaard dat er in de betreffende week een aantal berichten in de media verschenen, waarbij de rol van de provincie 'ten onrechte' negatief werd belicht. Zo verklaart de communicatieadviseur van mevrouw Haarsma:

'Op de 12e 's avonds hebben wij het er even over gehad en op 13 november heb ik 's ochtends contact gehad met Anneke Haarsma. Toen hebben wij gezegd dat wij met Martin de Bruin moesten gaan praten, want op dat moment werden bij de omroep en bij de krant allerlei verhalen gepresenteerd over de manier waarop de provincie een dubieuze rol zou hebben gespeeld bij de aanbesteding. Voor mij was dat het belangrijkste argument om een gesprek met de journalist aan te gaan.'
(...)
'Ik heb zonet al aangegeven dat het verhaal over de aanbesteding iets was waarvan mevrouw Haarsma en ik vonden dat er iets mee moest worden gedaan.'

Mevrouw Haarsma zegt hierover:

'Er werd in de media behoorlijk over het aanbestedingsbeleid van de provincie gesproken en wij hadden de behoefte om uit te leggen hoe dat in elkaar stak.'

Mevrouw Smith: Hoe wat in elkaar stak?

Mevrouw Haarsma: Dat het natuurlijk niet alleen om het aanbestedingsbeleid ging, maar met name om de inhoud van het rapport, en dat het aanbestedingsbeleid niet de hoofdmoot was van het rapport. Het ging om een andere zaak.'

In de Statenvergadering van 18 maart 2009 heeft mevrouw Haarsma, blijkens het verslag hiervan, hierover het volgende opgemerkt:

'Het volgende punt dat ik wil bespreken is de verwevenheid. De heer Klaver heeft gevraagd hoe het in dit huis met die verwevenheid zit. Net als hij vinden wij het belangrijk ons product goed te verkopen en wij – en ik spreek expres in de wij-vorm – vinden dat wij op een correcte en integere manier met de pers omgaan. Dat is het waardeoordeel dat ik namens het college kan geven.
Ik kom op 13 november, de datum waarop ik in aanwezigheid van mijn bestuursadviseur een gesprek heb gehad met de journalist. Er is toen uitvoerig gesproken over het feit dat mij was opgevallen dat het eigenlijk alleen nog maar over de aanbestedingsregels ging en niet meer over waarvoor het onderzoek was gestart, namelijk de vraag wat er onrechtmatig was gebeurd. Het was niet zo dat wij de aanbestedingsregels onbelangrijk vonden, integendeel, maar de kern waarop het onderzoek zich diende te richten waren de handelingen die in onze optiek niet door de beugel konden. Dat heb ik met de pers besproken, niet meer en niet minder en dat gesprek heeft pakweg drie kwartier geduurd.'
(...)

'Dat is heel simpel. Ik heb net al gezegd dat ik met de communicatieadviseur had besproken dat de zaak wel een gekke wending nam, omdat het bericht alleen ging over de aanbesteding, terwijl het volgens ons ook om heel andere zaken ging. Wij besloten een afspraak met het Dagblad van het Noorden te maken om ook die kant van de medaille te laten zien.'

De beleidsmedewerker Sport die de oplegnotitie voor de vergadering van GS van 11 november 2008 heeft geschreven, heeft desgevraagd over de beeldvorming het volgende aan de commissie verklaard (zijn verklaring ter zake is reeds in hoofdstuk 3 vermeld. Vanwege het belang in relatie tot het onderwerp van deze paragraaf nemen wij het volledigheidshalve ook hier op):

'Eurochamp is vanaf het begin af aan een organisatie geweest, die door heel veel mensen als positief werd gezien. Toen bij ons de mogelijke misstanden werden gemeld en wij het voornemen kenbaar hadden gemaakt de subsidie stop te zetten, was de reactie van de buitenwereld er een van: hoe kan je dat nu doen, want het is zo'n goede organisatie.
De beeldvorming zou daarom kunnen ontstaan dat wij heel snel subsidies zomaar stopzetten met de kans dat een organisatie failliet gaat. Zou dit gebeuren dan zou, als wij geen goede argumenten hadden waarom wij de subsidie hadden stopgezet, de schuld bij de provincie worden gelegd. Dat was de achterliggende gedachte van de paragraaf risico's beeldvorming. Daarnaast was er nog het feit dat de advocaat de heer Van Luyn de eerste week van november een persbericht had verspreid waarin werd gesteld dat de rapportage van Deloitte de heer Leijssenaar vrijpleitte. Daarbij heeft hij quotes uit de rapportage naar voren gehaald, waarin met name werd gezinspeeld op de betrokkenheid van onze bestuurders bij aanbestedingen die mogelijk niet conform de regels zouden zijn.
Maar wij hadden ook een rapport en uit dat rapport blijkt iets anders.
Met het oog op die twee aspecten: negatieve beeldvorming en de al in de media circulerende gedachte dat de provincie ook enige schuld had, is de risicoparagraaf geschreven.

De heer Beerda: Dat betekent dat de provincie uit een oogpunt van mediastrategie op dat moment ook belang had bij het rapport.

De beleidsmedewerker Sport: Ja.

De heer Beerda: En ook bij het wereldkundig maken van het rapport.

De beleidsmedewerker Sport: Wij hebben uitvoerig overleg met Deloitte gehad over de vraag welke gegevens wij zouden mogen gebruiken en welke niet. Het was immers een vertrouwelijk rapport, ook vertrouwelijk voor ons. Die afspraak was gemaakt toen Deloitte het onderzoek ging starten. Er gelden gewoon bepaalde normen als je een forensisch accountantsonderzoek laat doen.
Er zat dus wel enige spanning tussen wat wij wel en wat wij niet zouden mogen vertellen, maar wij hebben altijd heel zorgvuldig met onze juristen bekeken wat wij wel zouden mogen vertellen. Wij hebben Deloitte ook gevraagd om een openbare samenvatting te schrijven omdat wij het rapport niet konden en niet wilden openbaar maken. Pas later werd het rapport wel openbaar.'

De commissie meent dat uit bovenstaande naar voren komt dat de provincie een mogelijk belang had bij openbaarmaking van de inhoud van het rapport, omdat dit de beeldvorming over de rol van de provincie in de kwestie ten positieve zou kunnen beïnvloeden. De gedeputeerde spreekt dienaangaande over een product dat goed moest worden verkocht.
De in de ogen van de commissie nogal geforceerd overkomende drive om de beeldvorming in de media te beïnvloeden, is daarmee naar de mening van de commissie een bestuurlijk-culturele factor die het risico van een voortijdige verspreiding van het rapport heeft verhoogd.

4.4 Niet-naleving informatiebeveiligingsbeleid

In het Beleidskader informatiebeveiliging provincie Drenthe (februari 2009) staat dat informatie een bedrijfsmiddel is dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor de organisatie en voortdurend op een passende manier beveiligd dient te zijn. Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden of in gesproken vorm). Welke vorm de informatie ook heeft of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn.

In het Handboek Informatiebeveiliging, dat dateert uit 2005, wordt het beleid rondom het gebruik van e-mail beschreven. Hier wordt onder meer gesteld dat het niet toegestaan is om vertrouwelijke informatie te verzenden via de e-mail. Daarbij moet worden aangetekend dat er niet wordt gesproken over de ontvangst van vertrouwelijke informatie via de email.
Daarnaast wordt gesteld dat de provincie de e-mail alleen voor informele communicatie mag gebruiken.

De commissie wil op voorhand opmerken dat hetgeen hierboven over het gebruik van e-mail is genoemd en is vastgelegd in het beleidskader, anno 2009 een zeer rigide benadering betreft en naar de mening van de commissie een efficiënte manier van communicatie bemoeilijkt. Om die reden mag verwacht worden dat hier pragmatisch mee omgegaan zal worden en dat handhaving van het voorschrift niet zal plaatsvinden.
Uit het onderzoek van KPMG en dat van de commissie is vast komen te staan dat het de digitale versie van het definitieve Eurochamprapport betreft, die uiteindelijk in handen is gekomen van het Dagblad van het Noorden.
Dit rapport is op 10 november 2008 door Deloitte per email aan de secretaresse van de directie van de provincie verstuurd. Dit is gebeurd op eigen initiatief van deze secretaresse. Zij had daarover geen overleg gepleegd met de directie of hiervoor toestemming gevraagd (zie ook hoofdstuk 3). Het rapport is vervolgens onbeveiligd (zonder wachtwoord) per email aan haar verzonden.
Strikt formeel gezien had de secretaresse een dergelijk verzoek dus niet mogen doen, omdat daardoor de email voor formele communicatie werd gebruikt. De DpS was op de hoogte van de digitale ontvangst van het rapport. Ze heeft daar de secretaresse niet op aangesproken. Naar de mening van de commissie had de DpS opdracht kunnen geven om de email te verwijderen, temeer daar zij op dat moment al wist dat deze versie niet meer gebruikt zou worden.
Overigens heeft de DpS een week later de digitale versie van het definitieve rapport toch gebruikt en deze via de email onbeveiligd doorgestuurd aan de landsadvocaat. Dat is naar de mening van de commissie ook formeel gezien in strijd geweest met bovenstaande regelgeving, omdat hierdoor de email weer werd gebruikt voor formele communicatie en niet passend was beveiligd.
Nog kan worden opgemerkt dat ook het conceptrapport van Deloitte d.d. 3 november 2008 per email en onbeveiligd door Deloitte aan de DpS is verzonden. Hierbij is dus ook formeel gezien in strijd met de eigen regelgeving gehandeld.

Uit het (digitale) onderzoek van de commissie is niet duidelijk geworden wat er precies met de digitale definitieve versie van het rapport is gebeurd. Wel is dus vast komen te staan dat deze versie uiteindelijk bij het Dagblad van het Noorden is beland. Doordat het betreffende bestand niet passend was beveiligd met een wachtwoord, via de email is verzonden en niet werd beheerd door een bij het dossier/rapport betrokken ambtenaar of bestuurder, heeft naar de mening van de commissie geen controle over de digitale versie plaatsgevonden.
De commissie vindt dat het rapport niet naar de secretaresse van de directie verstuurd had mogen worden, maar uitsluitend naar een voor het rapport verantwoordelijke ambtenaar of bestuurder. De provincie had dit

kenbaar moeten maken aan Deloitte, maar heeft dat nagelaten. De DpS heeft ook niet ingegrepen toen zij op de hoogte was van het bestaan van deze niet-passend beveiligde versie.
De provincie, i.c. de betrokken medewerkers hebben daardoor gehandeld in strijd met het eigen informatiebeveiligingsbeleid.

De niet- naleving van het informatiebeleid door medewerkers van de provincie is daarmee een organisatorische factor die de voortijdige verspreiding van het rapport heeft kunnen bevorderen.

4.5 Beantwoording tweede onderzoeksvraag

De tweede onderzoeksvraag betreft de vraag of bij de provincie Drenthe organisatorische en/of 'bestuurlijk-culturele' factoren de voortijdige verspreiding hebben bevorderd.

De commissie is van mening dat een viertal organisatorische en bestuurlijk-culturele factoren de voortijdige verspreiding van het rapport hebben kunnen bevorderen dan wel het risico daarvan hebben vergroot.

Deze factoren betreffen:

1. De aard, frequentie en intensiteit van contacten met de media;
2. De naar het oordeel van de commissie geforceerd overkomende drive om de beeldvorming in de media te beïnvloeden;
3. Het in het bezit zijn van journalisten van een vaste toegangspas voor het provinciehuis;
4. Het op onderdelen niet naleven van het informatiebeveiligingsbeleid.

De commissie baseert zich daarbij onder meer op de volgende bevindingen:

a. Het veelvuldige contact tussen bestuurders van de provincie en journalisten van het Dagblad van het Noorden en de daarover afgelegde verklaringen;
b. De aard van de contacten tussen bestuurders van de provincie en journalisten van het Dagblad van het Noorden en de hierover afgelegde verklaringen;
c. Het in het bezit zijn van de journalist de heer De Bruin van een eigen toegangspas voor het provinciehuis;
d. Het interviewgesprek van mevrouw Haarsma op 13 november 2008 met de heer De Bruin en de hieraan ten grondslag liggende motieven om dit gesprek aan te gaan;
e. De citaten van mevrouw Haarsma in artikelen van het Dagblad van het Noorden in de week van 10-15 november 2008, waarbij zij kennelijk heeft gerefereerd aan de inhoud van het Deloitte rapport;
f. Het onderkende risico van de negatieve beeldvorming zoals dat is verwoord in de oplegnotitie die besproken is in de GS vergadering van 11 november 2008;
g. De wijze van verzending van de digitale versies van de Deloitte rapporten.

5 De derde onderzoeksvraag: Aanpassing gevoerd bestuur

5.1 Inleiding

De derde en laatste onderzoeksvraag van de commissie luidt:

In hoeverre moet het gevoerde bestuur worden aangepast om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen.

In het kader van deze onderzoeksvraag, zal in dit hoofdstuk specifiek worden stilgestaan bij het integriteitbeleid, het informatie- en informatiebeveiligingsbeleid en het mediabeleid in zijn algemeenheid.

5.2 Integriteit- en informatie(beveiligings)beleid

Uit onderzoek van de commissie is gebleken dat de provincie een actief integriteitbeleid voert. De commissie heeft kennisgenomen van relevante documenten terzake. Een aantal van die documenten is in hoofdstuk 2 besproken.
In de hoorzittingen is door de verantwoordelijke bestuurders en directieleden over het integriteitbeleid het volgende opgemerkt:

'De heer Bomhof: Een andere vraag gaat over integriteit. Hoe wordt in de ambtelijke organisatie vorm en inhoud gegeven aan het integriteitbeleid? Daar zijn niet alleen nota's over verschenen. Wordt erover gesproken in werkoverleggen en worden dan bepaalde casussen doorgenomen? Worden ambtenaren er in actieve zin mee geconfronteerd wat in het kader van integriteit nuttig en noodzakelijk is? Hoe werkt dat binnen de provincie?

De DpS: In landelijk verband is de eed of belofte voor de provinciaal ambtenaar ingevoerd. Tijdens introductiebijeenkomsten is toen heel uitvoerig en nadrukkelijk aandacht besteed aan het begrip integriteit, waarbij casussen met behulp van acteurs worden nagespeeld. Daarna heeft iedere provinciale ambtenaar de eed of belofte afgelegd. Nu is het zo dat alle nieuwe medewerkers ook naar introductiebijeenkomsten gaan en prominent onderdeel van die bijeenkomsten is het integriteitbeleid. Daar wordt uitgebreid over voorgelicht. Bij die introductiebijeenkomsten ben ik als één van de directieleden persoonlijk aanwezig. Daar worden dan ook stellingen behandeld, want integriteit is niet heel zwart-wit. Van bepaalde dingen weet je heel goed wat wel of niet kan, maar er is ook een groot grijs gebied. Daar worden discussies met nieuwe medewerkers over gevoerd, zodat zij zich hiervan bewust worden. Ook dienen die bijeenkomsten ertoe dat nieuwe medewerkers zich ervan bewust worden dat de provincie een politiek-bestuurlijke organisatie is en dat zij zich daarvan rekenschap moeten geven. Er wordt gevraagd de eed of belofte af te leggen. Dat doen wij op een heel formele manier, om nogmaals te benadrukken dat dit een grote betekenis heeft. In die zin is er bij de start van de medewerkers nadrukkelijk aandacht voor integriteit. Daarnaast zijn er nog heel veel andere zaken, zoals een aantal cursussen over bestuurlijk-ambtelijk samenspel, waarin dit thema ook expliciet aan de orde komt. Er is nu een nieuwe cursus ontwikkeld voor projectleiders over hoe zij daarmee omgaan. Op vele plekken besteden wij daar aandacht aan. Op het intranet staat ook een handboek voor de medewerker waar in begrijpelijk taal dergelijke zaken worden uitgelegd. Ook in werk- en teamoverleggen wordt hierover gesproken.'

De voor het integriteitbeleid verantwoordelijke portefeuillehouder Mevrouw Klip merkt hierover tijdens de hoorzittingen het volgende op:

'(...)Er is inderdaad gekeken van wat wij op dat terrein doen. Los van het feit dat we een, onparlementair gezegd, het boodschappenlijstje van alle punten waarvan Binnenlandse Zaken zegt die moet je implementeren hebben we dat op twee punten na gedaan. We scoren ook onverminderd hoog bij Binnenlandse Zaken wanneer die aspecten gemonitord worden èn toen we gestart zijn met de hele nieuwe werkwijze van Binnenlandse Zaken en dus ook massaal de toen werkzame ambtenaren in dit huis de eed of belofte moesten afleggen, hebben we dat heel zorgvuldig en grootscheeps aangepakt, zoals

ook vanmorgen is opgemerkt. Echt met acteurs die in deze zaal iedere keer met kleine groepjes ambtenaren rollenspelen hebben gedaan, waar steeds met een fase verschil wat in de besluitvorming, een soort van 'achterkant van het gelijkachtige' middagen. Op dezelfde manier, vergelijkbaar maar zonder acteurs gebeurt dat nu weer wanneer ambtenaren in dienst treden. De DpS besteedt daar een dagdeel aan, dan komt ook dat aspect, wat is nou integriteit en hoe geef je dat nu vorm, aan de orde. Aan de andere kant hebben we ook daarnaast naar aanleiding van de recente gebeurtenissen rondom het Eurochamprapport geïnventariseerd, is de directie geïnventariseerd, wat doen de teamleiders aan integriteitbeleid binnen hun team en dat heeft, ik heb het zelf nog niet gezien maar er al wel over gehoord, indrukkende lijst opgeleverd van hoe teamleiders met hun personeel omgaan en daarbij ook integriteitkwesties aan de orde stellen op dat specifieke team of de inhoud van het werk van dat team van toepassing is.'

De directeur-secretaris van de provincie is tevreden over het integriteitbeleid dat binnen de provincie wordt gevoerd:

'(...) We zijn heel erg aan het inzetten op integriteit, dat doen we al jaren. We hebben ook een veilige organisatie, we zijn geen integriteitschendingen gemeld, niet vanuit de bedrijfsarts en niet vanuit de vertrouwenspersoon. Dit is een hele veilige plezierige organisatie voor medewerkers om in te werken.

Mevrouw Smith: en daar bent u als eindverantwoordelijke tevreden over?

De DS: tevreden en gepast trots.

Mevrouw Smith: wordt er verder nog in werkoverleggen en dergelijke er zeer regelmatig aandacht besteed aan integriteit, vertrouwelijkheid et cetera heeft u daar enig zicht op of spreekt u uw managers aan om daar regelmatig aandacht aan te besteden?

De DS: beide, ik spreek ze er op aan en ze doen het ook uit zichzelf van uit hun eigen verantwoordelijkheid om dit te doen. Dat wordt zeer regelmatig gedaan.'

Een bij het dossier betrokken ambtenaar verklaart tijdens de hoorzitting over het integriteitbeleid als volgt:

'Ik ken het beleid. Ik heb zelf ook de eed afgelegd en bij het afleggen van de eed hebben we ook de nodige voorlichting gehad over de positie van de ambtenaar. Dus ja, ik ken het beleid'.
(...)
Het is niet zo vaak aan de orde geweest. Bij mij op de afdeling is het pas heel erg gaan spelen in de periode dat er twijfels gingen ontstaan over het voortijdig verspreiden van het rapport. Toen is in ieder geval door de directie maar ook door het management van de afdeling het belang van het goed omgaan met vertrouwelijke informatie nog eens goed benadrukt. Voor die periode gebeurde het zo nu en dan. Het was niet een terugkerend onderwerp.'

Een andere ambtenaar verklaart in de hoorzitting dat hij bekend is met de regels over integriteit:.

'De ambtenaar: Ja, in grote lijnen wel. Op Huisnet, ons intranetsysteem, staat daar informatie over en verder hebben wij, zoals gezegd, de ambtseed afgelegd. Daarnaast denk ik ook dat je als individuele ambtenaar een eigen verantwoordelijkheid en professionaliteit hebt die ook bij je werk hoort.'

Naast het integriteitbeleid kent de provincie ook een informatie- en informatiebeveiligingsbeleid dat hier nauw mee samenhangt. De commissie heeft kennis genomen van de relevante documenten en hierbij stilgestaan tijdens de voorgesprekken en hoorzittingen.

De DpS verklaart hierover:

'Beveiliging, veiligheid en integriteit hangen nauw met elkaar samen. Bij beveiliging ga je zorgen dat je allerlei maatregelen neemt, zodat er een veilige werkomgeving is en informatie beveiligd wordt. Ik denk dat u al heel veel informatie hebt gekregen over wat wij daaraan doen. Dat wordt dus in de slipstream van het praten over integriteit meegenomen en in bepaalde gevallen wordt er heel expliciet instructie over gegeven en aandacht aan gegeven en ook bij de introductie van nieuwe medewerkers op hun werkplek is dit een punt wat meegenomen wordt.
(...)
Wederom noemt u heel veel zaken die u waarschijnlijk in bepaalde gevallen hebt gezien. Je moet beveiligingsbeleid voortdurend evalueren en dat gebeurt regelmatig door nieuwe beleidskaders en regels te stellen, maar door de snelheid waarmee de ICT zich ontwikkelt vraagt dat altijd weer om vernieuwing. Wij hebben in 2008 een nieuw beleidskader laten opstellen en op dit moment loopt er een quick scan van die maatregelen, waarbij wordt gekeken wat wij nu goed voor elkaar hebben en wat niet. Die quick scan loopt al een poosje en daar komen straks de uitkomsten van binnen, evenals wat de provincie daarmee moet. Wij hebben ook al geconstateerd en opdracht gegeven om meer aandacht te geven aan maatregelen die meer in de fysieke – en de ICT-sector zitten en er komt een voorlichtingscampagne voor de medewerkers om zich daar meer bewust van te maken. Het is begrijpelijk dat je dat niet dagelijks, maar periodiek doet. Al die zaken lopen al lang.'

Ook tijdens de hoorzitting met de DS van de provincie komt het onderwerp ter sprake:

'Mevrouw Smith: Er is een beleidskader informatiebeveiliging van de provincie Drenthe van februari van dit jaar. Hoe is dit beleidskader geïmplementeerd, en welke kaders waren daar voorheen?

De DS: Wij zitten in een organisatieontwikkeling zoals u hebt gemerkt. Dat betekent dat de IT voortdurend aan verandering onderhevig is. En de directie samen met de afdeling Facilitaire ondersteuning heeft vorig jaar dit onderwerp voortvarend ter harte genomen en dit heeft geresulteerd in een beleidskader begin jaar en dat wordt nu verder uitgewerkt.

Mevrouw Smith:Een hoe wordt dit nu verder uitgewerkt?

De DS: Dat wordt verder uitgewerkt in een handboek en een aantal normen. En de DpS heeft vanochtend ook aangegeven dat er nog een quick scan wordt uitgevoerd en de uitkomsten met elkaar samen leiden tot een aantal maatregelen.

Mevrouw Smith: Weet u wanneer die maatregelen geïmplementeerd zullen gaan worden?

De DS: dat zal in de loop van het jaar gedaan worden.'

De verantwoordelijk portefeuillehouder voor het informatie- en informatiebeveiligingsbeleid heeft zich tijdens de Statenvergadering van 18 maart 2009, blijkens het verslag, uitgebreid uitgelaten over het beleid dienaangaand:

'Mijnheer de voorzitter. Ik wil nog graag een aantal aanvullende opmerkingen maken, die betrekking hebben op het door ons gevoerd informatiebeleid, ook in relatie tot de zaak die vanmiddag zo nadrukkelijk speelt. Daarbij wil ik ook van mijn kant nog eens benadrukken – het wordt bijna saai – dat ook informatiebeveiliging valt of staat met de zorgvuldigheid en integriteit waarmee iedereen in deze organisatie daarmee omgaat. Er kunnen nog zoveel voorschriften, maatregelen, protocollen en procedures gemaakt worden, als er niet op een goede manier invulling aan wordt gegeven, is het risico dat er dingen fout lopen, altijd aanwezig. Ook dit is mensenwerk en fouten zijn nooit en in geen enkele organisatie uit te sluiten. Dit is uiteraard geen excuus dat het is voorgevallen; het is ernstig genoeg dat het is gebeurd en dat dit nu zoveel van onze tijd kost.
De huidige maatregelen die binnen de provincie Drenthe gelden met betrekking tot de informatiebeveiliging zijn vastgelegd in ons Handboek informatiebeveiliging. Dit handboek is gebaseerd op de binnen de gehele overheid geldende code voor informatiebeveiliging. Die code dateert uit de jaren tachtig/negentig van de vorige eeuw en die geldt binnen de rijksoverheid en

de provinciale en gemeentelijke overheden als basis voor alles wat op het gebied van informatiebeveiliging in dit land moet worden gedaan. Binnen de provincie is dat verankerd in het Informatiestatuut.
Het Handboek informatiebeveiliging schrijft voor de informatiebeveiliging multidisciplinair te benaderen en integraal in de organisatie te beleggen in termen van verantwoordelijkheden. Dat wordt nader uitgewerkt in concrete maatregelen, gerubriceerd op onderwerp. De relevante onderwerpen op het gebied van toegang tot en verspreiding van informatie zijn als volgt in dat handboek vastgelegd.

- *Toegang tot informatie wordt bepaald door enerzijds de authenticatie en anderzijds de autorisatie van personen.*
- *Voor wat betreft de vaststelling van identiteit en de bevestiging daarvan, de authenticatie, zijn de maatregen in dat Handboek informatiebeleid vastgelegd en geïmplementeerd. Iedereen heeft een gebruikersnaam en een wachtwoord en die combinatie is altijd noodzakelijk om in de pc te komen en buiten het provinciehuis is er zelfs nog een token nodig om toegang tot het systeem te krijgen.*
- *De toegang tot de informatie binnen de systemen, de toegangsrechten, dus de autorisatie, is geregeld op grond van de functie die een medewerker heeft. Iemand die bij bodem werkt, komt niet in het deel dat bestemd is voor de treasury.'*

(...)
'Ik ga verder.
Dit noemen wij het rol-gebaseerde autorisatiemodel. De verantwoordelijkheid voor de juiste toegangsrechten ligt bij het functioneel beheer.
Er is een heel proces voor de uitgifte en het beheer van gebruikersnamen, wachtwoorden en toegangsrechten. Het toont allemaal aan dat het in dit huis conform alle overheidsregels is geregeld, maar – alweer – het gaat er ook om in hoeverre daar zorgvuldig, verantwoord en integer gebruik van wordt gemaakt.
Dat geldt ook voor het afdrukken van informatie op printers; alle decentrale copyers en printers hebben de mogelijkheid om met een persoonlijke code te printen en daar de printen af te halen, dit alles om te voorkomen dat ook onbevoegden documenten kunnen printen waarover zij niet de beschikking behoren te krijgen.
Het informatiebeleid is ontzettend afhankelijk van alle ontwikkelingen op ICT-gebied en die ontwikkelingen gaan heel snel. In 1997 zaten we nog in de tijd van de visstick en nu inmiddels in de tijd van de usb-stick. Dat vergt een doorlopende aanpassing van het systeem. De code voor informatiebeveiliging van overheidswege is in 2007 weer geactualiseerd; het beleidskader informatiebeveiliging van dit huis is daarop gebaseerd en is inmiddels door de directie vastgesteld. De basisnormen en maatregelen voor informatiebevelliging zijn ook afgerond, maar die hebben wij nog even aan KMPG om advies voorgelegd, want wij willen voldoen aan de modernste en nieuwste eisen op het gebied van ICT, die van ons worden verlangd.
Hoe het zit met de fysieke toegang tot het gebouw weten de statenleden als geen ander. Er is alleen toegang tot het provinciehuis, althans dat gedeelte dat buiten het openbare gedeelte van de hal ligt, te verkrijgen door middel van een toegangspas. De gebruikers van het gebouw zijn in verschillende categorieën ingedeeld: bestuur, medewerkers in vaste dienst, medewerkers in tijdelijke dienst, staten- en commissieleden, leveranciers, bezoekers en dienstverleners. Zij zijn allemaal geautoriseerd op het niveau dat voor hun werk noodzakelijk is. Ook dat is allemaal keurig vastgelegd in ons autorisatiereglement. Voor alle gebruikers geldt draagplicht van de pas.'

Uit het onderzoek van de commissie is niet gebleken dat de provincie met betrekking tot het integriteitbeleid en het informatie- en informatiebeveiligingsbeleid de zaken niet op orde heeft. De organisatie voert een actief integriteitbeleid. Ten aanzien van informatie- en informatiebeveiligingsbeleid is er voldoende geregeld in beleid- en regelgeving. Dat betekent uiteraard niet dat zaken niet voor verbetering vatbaar zouden zijn en dat het beleid in alle gevallen wordt gevolgd (zie paragraaf 4.3). De kennis van wet- en regelgeving over de genoemde onderwerpen is ook niet bij iedereen even groot. Een aantal documenten over het informatie- en het informatiebeveiligingsbeleid staan niet (meer) op het Huisnet, waardoor medewerkers ook niet eenvoudig kennis kunnen nemen van deze documenten. Tevens blijkt dat bovengenoemde beleidsonderwerpen ook niet stelselmatig aan de orde komen in werkoverleggen.
Bovendien kunnen zaken op papier dan wel goed geregeld zijn - de commissie sluit zich aan bij de door de heer Baas gegeven verklaring in het debat van PS op 18 maart 2009 - als er niet op een goede manier invulling aan wordt gegeven, is het risico dat er dingen fout lopen, altijd aanwezig.

De commissie is echter van mening dat er voor moet worden gewaakt dat naar aanleiding van deze affaire binnen de ambtelijke organisatie onnodig ingrijpende maatregelen worden genomen om herhaling te voorkomen.
Desalniettemin blijven onderwerpen als integriteit en informatiebeleid zaken die naar de mening van de commissie structureel aandacht behoeven van de organisatie en dient het informatiebeveiligingsbeleid van de provincie te allen tijde te worden nageleefd en dient daar toezicht op te bestaan.

5.3 Beleid ten aanzien van omgang met de media

In de vorige hoofdstukken is uitgebreid stilgestaan bij de aard en frequentie van contacten tussen gedeputeerden en journalisten en dat deze contacten daarmee een bestuurlijk-culturele factor vormen die mogelijk een rol heeft gespeeld in de voortijdige verspreiding van het Eurochamprapport .
Uit het onderzoek van de commissie is gebleken dat binnen GS niet regelmatig wordt gesproken over contacten met de media en de manier waarop daarmee dient te worden omgegaan.
Gedeputeerde mevrouw Haarsma verklaart over de omgang met de pers het volgende in de hoorzitting:

'Mevrouw Smith: Wat vindt u van de manier van omgaan door GS met de pers?

Mevrouw Haarsma: Die vind ik goed.

Mevrouw Smith: Goed op welke manier?

Mevrouw Haarsma: Het is maar net welke kwalificatie je aan "goed" geeft. Ik vind dat wij op een transparante manier met de pers omgaan. Daar waar nodig weten wij de pers te vinden en de pers ons. Volgens mij hoort dat ook zo in een politiek-bestuurlijke omgeving.

Mevrouw Smith: En wat voor soort relatie is dat met de pers?

Mevrouw Haarsma: Een zakelijke, professionele relatie.

Mevrouw Smith: Wordt hierover in het college van GS wel eens of regelmatig gesproken?

Mevrouw Haarsma: Niet dat ik mij kan herinneren dat het een thema is.

Mevrouw Smith: U spreekt elkaar er ook niet op aan in de zin van: "Goh, je hebt die journalist gebeld, had je dat wel moeten doen."

Mevrouw Haarsma: Iedereen is verantwoordelijk voor zijn eigen portefeuille en wij weten van elkaar dat wij allemaal regelmatig contacten hebben met de pers.'

Gedeputeerde mevrouw Klip verklaart hierover:

'Natuurlijk is er een algemene lijn in de richting van de media vanuit de afdeling communicatie. Maar de inhoudelijke contacten betreffende onze portefeuilles, want daar gaat het natuurlijk altijd over, lopen toch voornamelijk één op één tussen de portefeuillehouder, de bestuursadviseur, of de communicatieadviseur voor 1 januari, en de betreffende journalist.'

Hoewel er kennelijk binnen GS niet wordt gesproken hoe in specifieke gevallen om dient te worden gegaan met de media, volgt uit het sms'je dat gedeputeerde mevrouw Klip aan de heer Klaver heeft gestuurd, dat

men hier kennelijk in sommige gevallen wel een mening over heeft, maar dat die niet intern binnen GS wordt gedeeld.
In dit sms'je, dat reeds in het vorige hoofdstuk aan de orde is gekomen, stelt mevrouw Klip dat zij het vreemd vindt dat de heer De Bruin betrokken wordt bij het bedenken van scenario's. Mevrouw Klip verklaart hierover als volgt:

'Wat ik wist stond ongeveer in dat mailtje. Ik had via de tam-tam in het provinciehuis vernomen dat de heer De Bruin behulpzaam was bij het bedenken van scenario's. Ik heb dat opgevat als scenario's over hoe kan dat nou dat er eventueel informatie bij de krant terecht gekomen is.

Mevrouw Stijkel: U heeft in principe niets gehoord over de invulling van die scenario's?

Mevrouw Klip: Nee

De heer Bomhof: U zegt wel wat over het omgaan met de media. Als meneer De Bruin zomaar bij communicatie rondloopt en hij zich bemoeit met scenario's dan vraag ik me als eerste af: hoe komt die man daar, heeft hij een pasje blijkbaar, kan hij zomaar binnenkomen. Dat was toen nog het geval. De openheid, het gemak en de vertrouwelijkheid, althans volgens tam-tam, om hem maar zo te betrekken bij het pr-beleid van de provincie is verbazingwekkend.

Mevrouw Klip: Dat is een constatering van uw kant. Ik denk dat als vanuit uw commissie adviezen in onze richting komen wij daar heel serieus naar zullen kijken.

De heer Bomhof: Het is geen constatering van mijn kant maar het is een conclusie die ik heb kunnen trekken uit het mailtje waarin u zelf zegt: het is verbazingwekkend dat Martin de Bruin zich bemoeit met de scenario's in dit huis. Dan denk ik aan tweerichtingsverkeer, je mag je ermee bemoeien maar je staat ook toe dat iemand zich daar mee bemoeit. En dat is dus de houding waar dit huis, dat hij dus niet de deur gewezen wordt, zeg maar, van waar bemoei jij je mee. Nee, gechargeerd hoor, kom er maar in en wat vind je er van en verwen hem maar eens even. Dat is dus één van de vragen die gesteld zijn, het heeft ook met de houding te maken in dit huis, hoe staat je tegenover de pers. Eén sms'je geeft aan dat er zodanig open en gemakkelijk allemaal loopt en er weinig scheiding is tussen pers en ambtenaren dat dàt, naar mijn gevoel, een zorgpunt is, die al een verbeterpunt is. Of denkt u niet?

Mevrouw Klip: Over dit specifieke geval heeft u uit mijn sms kunnen constateren dat ik heb geformuleerd dat ik het vreemd vond.

De heer Bomhof: Vreemd, dus in algemene zin ook dan de omgang met de media op dat punt.

Mevrouw Klip: Wat betreft omgang met de media kan ik natuurlijk voornamelijk alleen over mijn eigen contacten met de media spreken. Niet over de andere bestuurders en ja ik heb eigenlijk niets toe te voegen aan dat sms'je. Ik vond dat vreemd, klopt.'

De commissie vindt het opmerkelijk dat dergelijk sms-verkeer tussen gedeputeerden en statenleden plaatsvindt en dat mevrouw Klip via de sms een dergelijke mededeling aan de heer Klaver doet en hierover niet mevrouw Haarsma aanspreekt of het onderwerp binnen een vergadering van GS of PS aan de orde stelt.

Uit het onderzoek van de commissie is gebleken, dat ten aanzien van het Eurochampdossier binnen GS niet is gesproken over een te voeren mediastrategie. Deze mediastrategie is zelfstandig bepaald door mevrouw Haarsma en haar communicatieadviseur.
De commissie zet vraagtekens bij het gevoerde mediabeleid in deze kwestie. Mevrouw Haarsma heeft in de Statenvergadering van 12 november 2008 verklaard dat het rapport vertrouwelijk was en dat er niet over

gesproken kon worden zolang de zaak onder de rechter was. Zelfs Statenleden konden op dat moment het rapport nog niet inzien.
Dit heeft mevrouw Haarsma er zelf niet van weerhouden om die week met journalisten te praten over het Eurochamprapport. Dit blijkt uit diverse krantenartikelen van die week waarin zij wordt geciteerd en waarin zij verwijst naar het Deloitte-rapport. Tevens geeft zij een interview aan de heer De Bruin, waarvan het initiatief van haar kant is uitgegaan, omdat zij graag de 'andere kant van de medaille wilde belichten'.

Gezien de in voorgaande hoofdstukken besproken aard en frequentie van contacten met de media, is naar de mening van de commissie de schijn gewekt dat in strijd is gehandeld met artikel 4 van de gedragscode (zie hoofdstuk 2) en dat niet zorgvuldig is omgegaan met vertrouwelijke informatie.
Die schijn had naar de mening van de commissie voorkomen kunnen worden als er in de periode vanaf 10 november 2008 tot aan de openbaarmaking van het rapport niet door bestuurders was gesproken met journalisten over het Eurochamprapport. Doordat mevrouw Haarsma in de week van 10-15 november een aantal malen is geciteerd in het Dagblad van het Noorden en er een interview is gegeven aan de krant om de 'andere kant van de medaille te belichten', is de schijn gewekt dat er over een vertrouwelijk rapport is gesproken, hetgeen in strijd is met artikel 4.1 en 4.2 van de integriteitcode van de provincie.

De onduidelijkheid die bestaat over de aard van het contact en hetgeen er in de contacten tussen gedeputeerde mevrouw Klip en de journalist de heer De Kleine ter sprake is gekomen, wekt eveneens de schijn dat in strijd met artikel 4 is gehandeld. Daarbij moet worden opgemerkt dat de vriendschap met deze journalist, waarbij meerdere keren per dag telefonisch contact plaatsvindt, deze schijn versterkt. Temeer als daar door betrokken personen geen transparantie in wordt betracht.
Mevrouw Klip is tegenover de commissie niet op eigen initiatief begonnen over haar vriendschap met de journalist. Naar de mening van de commissie had zij zich moeten realiseren dat deze vriendschap een relevant gegeven zou kunnen betekenen voor het onderzoek van de commissie. De commissie vindt daarom dat zij deze vriendschap en de vele contacten al in het voorgesprek ter sprake had moeten brengen.

5.4 Beantwoording derde onderzoeksvraag

De derde onderzoeksvraag van de commissie betreft de vraag in hoeverre het gevoerde bestuur moet worden aangepast om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen.

Uitgaande van de antwoorden op de eerste twee onderzoeksvragen, is de commissie van mening dat het gevoerde bestuur moet worden aangepast, zij het in beperkte mate, om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen. De commissie vindt dat met name het gevoerde bestuur ten aanzien van het omgaan met de media veranderd dient te worden. De commissie vindt dat hier in GS onderling meer over gesproken dient te worden en dat er meer transparantie moet komen over de aard, frequentie en inhoud van contacten van gedeputeerden met journalisten.
De commissie is van mening dat door het gevoerde mediabeleid in het Eurochampdossier de schijn is gewekt dat in strijd is gehandeld met artikel 4 van de Drentse gedragscode integriteit Commissaris van de Koningin, Gedeputeerde Staten en Provinciale staten.

De commissie is van mening dat er voor moet worden gewaakt dat naar aanleiding van deze affaire binnen de ambtelijke organisatie ingrijpende maatregelen worden genomen om herhaling te voorkomen. Naar de mening van de onderzoekscommissie valt, uitgaande van de bevindingen, de ambtelijke organisatie in zijn algemeenheid weinig aan te rekenen, al zijn er wel punten van kritiek op onderdelen. De organisatie voert een uitgebreid integriteitbeleid. Ten aanzien van informatie en informatiebeveiliging is er voldoende geregeld in beleid- en regelgeving. Wel dient er beter op te worden toegezien dat het informatie- en informatiebeveiligingsbeleid wordt nageleefd.

In hoofdstuk 6 doet de commissie enkele aanbevelingen op welke manieren het gevoerde bestuur kan worden aangepast.

6 Conclusies en aanbevelingen

6.1 Conclusies

De commissie acht het aannemelijk dat de digitale versie van het definitieve Eurochamprapport in de week van 10-15 november 2008 voortijdig vanuit het provinciehuis naar buiten is gebracht en in handen is gekomen van het Dagblad van het Noorden, al dan niet direct of indirect via een tussenpersoon. De commissie heeft niet kunnen vaststellen op welke wijze en in welke vorm het voortijdig is verspreid en door wie.
Daarmee kan niet worden vastgesteld wie er verantwoordelijk is voor de voortijdige verspreiding van het Eurochamprapport. Dit laat onverlet de bestuurlijke verantwoordelijkheid van het college van Gedeputeerde Staten.
De mogelijkheid dat het rapport vanuit Deloitte verzonden is aan mensen buiten het provinciehuis, is volgens de commissie niet meer dan een theoretische mogelijkheid. KPMG heeft hiernaar specifiek onderzoek gedaan en zij hebben daar geen aanwijzingen voor gevonden.

De commissie is van mening dat een viertal organisatorische en/of bestuurlijk-culturele factoren deze voortijdige verspreiding van het rapport kunnen hebben bevorderd dan wel het risico daarvan hebben vergroot. Dit zijn de aard, frequentie en intensiteit van contacten met de media, de geforceerde wil om de beeldvorming in de media te beïnvloeden, het in het bezit zijn van journalisten van een vaste toegangspas voor het provinciehuis en het op onderdelen niet naleven van het informatiebeveiligingsbeleid.

De commissie is van mening dat het gevoerde bestuur moet worden aangepast, zij het in beperkte mate, om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen. De commissie vindt dat met name het gevoerde bestuur ten aanzien van het onderhouden van contacten met media veranderd dient te worden. De commissie vindt dat hier binnen het college van GS en ook in PS meer over gesproken dient te worden en dat er meer transparantie moet komen over de aard en frequentie van contacten van bestuurders met journalisten.
De commissie is van mening dat door het gevoerde mediabeleid in het Eurochampdossier de schijn is gewekt dat in strijd is gehandeld met artikel 4 van de Drentse gedragscode integriteit Commissaris van de Koningin, Gedeputeerde Staten en Provinciale Staten.

De commissie is van mening dat er voor moet worden gewaakt dat naar aanleiding van deze affaire binnen de ambtelijke organisatie onnodig ingrijpende maatregelen worden genomen om herhaling te voorkomen. Naar de mening van de onderzoekscommissie valt, uitgaande van de bevindingen, de ambtelijke organisatie in zijn algemeenheid weinig aan te rekenen, al zijn er punten van kritiek op onderdelen. De organisatie voert een uitgebreid integriteitbeleid. Ten aanzien van informatie en informatiebeveiliging is er voldoende geregeld in beleid- en regelgeving. Wel dient er beter op te worden toegezien dat het informatie- en informatiebeveiligingsbeleid wordt nageleefd.

6.2 Aanbevelingen

De commissie doet de volgende aanbevelingen:

1. Gedeputeerden dienen in hun contacten met de media de afdeling communicatie nadrukkelijker te betrekken. Directe contacten tussen gedeputeerden en journalisten dienen professioneel, zakelijk en transparant te blijven, omdat anders de schijn van ongewenste informatie-uitwisseling kan worden gewekt.

2. Het onderwerp omgang met de media dient te worden geagendeerd voor zowel de vergadering van GS als PS, waarbij duidelijke uitgangspunten ten aanzien van gewenste omgangsvormen van gedeputeerden en statenleden met de media moeten worden geformuleerd.
3. De vaste toegangspassen van journalisten moeten worden ingenomen. De commissie vindt dat voor journalisten dezelfde regels moeten gelden als voor andere bezoekers van het provinciehuis. De commissie heeft vernomen dat het beleid dienaangaand tijdens haar onderzoeksperiode inmiddels is aangepast.
4. Documenten op het gebied van veiligheid, integriteit, informatiebeleid en omgang met media, dienen een nadrukkelijke plaats op het intranet/huisnet te krijgen, zodat iedere medewerker hier eenvoudig kennis van kan nemen.
5. In het verlengde daarvan dient de naleving van het informatie- en informatiebeveiligingsbeleid onder de aandacht van de ambtelijke organisatie te worden gebracht, waarbij voorts een nadere uitwerking van de spelregels ten aanzien van het gebruik van e-mailverkeer voor vertrouwelijke informatie te overwegen is.
6. Regels met betrekking tot informatiebeveiliging zullen door de steeds veranderende technische omgeving en mogelijkheden regelmatig moeten worden geëvalueerd en aangepast.
7. Het voeren van een intensief integriteitbeleid dient te worden gecontinueerd en op gezette tijden geëvalueerd te worden.
8. De door een ieder aan andere ambtenaren/bestuurders verleende toegangsrechten tot de eigen e-mailbox, dienen periodiek individueel te worden nagelopen. Voorkomen moet worden dat verleende toegangsrechten onbedoeld blijven bestaan.
9. Het verdient overweging om alle inkomende e-mailberichten automatisch te bewaren ('weg te schrijven') teneinde onbedoeld verlies van informatie te voorkomen.

dat is een vertrouwelijk stuk?!

2.3.2 Beleidskader informatiebeveiliging provincie Drenthe (februari 2009)

In het Beleidskader informatiebeveiliging provincie Drenthe (getiteld: *Veilig, integer en vertrouwd: hoe is onze informatie beveiligd?*) wordt beschreven hoe ambtenaren (en bestuurders) van de provincie Drenthe dienen om te gaan met informatiebeveiliging.
In het beleidskader worden de volgende definities gehanteerd:

*'**Informatie** is een bedrijfsmiddel dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor de organisatie en voortdurend op een passende manier beveiligd dient te zijn.*
Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden of in gesproken vorm). Welke vorm de informatie ook heeft of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn.

***Informatiebeveiliging** bestaat uit het treffen van maatregelen die beogen te voorkomen dat onbevoegden vertrouwelijke gegevens kunnen bezitten, raadplegen of beschadigen.*
Informatiebeveiliging wordt gekarakteriseerd als het waarborgen van:
Veilige beschikbaarheid: geautoriseerde gebruikers hebben op de juiste momenten tijdig toegang tot informatie en aanverwante bedrijfsmiddelen;
Integriteit: correctheid en volledigheid van informatie en de verwerking daarvan;
Vertrouwelijkheid: informatie is alleen toegankelijk voor degenen, die hiertoe geautoriseerd zijn en daarmee op de juiste wijze omgaan'.

Als uitgangspunt voor het informatiebeveiligingsbeleid wordt door de Provincie Drenthe de Code voor Informatiebeveiliging (NEN/ISO 270001 en 270002) gehanteerd. In deze code worden de volgende tien categorieën noodzakelijke beveiligingsmaatregelen onderscheiden:

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie en beheer van bedrijfsmiddelen
4. Beveiligingseisen ten aanzien van personeel.
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatie- en bedieningsprocessen
7. Toegangsbeveiliging
8. Aanschaf, ontwikkeling en onderhoud van systemen
9. Continuïteitsmanagement
10. Naleving

In het handboek Informatiebeveiliging worden bovenstaande onderwerpen en de regelingen omtrent naleving meer in detail behandeld.

2.3.3 Handboek Informatiebeveiliging (2005)

Dit document geldt als bijlage bij het Beleidskader informatiebeveiliging. De tien beveiligingsmaatregelen, zoals in de vorige paragraaf beschreven, worden hierin uitgebreid behandeld. Met name wordt ingegaan op de richtlijnen, procedures en werkwijzen van de beveiligingsmaatregelen. Deze maatregelen gelden als basisnorm waaraan de provincie Drenthe zich minimaal wil houden om veilig, integer en vertrouwd met informatie om te gaan. Hieronder worden kort een aantal aspecten uit dit handboek belicht.
In hoofdstuk 5 van het Handboek wordt gesproken over classificatie en beheer van bedrijfsmiddelen.

Hier wordt beschreven op welke wijze informatie geclassificeerd kan worden en welke typen er bestaan. Op deze manier wordt het duidelijk welke toegangsrechten er verbonden zijn aan een bepaalde classificatie,zoals vertrouwelijkheid. De volgende typen classificaties worden onderscheiden:

- ***Openbaar***
  Informatie die voor derden toegankelijk is (lezen). Wijzigen van deze informatie kan uitsluitend door medewerkers van de Provincie (eigenaar) plaats vinden.

- ***Niet Openbaar,*** *onderverdeeld in:*
  - *Intern gebruik:*
    Alle interne informatie die uitsluitend voor medewerkers van de provincie Drenthe toegankelijk is. Op basis van functie worden toegangsrechten tot deze informatie toegekend.
  - *Vertrouwelijk:*
    Informatie die uitsluitend voor een beperkte groep medewerkers van de provincie toegankelijk is. Bij de informatie dient aangegeven te worden wie toegang heeft tot de informatie.
  - *Persoonlijk:*
    Informatie uitsluitend bestemd voor de geadresseerde.

Tevens staat in dit hoofdstuk beschreven hoe informatie gelabeld dient te worden:
- *Voor alle informatiesystemen wordt de geldende classificatie van informatie vastgesteld.*
- *Informatie zonder label wordt als "Intern gebruik" behandeld.*
- *Documenten met vertrouwelijke en persoonlijke informatie dienen op de voorpagina en in de koptekst voorzien te zijn van het label.'*

In hoofdstuk 8 van het Handboek wordt het beleid rondom het gebruik van e-mail beschreven. Hier wordt onder meer gesteld dat het niet toegestaan is om vertrouwelijke informatie te verzenden via de e-mail. Daarnaast wordt gesteld dat de provincie de e-mail alleen voor informele communicatie mag gebruiken.
In hoofdstuk 12 van het Handboek wordt onder meer ingegaan op welke wijze bedrijfsdocumenten dienen te worden beschermd tegen verlies, diefstal, vernietiging en vervalsing. Naast de classificatie en labelling van informatie zoals beschreven in hoofdstuk 5, worden er extra maatregelen ondernomen om informatie optimaal te beveiligen. Zo staat er onder meer geschreven:

- *'Vertrouwelijke informatie dient in afgesloten kasten te worden bewaard na werktijd en bij het verlaten van de werkruimte*
- *Belangrijke systeeminformatie (systeemtoegang) dient centraal in een afgesloten ruimte bewaard te worden'.*

PERSOONLIJK EN VERTROUWELIJK
Provincie Drenthe
Onderzoekscommissie Eurochamp PS Drenthe
T.a.v. de secretaris, mevrouw I.M. Rozema
Postbus 122
9400 AC ASSEN

Amersfoort, 4 mei 2009

Betreft: Rapportage deskresearch

Geachte Onderzoekscommissie,

Op uw verzoek hebben wij een deskresearch verricht. Deze dekresearch betreft ondersteuning van de commissie in de eerste fase van uw onderzoek naar de voortijdige verspreiding van een als vertrouwelijk bestempeld onderzoeksrapport. De opdracht voor ondersteuning van uw commissie is vastgelegd in uw opdrachtbrief van 21 april en onze offerte van 17 april jongstleden. Hierbij rapporteren wij onze bevindingen.

1. BING

BING biedt gespecialiseerde adviesexpertise en onderzoeksexpertise aan.
Het bureau richt zich daarbij exclusief op de overheid, wat borg staat voor specifieke branchekennis, verdieping van ervaringen en de mogelijkheid om duurzame relaties met de doelgroep te onderhouden. BING is een initiatief van de Vereniging van Nederlandse Gemeenten (VNG).

2. Aanleiding en doel van opdracht

Provinciale Staten (PS) van Drenthe hebben besloten om een onderzoek in te stellen op grond van artikel 151a van de Provinciewet naar de voortijdige verspreiding van een als vertrouwelijk bestempeld onderzoeksrapport. Provinciale staten hebben daartoe op 8 april jl. een onderzoekscommissie geïnstalleerd.

De centrale vragen in het onderzoek zijn:

- wie is verantwoordelijk voor de voortijdige verspreiding van het rapport van Deloitte en op welke wijze is dat geschied;
- waren er bij de provincie Drenthe organisatorische en/of 'bestuurlijk-culturele' factoren die de voortijdige verspreiding hebben bevorderd;
- in hoeverre moet het gevoerde bestuur worden aangepast om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen.

De eerste fase van het onderzoek is met name de fase van deskresearch. Doelstelling van deze fase is het verzamelen en analyseren van beschikbare informatie. Deze fase dient uit te monden in een advies waarin

onder meer moet worden aangegeven op welke punten in de tweede fase zich het nader onderzoek zou moeten toespitsen.

3. Door BING verrichte werkzaamheden

Wij hebben onder meer de volgende werkzaamheden verricht:

- Kennisname en analyse van het KPMG rapport;
- Kennisname en analyse van het verslag van het debat op 18 maart 2009 in Provinciale Staten;
- Kennisname en analyse van de van toepassing zijnde regelgeving en procedures en andere relevante documenten.

4. Kader

In dit hoofdstuk wordt kort het kader geschetst dat relevant is voor de beantwoording van de onderzoeksvragen. Dit kader bestaat uit een juridisch kader, de relevante wet- en regelgeving, en een beleidskader. Tot dit beleidskader behoren diverse documenten die door de provincie ten aanzien van het onderwerp informatie en informatiebeveiliging zijn opgesteld.[1]

4.1 Juridisch kader

Wij vermelden hier de wettelijke artikelen die - gelet de casus - het meeste relevant zijn.
Op basis van artikel 125a lid 3 van de Ambtenarenwet is een ambtenaar verplicht tot geheimhouding van hetgeen hem in verband met zijn functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt. Een breder kader wordt geschetst door artikel 125ter: 'Het bevoegd gezag en de ambtenaar zijn verplicht zich als een goed werkgever en een goed ambtenaar te gedragen.'

Op basis van artikel 55 van de Provinciewet kunnen Gedeputeerde Staten (GS) geheimhouding opleggen omtrent de inhoud van stukken die aan hen worden overgelegd.

Een schending van de geheimhouding kan een strafbaar feit opleveren. In artikel 272 van het Wetboek van Strafrecht is de schending van de geheimhouding geregeld. De tekst van het artikel luidt als volgt:

Artikel 272
1. Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.
2. Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.

---

[1] Als bijlage bij deze rapportage is een document bijgevoegd met alle geraadpleegde documenten

4.2 Integriteitcode

De provincie Drenthe beschikt over zowel een ambtelijke gedragscode (Gedragscode ambtelijke integriteit) als een code voor de bestuurders; de Drentse gedragscode integriteit voor de CvdK, GS en PS.

4.2.1 Bestuurlijke gedragscode

De integriteitcode voor de statenleden en leden van GS van de Provincie Drenthe is vastgesteld door PS op 3 september 2003.
In de integriteitcode worden een aantal kernbegrippen genoemd. Dit zijn: dienstbaarheid, functionaliteit, onafhankelijkheid, openheid, betrouwbaarheid en zorgvuldigheid.
Deze kernbegrippen worden in de integriteitcode gezien als toetssteen voor de in de integriteitcode opgenomen gedragsafspraken. De leden van het college van GS en PS worden geacht de regels na te leven. Wanneer zij zich er niet aan houden, kan dat - blijkens de tekst van de code - gevolgen hebben voor hun functioneren en voor hun positie.

Voor deze casus is met name artikel 4 van de code van belang. In dit artikel, getiteld 'Informatie', staat het volgende:
Artikel 4.1 Een bestuurder gaat zorgvuldig en correct om met informatie waarover hij uit hoofde van zijn ambt beschikt. Hij verstrekt geen geheime informatie.

Artikel 4.2 Een bestuurder verstrekt informatie, tenzij deze geheim of vertrouwelijk is en het geven van informatie niet mogelijk is op grond van de Wet openbaarheid van bestuur.

Artikel 4.3 Een bestuurder maakt niet ten eigen bate of ten bate van zijn persoonlijke betrekkingen gebruik van in de uitoefening van het ambt verkregen informatie.

In de inleiding van de bestuurlijke gedragscode staat dat er voor ambtenaren tevens een beroepscode is opgesteld, waar integriteit een belangrijk deel van uitmaakt. De voorliggende code en de beroepscode voor ambtenaren zijn op elkaar afgestemd. Er staan geen tegenstrijdige bepalingen in, zo staat er geschreven.

4.2.2 Ambtelijke gedragscode

De Gedragscode ambtelijke integriteit is vastgesteld bij besluit van GS van 18 maart 2003. In de code worden de volgende zes kernbegrippen van ambtelijke integriteit onderscheiden: dienstbaarheid, professionaliteit, onafhankelijkheid, verantwoordelijkheid, betrouwbaarheid en zorgvuldigheid.
In de code zelf komt het onderwerp omgaan met informatie niet terug. Wel bestaat er bij de provincie een document getiteld 'Omgaan met provinciale informatie' **[datum opnemen].** Hierin wordt gesteld dat zorgvuldig moet worden omgegaan met informatie. Voor vertrouwelijke stukken geldt dit – volgens de tekst van het document – nog eens extra. Tevens staat in het document letterlijk: 'Lekt informatie bijvoorbeeld via de pers uit, dan kun je hier als medewerker persoonlijk op worden aangesproken.'

4.3 Beleidskader

Tot het beleidskader behoren een aantal documenten. De meest relevante documenten worden hieronder besproken.

4.3.1 Reglement gebruik bedrijfsmiddelen (2006)

In het Reglement gebruik bedrijfsmiddelen staat de procedure omschreven omtrent beschikbaarheid, gebruik, controle en bewaring van bedrijfsmiddelen. Artikel 2 t/m 6 worden als relevant beschouwd voor het onderzoek en zullen hieronder worden toegelicht.

In artikel 2 van het reglement staat dat gedragingen worden toegerekend aan diegene die op de computer is ingelogd. De tekst van het artikel luidt als volgt:

Artikel 2.

1. De directie kan de beschikbaarheid van bedrijfsmiddelen beëindigen of beperken wanneer een medewerker de bedrijfsmiddelen gebruikt op een wijze die in strijd is met dit reglement.
2. Een medewerker die de beschikking heeft over e-mailfaciliteiten is verplicht zijn postbus regelmatig te controleren of te doen controleren. De directie kan hiervoor nog nadere aanwijzingen geven.
3. Gedragingen worden toegerekend aan degene die op de computer is ingelogd.
4. Het installeren van software en applicaties is niet toegestaan, tenzij vooraf toestemming is verleend door de directie. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en eventuele licenties worden betaald.

In artikel 4 van het reglement staat dat het een medewerker niet is toegestaan om door het gebruik van bedrijfsmiddelen, schade te berokkenen aan de provincie Drenthe als instantie, haar werknemers en/of aan derden. De tekst van het artikel luidt als volgt:

Artikel 4.

1. De gebruiker mag alleen gebruikmaken van de bedrijfsmiddelen die beschikbaar worden gesteld door de provincie Drenthe. Uitzonderingen op deze bepaling zijn slechts mogelijk met schriftelijke toestemming van de directie. Aan deze toestemming kunnen voorwaarden worden verbonden.
2. Het is de gebruiker niet toegestaan om door middel van het gebruik van bedrijfsmiddelen zich zodanig te gedragen dat:
- de goede naam van de provincie kan worden geschaad;
- het ongestoord functioneren van de technische infrastructuur van de provincie in gevaar wordt gebracht;
- de vertrouwelijkheid van gegevens kan worden geschaad;
- het strijdig is met geaccepteerde omgangsvormen of goede zeden, belastend is voor de goede werksfeer dan wel beledigend is voor medewerkers en/of derden;
- het onrechtmatig is of een strafbaar feit oplevert;
- het strijdig is met de CAP;
- de provincie op enigerlei andere wijze dan op vorenstaande genoemde wijzen kan worden geschaad, hetzij in financiële zin, hetzij anderszins.
3. Het gebruik van middelen gericht op het verhinderen van kennisname binnen de provinciale organisatie van de inhoud van berichten en bijlagen door anderen dan de opsteller is niet geoorloofd. Van deze bepaling kan door de directie ontheffing worden verleend. Aan de ontheffing kunnen voorwaarden worden verbonden.

4. Gebruik van bedrijfsmiddelen voor privé-doeleinden wordt toegestaan mits met mate, uitgedrukt in zowel tijd en kosten, en niet in strijd met dit reglement. Voor het privé-gebruik van bedrijfsmiddelen kan de directie een financiële vergoeding vragen.

In artikel 5 van het Reglement gebruik bedrijfsmiddelen (2006) staat omschreven hoe de observatie en controle van gebruiksmiddelen plaatsvindt en welk doel het dient. Er staat onder meer in dat de directie ten allen tijde opdracht kan geven tot observatie. In artikel 6 wordt nader ingegaan op de regels omtrent het bewaren van gegevens. In dit artikel staat onder andere vermeld dat e-mails bewaard worden overeenkomstig de termijnen van de Archiefwet.

4.3.2 Uitvoeringsprogramma Drenthe (2006-2007)

In dit uitvoeringsprogramma (getiteld: Welkom in digitaal Drenthe) staat omschreven welke stappen de provincie onderneemt om de inzet van IT te verbeteren. Hoofdstuk 2 van dit document is het informatiestatuut. In dit statuut wordt specifiek ingegaan op het onderwerp informatiebeveiliging. Hierin wordt gesteld dat de provincie werkt op basis van de Code voor Informatiebeveiliging en dat in de planperiode wordt gestreefd naar een volledige invulling daarvan. Daarnaast staat beschreven dat medewerkers als gebruikers van de IT-hulpmiddelen geen misbruik mogen maken van de aan hen toevertrouwde middelen en gegevens. Zij mogen deze middelen slechts gebruiken voor hun werkzaamheden voor de provincie.

4.3.3 Beleidskader informatiebeveiliging provincie Drenthe (februari 2009)

In het Beleidskader informatiebeveiliging provincie Drenthe (getiteld: Veilig, integer en vertrouwd: hoe is onze informatie beveiligd?) wordt beschreven hoe ambtenaren van de provincie Drenthe dienen om te gaan met informatiebeveiliging.
In het beleidskader worden de volgende definities gehanteerd:

*'**Informatie** is een bedrijfsmiddel dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor de organisatie en voortdurend op een passende manier beveiligd dient te zijn.*
Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden of in gesproken vorm). Welke vorm de informatie ook heeft of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn.

***Informatiebeveiliging** bestaat uit het treffen van maatregelen die beogen te voorkomen dat onbevoegden vertrouwelijke gegevens kunnen bezitten, raadplegen of beschadigen.*
Informatiebeveiliging wordt gekarakteriseerd als het waarborgen van:
Veilige beschikbaarheid: geautoriseerde gebruikers hebben op de juiste momenten tijdig toegang tot informatie en aanverwante bedrijfsmiddelen;
Integriteit: correctheid en volledigheid van informatie en de verwerking daarvan;
Vertrouwelijkheid: informatie is alleen toegankelijk voor degenen, die hiertoe geautoriseerd zijn en daarmee op de juiste wijze omgaan'.

Als uitgangspunt voor het informatiebeveiligingsbeleid wordt door de Provincie Drenthe de Code voor Informatiebeveiliging (NEN/ISO 270001 en 270002) gehanteerd. In deze code worden de volgende tien categorieën noodzakelijke beveiligingsmaatregelen onderscheiden:

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie en beheer van bedrijfsmiddelen
4. Beveiligingseisen ten aanzien van personeel.
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatie- en bedieningsprocessen
7. Toegangsbeveiliging
8. Aanschaf, ontwikkeling en onderhoud van systemen
9. Continuïteitsmanagement
10. Naleving.

In het handboek Informatiebeveiliging worden deze bovenstaande onderwerpen en de regelingen omtrent naleving meer in detail behandeld.

4.3.4 Handboek Informatiebeveiliging (2005)

Dit document geldt als bijlage bij het Beleidskader informatiebeveiliging en is bestemd voor de afdeling automatisering van de provincie Drenthe. De tien beveiligingsmaatregelen, zoals in de vorige paragraaf beschreven, worden hierin uitgebreid behandeld. Met name wordt ingegaan op de richtlijnen, procedures en werkwijzen van de beveiligingsmaatregelen. Deze maatregelen gelden als basisnorm waaraan de provincie Drenthe zich minimaal wil houden om veilig, integer en vertrouwd met informatie om te gaan.
In deze paragraaf wordt stilgestaan bij drie relevante hoofdstukken uit dit handboek.

Hoofdstuk 5: Classificatie en beheer bedrijfsmiddelen
In dit hoofdstuk wordt beschreven op welke wijze informatie geclassificeerd kan worden en welke typen er bestaan. Op deze manier wordt het duidelijk welke toegangsrechten er verbonden zijn aan een bepaalde classificatie,zoals vertrouwelijkheid. De volgende typen classificaties worden onderscheiden:

- ***Openbaar***
  Informatie die voor derden toegankelijk is (lezen). Wijzigen van deze informatie kan uitsluitend door medewerkers van de Provincie (eigenaar) plaats vinden.

- ***Niet Openbaar,*** *onderverdeeld in:*
  - *Intern gebruik:*
    Alle interne informatie die uitsluitend voor medewerkers van de provincie Drenthe toegankelijk is. Op basis van functie worden toegangsrechten tot deze informatie toegekend.
  - *Vertrouwelijk:*
    Informatie die uitsluitend voor een beperkte groep medewerkers van de provincie toegankelijk is. Bij de informatie dient aangegeven te worden wie toegang heeft tot de informatie.
  - *Persoonlijk:*
    Informatie uitsluitend bestemd voor de geadresseerde.

In dit hoofdstuk staat beschreven hoe informatie gelabeld dient te worden:
'Labelen en verwerken van informatie
- *Voor alle informatiesystemen wordt de geldende classificatie van informatie vastgesteld.*
- *Informatie zonder label wordt als "Intern gebruik" behandeld.*
- *Documenten met vertrouwelijke en persoonlijke informatie dienen op de voorpagina en in de koptekst voorzien te zijn van het label.'*

Hoofdstuk 8: Beheer van communicatie- en bedieningsprocessen; Onderwerp: Beleid ten aanzien van e-mail
In dit hoofdstuk wordt het beleid rondom het gebruik van e-mail beschreven. Hier wordt onder meer gesteld dat het niet toegestaan is om vertrouwelijke informatie te verzenden via de e-mail. Daarnaast wordt gesteld dat de provincie de e-mail alleen voor informele communicatie mag gebruiken.

Hoofdstuk 12: Naleving; Onderwerp: Beveiliging van bedrijfsdocumenten
In dit hoofdstuk wordt onder meer ingegaan op welke wijze bedrijfsdocumenten dienen worden beschermd tegen verlies, diefstal, vernietiging en vervalsing.
Naast de classificatie en labelling van informatie zoals beschreven in hoofdstuk 5, worden er extra maatregelen ondernomen om informatie optimaal te beveiligen. Deze maatregelen staan als volgt beschreven:

- *'Vertrouwelijke informatie dient in afgesloten kasten te worden bewaard na werktijd en bij het verlaten van de werkruimte*
- *Belangrijke systeeminformatie (systeemtoegang) dient centraal in een afgesloten ruimte bewaard te worden.*
- *Applicatiebeheerders beheren systeemdocumentatie van de diverse informatiesystemen. Deze documentatie bestaat uit:*
  - *Documentatie inzake de logische werking;*
  - *Documentatie inzake de technische werking;*
  - *Contracten e.d. met de leverancier(s) van de applicatie (archief);*
  - *Kwaliteitsgegevens over het systeem (meta-informatie);*
- *Bij het gebruik van elektronische opslagmedia worden maatregelen getroffen die ervoor zorgen dat de informatie leesbaar blijft (zowel de media zelf, als het gegevensformaat) gedurende de gehele bewaarperiode, teneinde te voorkomen dat de informatie verloren gaat ten gevolge van toekomstige technologische veranderingen. Deze maatregelen met betrekking tot de houdbaarheid van gegevens betreffen uitsluitend actuele systemen.'*

5. KPMG rapport

Het KPMG rapport naar het 'lekken' van het Eurochamprapport dient als basis voor het onderzoek van de provinciale onderzoekscommissie. In dit hoofdstuk worden de belangrijkste bevindingen van het KPMG rapport besproken.

5.1 Onderzoeksvraag en conclusies KPMG

De onderzoeksvraag voor het onderzoek van KPMG luidde als volgt:

'Is het definitieve rapport van Deloitte Forensic Services inzake Stichting Eurochamp Foundation voortijdig verspreid vanuit het Provinciehuis? Zo ja, op welke wijze, wanneer en door wie?'

De conclusie van KPMG is dat het definitieve rapport van Deloitte buiten het Provinciehuis terecht is gekomen, voordat het openbaar is gemaakt op 27 november 2009. KPMG heeft niet kunnen vaststellen op welke wijze dit is gebeurd en door wie.

KMPG heeft in haar rapport de belangrijkste feiten samengevat op een rijtje gezet. Deze luiden als volgt:

- 'De versie van het rapport die is verspreid voordat het rapport openbaar is gemaakt op 27 november 2008 betreft het definitieve *'Rapport inzake onderzoek naar de Stichting Eurochamp Foundation'*. Het rapport heeft het referentienummer 3112182270/2111.
- De versie die de heer Klaver in zijn bezit heeft vanaf 21 november 2008, betreft de digitale (pdf-) versie van voornoemde rapportage.
- De digitale (pdf-) versie van de rapportage is in de periode tussen 10 en 16 november niet verder per e-mail verspreid.
- De informant heeft verklaard dat hij de wetenschap heeft dat een exemplaar van het rapport in ieder geval op de ochtend van 13 november in het bezit is van Dagblad van het Noorden.
- Het Dagblad van het Noorden heeft aangegeven inzage te hebben gehad in de rapportage. Dit is in een redactioneel commentaar in Dagblad van het Noorden bevestigd. Niet is aangegeven welke versie van het rapport door Dagblad van het Noorden is ingezien.'

5.2 Uitgelekte versie

Door de onderzoekers van KPMG is vastgesteld dat er een aantal versies van het Deloitte rapport in omloop zijn geweest. Dit betreffen de volgende vier versies:

1. Een concept versie die in het kader van hoor en wederhoor aan de advocaat van een betrokkene in het Eurochamponderzoek is voorgelegd.
2. Een concept versie met nummer 3112182270/2135 die op 3 november 2008 per e-mail is verstuurd naar de provincie en op basis waarvan op 4 november 2008 overleg tussen de provincie Drenthe en Deloitte heeft plaatsgevonden.
3. De digitale versie van het definitieve rapport met nummer 311218227/2111 die op 10 november 2008 door Deloitte per email is verstuurd aan de secretaresse van de directie van de provincie, [redacted]
4. De ingebonden versie van het definitieve rapport met nummer 311218227/2111 die op 10 november 2008 door Deloitte per koerier aan de provincie is verzonden.

Door de onderzoekers van KPMG is vastgesteld dat het de digitale versie van het definitieve rapport (hierboven genoemd onder drie) betreft die uiteindelijk 'gelekt' is naar de buitenwereld, hoewel het woord 'lekken' niet als zodanig benoemd is. Het verschil tussen deze versie en de onder vier genoemde versie betreft volgens KPMG een lay out verschil. Tevens bevat de digitale versie van het definitieve rapport abusievelijk één pagina twee maal. Dit is bij de ingebonden versie niet het geval.

5.3 Kennis van de digitale versie

Volgens KPMG is de digitale versie van het definitieve rapport door Deloitte op 10 november 2008 om 14.11 uur verzonden aan de secretaresse van de directie van de provincie Drenthe [redacted] Dit is gebeurd naar aanleiding van een telefoongesprek tussen een medewerker van Deloitte en [redacted]

Door Deloitte is er op 10 november 2008 telefonisch contact opgenomen met de provincie om mede te delen dat het rapport die middag per koerier aan de provincie zou worden verzonden. Door [redacted] is, volgens het onderzoek van KPMG, vervolgens uit eigen initiatief aangegeven dat zij ook graag een digitale versie van het rapport zou willen ontvangen. Deze versie is uiteindelijk om 14.11 uur die dag verzonden [redacted]. Deze digitale versie van het rapport was volgens KPMG opgeknipt in drie aparte PDF-bestandjes, die als bijlagen bij één email zijn verzonden aan [redacted] heeft deze email bewaard in een archief map van haar emailprogramma.
KPMG heeft niet kunnen achterhalen/vaststellen of de digitale versie tussen 10 en 13 november 2008 (de datum waarop de krant volgens de informant over een exemplaar van het rapport beschikte) verder digitaal is verspreid en/of gekopieerd op een externe mediadrager.
[redacted] zou in het interview met KMPG hebben gezegd dat haar inloggegevens van haar computer op dat moment bij niemand bekend zouden zijn geweest. Pas op 17 november 2008 zou zij deze gegevens hebben verstrekt aan de plaatsvervangend directeur. Op die datum heeft de plaatsvervangend directeur het rapport doorgezonden aan de landsadvocaat.
De gedeputeerde mevrouw Klip zegt tijdens het debat van 18 maart 2008 dat [redacted] twee andere medewerkers heeft geautoriseerd om toegang te krijgen tot haar inloggegevens (zie hoofdstuk 6). Dit komt niet overeen met de verklaring van [redacted]

Uit het KPMG rapport wordt niet duidelijk wie nu precies op de hoogte waren van het feit dat [redacted] een digitale versie van het rapport had ontvangen. In het rapport van KPMG staat hierover het volgende:
'Er zijn volgens een aantal geïnterviewden een paar medewerkers en/of gedeputeerden op de hoogte dat het rapport op 10 november 2008 per mail is ontvangen van Deloitte.'

De mogelijkheid bestaat dat de directie (directeur/secretaris en directeur/plaatsvervangend secretaris) hiervan op de hoogte was. Het was immers hun secretaresse die dit document in haar bezit had gekregen. Mogelijk zou ook de communicatie-adviseur van mevrouw Haarsma, de heer Van de Bosch, alsmede mevrouw Haarsma zelf hiervan op de hoogte kunnen zijn. Mevrouw Haarsma ontkent tijdens het debat dat later is gevoerd in PS, dat zij hiervan op de hoogte was.
Vermeldenswaard is dat mevrouw Haarsma op maandagmiddag 10 november 2008 op pad was met de plaatsvervangend secretaris van de provincie, mevrouw Weistra (dit staat overigens niet in het KPMG rapport, maar is mondeling medegedeeld). Mevrouw Weistra heeft diezelfde avond op het provinciehuis de doos met ingebonden rapporten in ontvangst genomen van de beveiliging van het provinciehuis, waarna de ongeopende doos in een afgesloten kast is opgeborgen.

Ook kan nog worden opgemerkt dat op 11 november 2008 een bespreking heeft plaatsgevonden over het Eurochamprapport. Bij die bespreking waren volgens KPMG aanwezig mevrouw Haarsma, de heer Van de Bosch, mevrouw Weistra en een vertegenwoordiger van Deloitte. Volgens het KPMG rapport zou uit de interviews met de betrokkenen zijn gebleken, dat deze bespreking heeft plaatsgevonden aan de hand van het concept rapport en dus niet op basis van het de dag daarvoor binnengekomen definitieve rapport.

5.4 Statenlid de heer Klaver

De fractievoorzitter van het CDA in PS, de heer Klaver, heeft een belangrijke rol gespeeld in de totstandkoming van het onderzoek van KPMG, als ook in het onderzoek zelf. De heer Klaver heeft in een schrijven (vermoedelijk aan GS) d.d. 21 november 2008 het verzoek gedaan tot het doen van een onderzoek naar de verspreiding van het Eurochamprapport. De inhoud van dit rapport zou volgens hem reeds bekend zijn bij de regionale media. De heer Klaver zou deze informatie hebben ontvangen van een informant, waarover in de volgende paragraaf meer.

De heer Klaver zou, blijkens het KPMG rapport, in de middag van 21 november 2008 van zijn informant te horen hebben gekregen dat de informant in de ochtend van 13 november 2008 de beschikking zou hebben gekregen over een versie van het Eurochamprapport. De heer Klaver heeft op vrijdagmiddag 21 november 2008 van zijn informant een kopie van deze versie van het rapport in zijn bezit gekregen.
Naast dit document, zou de heer Klaver ook meerdere e-mails in handen hebben gekregen. Uit één van die e-mails zou blijken dat het Dagblad van het Noorden 'een bron op hoogste bestuursniveau' van de provincie uit de wind wil houden. Dit heeft de heer Klaver tijdens het debat op 18 maart 2008 in PS verklaard. Tevens zou de heer Klaver in november en december 2008 een aantal anonieme brieven hebben ontvangen omtrent zijn rol in deze kwestie. KPMG heeft hiernaar verder geen onderzoek gedaan. De heer Klaver heeft hiervan aangifte gedaan bij de politie.

5.5 Rol informant

Het onderzoek van KPMG is mede gebaseerd op de verklaringen van een informant. KPMG heeft uitvoerig met deze informant (het betreft een man, afgaande op de mondelinge mededelingen van KPMG) gesproken De onderzoekers van KPMG betitelen de informatie van de informant als betrouwbaar. Letterlijk schrijven zij:
'*De bevindingen in deze rapportage zijn mede gebaseerd op vertrouwelijke informatie die wij van deze informant ter beschikking hebben gekregen. Wij achten de van deze informant verkregen informatie, op grond van de samenhang met andere voor het onderzoek beschikbare informatie, betrouwbaar.*'

De onderzoekers van KPMG kunnen (of willen) niet vertellen waarom deze informant zich tot de heer Klaver heeft gericht. Dit zou mogelijk de identiteit van de informant kunnen onthullen.

Over de persoon van de informant gaan inmiddels diverse geruchten rond. Daarbij wordt gesuggereerd dat de informant werkzaam zou zijn bij het Dagblad van het Noorden. Vooralsnog zijn deze geruchten echter niet bevestigd. Eén van de twee journalisten die verslag heeft gedaan van de bevindingen van het Eurochamprapport, zit momenteel ziek thuis. Gesuggereerd is dat dit te maken zou hebben met de kwestie van het lekken. Officieel wordt echter gesteld dat de journalist om gezondheidsredenen thuis zit.

Wat volgens KPMG vaststaat, is dat de informant de wetenschap heeft dat het Dagblad van het Noorden op de ochtend van 13 november 2008 in het bezit was van een exemplaar van het Eurochamprapport. Op 12 november 2008 zou de informant te horen hebben gekregen dat er een definitief rapport beschikbaar was.

De informant heeft zijn wetenschap op 21 november 2008 doorgespeeld aan de heer Klaver. Volgens KPMG heeft er een ontmoeting plaatsgevonden, waarbij door de heer Klaver een kopie is gemaakt van het rapport dat in het bezit was van de informant. De versie die in het bezit was van de informant betrof een print van de digitaal verzonden definitieve versie van het rapport.

5.6 Dagblad van het Noorden

Uit het KPMG rapport volgt dat twee journalisten van het Dagblad van het Noorden zich hebben bezig gehouden met het Eurochamprapport. Dit zijn de journalisten de heer De Bruin en de heer De Kleine. Hieronder wordt in chronologische volgorde hun betrokkenheid toegelicht.

Volgens KPMG heeft de heer De Bruin op 12 november 2008 een bezoek gebracht aan de advocaat van een van de betrokkenen van het Eurochamponderzoek. De journalist heeft hierover later aangegeven dat hij bij dit bezoek inzage heeft gehad in de versie van het rapport die de advocaat in zijn bezit had. Door de

advocaat wordt deze inzage ontkend. Uit het KMPG rapport volgt dat de advocaat, in ieder geval op dat moment, geen versie van het definitieve rapport in zijn bezit had, maar 'slechts' een gedeeltelijke concept versie die hem in het kader van hoor en wederhoor was verstrekt. Naar aanleiding van dit bezoek zou de heer De Bruin het artikel '*Jan heeft geen strafbare feiten begaan'* hebben geschreven dat op 15 november 2008 is gepubliceerd.

Eveneens op 12 november 2008 was de heer De Bruin, volgens KPMG, aanwezig op een avondbijeenkomst op het provinciehuis. Hij zou daarbij hebben gesproken met de gedeputeerde mevrouw Haarsma. Mevrouw Haarsma zou naar aanleiding van dit 'gesprek' het idee hebben gekregen dat de journalist in het bezit zou zijn van het Eurochamprapport. Op een later moment heeft zij volgens KPMG de journalist hierover aangesproken en hem hierop bevraagd. De journalist zou daarbij hebben aangegeven dat hij inzage had gehad, maar dat hij zijn bronnen niet bekend zou kunnen maken.

Op donderdagmiddag 13 november 2008 heeft mevrouw Haarsma een gesprek gehad met journalist De Bruin. Bij dat gesprek was ook haar communicatieadviseur de heer Van de Bosch aanwezig. Bij dat gesprek zou, volgens het KPMG rapport, zijn gesproken over de 'wijze van aanbesteding', zoals die in het Eurochamprapport naar voren komt. (Op dat moment is de krant, volgens de informant, reeds in het bezit van het definitieve rapport.)

Op 15 november 2008 wordt in de krant het artikel '*Het rapport over opkomst en ondergang van Eurochamp'* gepubliceerd. In dat artikel wordt volgens KPMG gemeld dat de journalisten inzage hebben gehad in het Deloitte rapport over Eurochamp.

Op woensdag 19 november 2008 hebben de heren De Bruin en De Kleine volgens het KPMG rapport een bezoek gebracht aan de advocaat van een van de betrokkenen van het Eurochamprapport. Niet duidelijk wordt of dit dezelfde advocaat betreft als de eerdergenoemde advocaat.
Twee dagen later, op 21 november 2008, meldt de informant zich bij de heer Klaver.

5.7 Bevindingen digitaal onderzoek

Door KPMG is een forensisch IT onderzoek uitgevoerd. Daarbij heeft KPMG, zoals eerder opgemerkt, niet kunnen vaststellen of de digitale versie tussen 10 november 2008 14.11 uur en 13 november 2008 (de datum waarop de informant over deze versie beschikte en ook de krant over een versie (dezelfde?) beschikte) verder digitaal is verspreid en/of gekopieerd op een externe mediadrager.
Daartoe is onder andere de computer van [redacted] onderzocht. Daarbij heeft men niet kunnen vaststellen of zij tussen 10 november 2008 en 13 november 2008 de betreffende digitale versie heeft uitgeprint. Andere computers zijn niet onderzocht.
Tevens is door KPMG het e-mailverkeer aan de hand van logginggegevens onderzocht. Daarbij heeft men niet kunnen vaststellen dat andere medewerkers van de provincie en/of leden van GS de betreffende versie van het rapport tussen 10 en 16 november 2008 per email hebben ontvangen. KPMG concludeert dat de digitale (pdf-)versie van het rapport in de periode tussen 10 en 16 november niet verder per e-mail verspreid is

6. Debat in provinciale staten

Op 18 maart 2009 is in Provinciale Staten gesproken over het rapport van KPMG. Tijdens dit debat is besloten tot het instellen van een provinciale onderzoekscommissie. In het debat zijn een aantal zaken aan de orde gekomen die van belang zijn voor het onderzoek van de provinciale onderzoekscommissie. Dit betreft met name uitlatingen van leden van GS.

Mevrouw Haarsma heeft tijdens het debat gereageerd op een groot aantal vragen die haar zijn gesteld door leden van de PS.
Over het gesprek met de journalist De Bruin op woensdagavond 12 november 2008 heeft zij het volgende verklaard:
'Ik stond in de rij met mijn bordje, voor of naast mij – dat weet ik niet meer precies – stond collega Klip en aan de andere kant stond de journalist. De journalist stelde mij verschillende vragen, waarop ik geen antwoord heb gegeven en vervolgens heb ik tegen mevrouw Klip gezegd: "Het lijkt wel alsof het rapport bij het Dagblad van het Noorden is." Dat heb ik aan mevrouw Klip gemeld.
Vervolgens heb ik mijn bordje leeggegeten en daarna ben ik 's avonds met de fractievoorzitter naar huis gereden en heb ik nog eens over alles nagedacht. De volgende ochtend heb ik in aanwezigheid van mijn bestuursadviseur een afspraak menen te moeten maken met het Dagblad van het Noorden. De reden hiervoor was dat wij beiden vonden dat het in de media voornamelijk nog ging over het aanbestedingsbeleid, terwijl de echte inhoud volledig uit het zicht was verdwenen. Mijn communicatie-adviseur en ik hebben met de journalist een gesprek gehad, in welk gesprek mijn eerste vraag aan hem was of er een rapport in het bezit was van het Dagblad van het Noorden. De journalist heeft geantwoord dat er geen rapport in het bezit van het dagblad was, dat ook hij geen rapport had, maar dat hij wel inzage in het rapport had gehad. Hij wist ook feilloos aan te geven wanneer dat was – het staat ook in het KPMG-rapport – want hij was woensdagochtend in Almere of Lelystad - waar precies weet ik niet meer – op bezoek geweest bij de advocaat van de heer Leijssenaar. Dat is wat de journalist mij heeft verteld.'

Over het opvragen van een digitale versie van het rapport verklaart zij het volgende:
'Ik kom bij een essentieel deel van het verhaal, het pdf-bestand. Op 14.11 uur is een pdf-bestand ontvangen. De heer Klaver heeft gevraagd op wiens verzoek en op wiens initiatief dit bestand is opgevraagd. Ik heb hiernaar uiteraard navraag gedaan bij de directie en mij is verteld dat de directie de secretaresse heeft gevraagd nog eens met Deloitte te bellen of de provincie het definitieve rapport daadwerkelijk die dag zou ontvangen. Wij vonden het nodig over het definitieve rapport te beschikken omdat wij voornemens waren om, zodra het college hierover de daaropvolgende dinsdag een besluit zou hebben genomen, aangifte te doen bij het OM.'

(...)

'De opdracht was niet te vragen of een pdf-bestand opgestuurd kon worden, maar wanneer het rapport binnen zou komen. Het antwoord was dat dit waarschijnlijk aan het eind van de dag zou zijn. Daarop heeft de secretaresse met de beste bedoelingen gevraagd het rapport per e-mail te sturen. Dat is gebeurd en die e-mail is om 14.11 uur ontvangen.
Dan is natuurlijk de volgende vraag wie wisten dat dit e-mail bericht zou binnenkomen, maar....'

(...)

'*Wie wist dat het pdf-bestand bij de provincie is terechtgekomen? Dat waren een aantal medewerkers, een paar collegeleden en de directie. Ik kan naar eer en geweten zeggen dat ik het niet wist.*'

Deze verklaring van mevrouw Haarsma komt niet geheel overeen met hetgeen door KPMG aan de onderzoekscommissie is verteld. Volgens KPMG heeft Deloitte gebeld met de provincie en heeft de secretaresse toen uit eigen beweging gevraagd naar een digitale versie van het rapport. Later tijdens het debat spreekt mevrouw Haarsma over medewerkers en/of gedeputeerden.

Mevrouw Haarsma stelt in het debat dat zij wel op de hoogte was van het feit dat het rapport van Deloitte op 10 november 2008 zou binnenkomen:
'*Ik wist dat de doos binnen kwam, want ik had die dag met de plaatsvervangend directeur een bespreking bij de NAM in Assen en toen wij op het provinciehuis terug kwamen, was de doos gearriveerd. De plaatsvervangend directeur heeft toen gezegd de doos bij haar in de kast te zetten, omdat de volgende dag de besluitvorming op basis van de oplegnotitie zou plaatsvinden. Het was daarna aan de directie om op enig moment, omdat het in de aanloop naar de aangifte toch wel relevant werd de doos eens te openen, te openen. Daar heb ik mij niet mee bemoeid.* '

Mevrouw Haarsma verklaart over haar gesprek met de journalist De Bruin op 13 november 2008 het volgende:
'*Het volgende punt dat ik wil bespreken is de verwevenheid. De heer Klaver heeft gevraagd hoe het in dit huis met die verwevenheid zit. Net als hij vinden wij het belangrijk ons product goed te verkopen en wij – en ik spreek expres in de wij-vorm – vinden dat wij op een correcte en integere manier met de pers omgaan. Dat is het waardeoordeel dat ik namens het college kan geven.*
Ik kom op 13 november, dat datum waarop ik in aanwezigheid van mijn bestuursadviseur een gesprek heb gehad met de journalist. Er is toen uitvoerig gesproken over het feit dat mij was opgevallen dat het eigenlijk alleen nog maar over de aanbestedingsregels ging en niet meer over waarvoor het onderzoek was gestart, namelijk de vraag wat er onrechtmatig was gebeurd. Het was niet zo dat wij de aanbestedingsregels onbelangrijk vonden, integendeel, maar de kern waarop het onderzoek zich diende te richten waren de handelingen die in onze optiek niet door de beugel konden. Dat heb ik met de pers besproken, niet meer en niet minder en dat gesprek heeft pakweg drie kwartier geduurd. '

(...)

'*Dat is heel simpel. Ik heb net al gezegd dat ik met de communicatieadviseur had besproken dat de zaak wel een gekke wending nam, omdat het bericht alleen ging over de aanbesteding, terwijl het volgens ons ook om heel andere zaken ging. Wij besloten een afspraak met het Dagblad van het Noorden te maken om ook die kant van de medaille te laten zien.*'

Mevrouw Haarsma stelt hier dat er in een bericht voornamelijk alleen nog maar wordt gesproken over de aanbestedingsregels. Onduidelijk is aan welk bericht zij refereert. Op het moment van het gesprek met de journalist is het artikel over het rapport nog niet verschenen. Wellicht refereert zij aan andere berichten in de media. De onderzoekscommissie dient mevrouw Haarsma hierover tijdens het voorgesprek nader te bevragen.

Mevrouw Klip reageert in het debat onder meer op een vraag van de heer Klaver of de secretaresse van de directie haar inloggegevens heeft gedeeld met anderen:
'*Mijnheer de voorzitter. Ik heb nog twee vragen van de heer Klaver openstaan.*

De eerste ervan was of de betreffende medewerker van het directiesecretariaat haar wachtwoord ook aan anderen heeft gegeven, met andere woorden of ook anderen in de bestanden op de computer van de bewuste medewerker van het directiesecretariaat kunnen komen.
Op pagina 15 van het rapport van KPMG staat dat die medewerkster haar wachtwoord heeft gegeven aan de directeur/plaatsvervangend secretaris zodat die het bestand naar haar eigen computer kon overbrengen om het vervolgens te verzenden naar de landsadvocaat. Verder heeft deze medewerker van het directiesecretariaat twee mensen gemachtigd om via hun eigen e-mailaccount in haar bestanden te komen. Het gaat dan om haar kamergenoot en de secretaresse van de CvdK.'

heeft ze later herroepen

Uit dit antwoord volgt dat er mogelijk twee mensen zijn die in de periode tussen 10 en 13 november 2008 reeds in de bestanden van [redacted] konden komen, te weten de kamergenoot (onduidelijk is wie dit is) van [redacted] en de secretaresse van de Commissaris van de Koningin. Dit gegeven volgt niet uit het KPMG rapport.

Tijdens het debat laat gedeputeerde mevrouw Klip zich ook uit over het integriteitbeleid van de provincie en het onderwerp informatiebeveiliging:
'Voorzitter. Ik kom op mijn andere verantwoordelijkheid: de portefeuille personeel en organisatie. Waar gaat dat over? Het gaat daarbij om de besteding van personeelsbudgetten, samen met de portefeuillehouder financiën, het gaat over organisatieontwikkeling en reorganisatie en het gaat dan inderdaad ook over integriteitbeleid. Het Rijk heeft het integriteitsbeleid hoog in het vaandel en hetzelfde geldt voor deze provincie. Dit betekent dat wij allerlei dingen uit een voorschriftenlijst van het Rijk moeten implementeren in onze organisatie. Ik noem er een paar. Het gaat over gedragscodes, over noodzakelijke onderzoeken bij werving en selectie, het gaat over het kwalificeren van kwetsbare functies en de mogelijk niet integere relatie waarvan tussen bepaalde bevoegdheden en functies sprake kan zijn, het gaat over het afleggen van de ambtseed of –belofte, het gaat over het inventariseren van nevenwerkzaamheden, het gaat over relatiegeschenken en zo kan ik nog wel even doorgaan.
Implementeren is een en op een puntje na hebben wij dit allemaal al geruime tijd geleden gedaan. In alle monitoringsrapportages van het Ministerie van BZK scoren wij heel hoog. Maar dat is niet alles, want wij moeten die integriteit ook levend houden. Er moet voor gezorgd worden dat ambtenaren zich er voortdurend bewust van zijn. Dat betekent dat wij rond het afleggen van de ambtseed een programma organiseren dat er op gericht is dat mensen zich hiervan bewust zijn. Dat gebeurt via programma's op internet en via gesprekken binnen de verschillende teams.
Toch – en dat hebben wij de staten ook op papier laten weten – lijkt het ons naar aanleiding van de huidige situatie niet alleen verstandig maar ook noodzakelijk ons integriteitsbeleid nogmaals tegen het licht te houden. Daarbij kan gedacht worden aan nog dwingender gesprekken van managers en aan het incorporeren van bepaalde integriteitsaspecten in de individuele werkplannen van medewerkers. Daarvoor kunnen allerlei vormen gevonden worden en wij starten daar ik zou bijna zeggen morgen mee.
Daarnaast houden wij ook – dit hebben wij de staten ook laten weten – het huidige beleid op het gebied van informatiebeveiliging en fysieke beveiliging – het gaat dan om het gebouw – opnieuw tegen het licht. Collega Baas, kenner op dit gebied en bovendien verantwoordelijk portefeuillehouder, zal daar straks meer over zeggen. Want de opmerking dat de vertrouwelijkheid van onze provinciale informatie gewaarborgd moet zijn, is volstrekt terecht. Maar – en dat is niet een maar van "ach, het doet er niet toe," maar dat is de maar van de realiteit – wij kunnen als openbaar bestuur in een openbaar, of bijna openbaar toegankelijk gebouw zowel fysiek als digitaal geen vesting worden.
Integriteit zit tussen de oren. Wij hebben als bestuur en als directie de verantwoordelijkheid om zowel via de structuur, waarvan ik zojuist een aantal voorbeelden heb genoemd, als via een permanent proces van bewustwording en bewust houden, ervoor te zorgen dat die integriteit ook tussen de oren blijft zitten. Uiteindelijk moet dit ertoe leiden – maar in deze mensenwereld blijft dat een utopie – dat integriteit een

vanzelfsprekendheid is. Daar zetten we erg op in en daar gaan we naar aanleiding van deze gebeurtenis nog strakker op inzetten.
Voorzitter. Ik kom op de vragen die gesteld zijn aangaande de medewerker van het secretariaat.
Wij hebben een hele reorganisatie en een organisatieontwikkeling achter de rug. Wij proberen – de staten zijn daarover de afgelopen jaren voldoende bijgepraat – onder mijn bestuurlijke verantwoordelijkheid een provincie voor de toekomst te worden. Dat betekent niet binnenskamers heel goed zijn in je eigen vakgebied, maar van buiten naar binnen samen met de buitenwereld zorgen dat die ontwikkelingen tot stand gebracht worden waar de maatschappij om vraagt. Dat betekent dat wij steeds de nadruk leggen op proactieve ambtenaren, ambtenaren die meedenken met het bestuur en zo zelf nadenken over wat er nodig zou zijn.
Natuurlijk is er een grens aan proactief handelen en – ik moet nu even gaan voorlezen wat ik al eerder aangeleverd heb gekregen – de vraag of een ambtenaar, in dit geval een medewerker van het directiesecretariaat op eigen houtje een vertrouwelijk pdf-file kan aanvragen, moet ik als volgt beantwoorden. Ik citeer: "Iedere ambtenaar is bevoegd en bekwaam voor zijn functie en wordt geacht keuzes te maken die passen bij en vallen binnen de verantwoordelijkheid en bevoegdheid van de functie." Dat is een citaat uit de Collectieve arbeidsvoorwaarden van de provincies (CAP) die gelden voor alle 12 provincies en zijn vastgelegd in CAO-afspraken.
Deze keuze van de medewerker van de directiesecretariaat valt binnen die kaders. '

De gedeputeerde de heer Baas heeft zich in het debat ook uitgelaten over het onderwerp informatiebeveiliging:
'*Mijnheer de voorzitter. Ik wil nog graag een aantal aanvullende opmerkingen maken, die betrekking hebben op het door ons gevoerd informatiebeleid, ook in relatie tot de zaak die vanmiddag zo nadrukkelijk speelt. Daarbij wil ik ook van mijn kant nog eens benadrukken – het wordt bijna saai – dat ook informatiebeveiliging valt of staat met de zorgvuldigheid en integriteit waarmee iedereen in deze organisatie daarmee omgaat. Er kunnen nog zoveel voorschriften, maatregelen, protocollen en procedures gemaakt worden, als er niet op een goede manier invulling aan wordt gegeven, is het risico dat er dingen fout lopen, altijd aanwezig. Ook dit is mensenwerk en fouten zijn nooit en in geen enkele organisatie uit te sluiten. Dit is uiteraard geen excuus dat het is voorgevallen; het is ernstig genoeg dat het is gebeurd en dat dit nu zoveel van onze tijd kost.*
De huidige maatregelen die binnen de provincie Drenthe gelden met betrekking tot de informatiebeveiliging zijn vastgelegd in ons Handboek informatiebeveiliging. Dit handboek is gebaseerd op de binnen de gehele overheid geldende code voor informatiebeveiliging. Die code dateert uit de jaren tachtig/negentig van de vorige eeuw en die geldt binnen de rijksoverheid en de provinciale en gemeentelijke overheden als basis voor alles wat op het gebied van informatiebeveiliging in dit land moet worden gedaan. Binnen de provincie is dat verankerd in het Informatiestatuut.
Het Handboek informatiebeveiliging schrijft voor de informatiebeveiliging multidisciplinair te benaderen en integraal in de organisatie te beleggen in termen van verantwoordelijkheden. Dat wordt nader uitgewerkt in concrete maatregelen, gerubriceerd op onderwerp. De relevante onderwerpen op het gebied van toegang tot en verspreiding van informatie zijn als volgt in dat handboek vastgelegd.
- *Toegang tot informatie wordt bepaald door enerzijds de authenticatie en anderzijds de autorisatie van personen.*
- *Voor wat betreft de vaststelling van identiteit en de bevestiging daarvan, de authenticatie, zijn de maatregen in dat Handboek informatiebeleid vastgelegd en geïmplementeerd. Iedereen heeft een gebruikersnaam en een wachtwoord en die combinatie is altijd noodzakelijk om in de pc te komen en buiten het provinciehuis is er zelfs nog een token nodig om toegang tot het systeem te krijgen.*
- *De toegang tot de informatie binnen de systemen, de toegangsrechten, dus de autorisatie, is geregeld op grond van de functie die een medewerker heeft. Iemand die bij bodem werkt, komt niet in het deel dat bestemd is voor de treasury. '*

(...)

'Ik ga verder.
Dit noemen wij het rol-gebaseerde autorisatiemodel. De verantwoordelijkheid voor de juiste toegangsrechten ligt bij het functioneel beheer.
Er is een heel proces voor de uitgifte en het beheer van gebruikersnamen, wachtwoorden en toegangsrechten. Het toont allemaal aan dat het in dit huis conform alle overheidsregels is geregeld, maar – alweer – het gaat er ook om in hoeverre daar zorgvuldig, verantwoord en integer gebruik van wordt gemaakt.
Dat geldt ook voor het afdrukken van informatie op printers; alle decentrale copyers en printers hebben de mogelijkheid om met een persoonlijke code te printen en daar de printen af te halen, dit alles om te voorkomen dat ook onbevoegden documenten kunnen printen waarover zij niet de beschikking behoren te krijgen.
Het informatiebeleid is ontzettend afhankelijk van alle ontwikkelingen op ict-gebied en die ontwikkelingen gaan heel snel. In 1997 zaten we nog in de tijd van de visstick en nu inmiddels in de tijd van de usb-stick. Dat vergt een doorlopende aanpassing van het systeem. De code voor informatiebeveiliging van overheidswege is in 2007 weer geactualiseerd; het beleidskader informatiebeveiliging van dit huis is daarop gebaseerd en is inmiddels door de directie vastgesteld. De basisnormen en maatregelen voor informatiebeveiliging zijn ook afgerond, maar die hebben wij nog even aan KMPG om advies voorgelegd, want wij willen voldoen aan de modernste en nieuwste eisen op het gebied van ICT, die van ons worden verlangd.
Hoe het zit met de fysieke toegang tot het gebouw weten de statenleden als geen ander. Er is alleen toegang tot het provinciehuis, althans dat gedeelte dat buiten het openbare gedeelte van de hal ligt, te verkrijgen door middel van een toegangspas. De gebruikers van het gebouw zijn in verschillende categorieën ingedeeld: bestuur, medewerkers in vaste dienst, medewerkers in tijdelijke dienst, staten- en commissieleden, leveranciers, bezoekers en dienstverleners. Zij zijn allemaal geautoriseerd op het niveau dat voor hun werk noodzakelijk is. Ook dat is allemaal keurig vastgelegd in ons autorisatiereglement.
Voor alle gebruikers geldt draagplicht van de pas.'

Over het rapport op de computer van [redacted] zegt de heer Baas onder meer nog het volgende:
'Het is in ieder geval zo dat de bijlage bij de e-mail niet apart op de pc is opgeslagen. Het rapport is dus gewoon als bijlage bij de e-mail in het bestand blijven zitten.
Maar ik moet nu even op mijn gezonde boerenverstand afgaan en dat is veel slechter dan dat van een hacker: als ik thuis op de pc van de betrokken secretaresse wil inloggen, moet ik beschikken over zowel haar password en gebruikersnaam als haar token. Om die drie hindernissen te overwinnen, moet je toch heel wat mans zijn en wat mij betreft is het haast onmogelijk dat te doen.
Voor wat de heer Vester aangeeft met betrekking tot het gebruik van een usb-stick en printers, zitten op het huidige systeem geen programma's. '

7. Aandachtspunten vervolgonderzoek

De informant beschikte over de digitale versie van het definitieve rapport. Uit het KPMG onderzoek blijkt niet dat dit ook de versie is waarover het Dagblad van het Noorden beschikte. Dat is echter wel waarschijnlijk, aangezien de informant heeft bevestigd dat hij de wetenschap heeft dat een exemplaar van het rapport op de ochtend van 13 november in het bezit is van Dagblad van het Noorden. Het 'lekken' moet hebben plaatsgevonden tussen maandag 10 november 2008 14.11 uur (het moment van ontvangst van het digitale rapport) en donderdagochtend 13 november 2008 12.00 uur, het moment dat het rapport volgens de informant in het bezit is van het Dagblad van het Noorden.

Uit het KPMG rapport wordt niet duidelijk wie, naast [redacted] in de betreffende periode kennis heeft van de ontvangst/het bestaan van een digitale versie van het rapport. Dit is het eerste punt van aandacht voor het vervolgonderzoek van de onderzoekscommissie: vaststellen (door middel van interviews) wie binnen de provincie kennis had van het bestaan van een digitale versie van het rapport in de periode 10 tot en met 13 november 2008.

Uit het onderzoek van KPMG is niet vast komen te staan of het rapport in de periode 10 tot en met 13 november 2008 verder digitaal is verspreid en/of gekopieerd op een externe mediadrager. Ook is niet duidelijk geworden wie mogelijk toegang hadden tot de computer van [redacted]
Dit betreft het tweede aandachtspunt voor het vervolgonderzoek: vaststellen (door middel van interviews) van de kring van personen die in de betreffende periode toegang hadden tot de computer of de e-mail van [redacted] en het eventueel nader onderzoeken van de computers van deze betreffende personen.

De bestudering door een forensisch IT expert van BING van de resultaten van het digitale onderzoek van KMPG zou mogelijk nieuwe aanknopingspunten kunnen opleveren voor nader te doen forensisch IT onderzoek. Wellicht dat hiermee nieuwe informatie kan worden verkregen over de eventuele verspreiding van het Eurochamprapport in de periode 10-13 november 2008. Op dit moment zijn deze gegevens nog niet bekend. De bestudering van het materiaal van KPMG en de resultaten van het door BING te verrichten aanvullend forensisch IT onderzoek vormen daarmee het derde aandachtspunt voor het vervolgonderzoek van de onderzoekscommissie.

Andere aandachtspunten voor het vervolgonderzoek, gericht op de lekvraag, zijn kort samengevat:

- Zo mogelijk controleren van de informatie van de informant en het vaststellen van de betrouwbaarheid van de informant;
- Verkrijgen en bestudering van andere 'bewijsstukken' zoals de uitgelekte emails die heer Klaver in zijn bezit zou hebben en waaruit zou blijken dat het Dagblad van het Noorden een hooggeplaatste bestuurder uit de wind zou willen houden;
- Vaststellen door middel van interviews van de motieven voor mevrouw Haarsma en haar communicatieadviseur om actief de pers op te zoeken (benaderen van de heer De Bruin) om te praten over een op dat moment nog vertrouwelijk rapport;
- Bestudering van de verschillen tussen de concept versie van het rapport en de definitieve versie van het rapport;
- Bestudering van de verschillen tussen de concept versie van het rapport die de advocaat in zijn bezit heeft gehad in het kader van hoor en wederhoor en de andere versies van het rapport;
- Bestudering van verslag van PS bijeenkomst op 12 november 2008 waarin geheimhouding over rapport Eurochamp zou zijn opgelegd

Naast bovengenoemde aandachtspunten, dient er in het vervolgonderzoek ook nadrukkelijk te worden stilgestaan bij de beantwoording van de tweede en derde onderzoeksvraag:

- waren er bij de provincie Drenthe organisatorische en/of 'bestuurlijk-culturele' factoren die de voortijdige verspreiding hebben bevorderd?
- in hoeverre moet het gevoerde bestuur worden aangepast om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen?

Voor de beantwoording van deze vragen, dienen - naast de bestudering van de relevante documenten (zie hoofdstuk 4)- in de interviews vragen te worden gesteld aan zowel bestuurders als ambtenaren over zaken als:

- Hoe worden contacten met journalisten onderhouden?
- Is men op de hoogte van wet- en regelgeving op dit gebied?
- Wordt er in werkoverleggen en in GS/PS bijeenkomsten stilgestaan bij onderwerpen als contacten met de pers, informatiebeveiliging, vertrouwelijkheid van documenten?
- Hoe wordt het afleggen van de eed/gelofte door werknemers ervaren?
- Leeft integriteit als onderwerp binnen de provincie?
- Waaruit blijkt dat, welke concrete aandacht krijgt het?
- Wat zou er volgens de mening van betrokkenen dienen te veranderen om het risico van nieuwe incidenten te beperken?

8 Tot slot

Wij vertrouwen hiermede aan het eerste deel van onze opdracht te hebben voldaan.

Hoogachtend,

[redacted]
Directeur

BIJLAGE I:

Lijst van geraadpleegde documenten

1. KPMG rapport, Onderzoek naar mogelijke voortijdige verspreiding rapport Eurochamp, 10 maart 2009.
2. Schriftelijke weergave debat in PS op 18 maart 2009.
3. Reglement gebruik bedrijfsmiddelen (2006)
4. Uitvoeringsprogramma Drenthe (2006-2007), Welkom in digitaal Drenthe.
5. Beleidskader informatiebeveiliging provincie Drenthe (februari 2009), Veilig, integer en vertrouwd, hoe is onze informatie beveiligd?
6. Basisnorm maatregelen informatiebeveiliging (bijlage bij beleidskader informatiebeveiliging).
7. Handboek informatiebeveiliging (2005).
8. Diverse functiebeschrijvingen.
9. Gedragscode ambtelijke integriteit (maart 2003, laatste update 10 oktober 2008).
10. Drentse gedragscode integriteit voor de CvdK, GS en PS.
11. Organogram Provincie Drenthe.
12. Organisatiebesluit Provincie Drenthe 2008.
13. Meer samen, nóg sterker, Besturings- en managementconcept, oktober 2007.
14. *Het rapport over de opkomst en ondergang van Eurochamp*, Dagblad van het Noorden, 15 november 2008, door Gerard de Kleine en Martin de Bruin
15. *Advocaat: Jan heeft geen strafbare feiten begaan,* Dagblad van het Noorden, 15 november 2008.
16. *J'accuse!,* column van Denker (bronvermelding...)

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
26 juni 2009

Aanwezig: Leo Bomhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester, [redacted] (BING)
Inge Rozema (secretaris).
Afwezig: [redacted] (BING)

1. Tweede concept van het rapport

De secretaris legt bijlage 6 met de opsomming van geïnterviewden en gehoorden voor aan de commissie ter goedkeuring. De commissie gaat daar mee akkoord.
De voorzitter heeft het voorwoord drastisch aangepast. Er worden nog enkele wijzigingen in aangebracht.
Het rapport wordt pagina voor pagina doorgelopen. Sietze de Jong wil graag bij de procesbeschrijving over de aanlevering van gegevens een sterkere formulering. Het was te laat en te traag en er was weinig gevoel voor urgentie. En hij blijft van mening, dat de commissie niet alles te zien heeft gekregen. Afgesproken wordt, dat de tekst mbt de aanlevering van gegevens nog wordt aangevuld.
Herman Beerda en Gea Smith vinden dat er iets moet worden opgeschreven over de interventies van buiten. De voorzitter meent, dat je dan al snel uit de school klapt als commissie. Hij stelt voor om in algemene bewoordingen er iets van te zeggen tijdens de mondelinge toelichting in PS op 2 juli. In tweede instantie, als er door leden van PS op door wordt gevraagd, kan hij zonodig meer in detail treden en man en paard noemen. Maar niet op papier.
Daar kunnen de anderen mee leven.

Over de passages mbt de telefoontjes tussen gedeputeerden en journalisten, inclusief aantallen en tijdstippen, vindt discussie plaats. Afgesproken wordt, dat in de reconstructie van dag tot dag wel wordt aangegeven wie met wie belde en hoe vaak. Maar in de samenvattende passage in paragraaf 3.6 kan niet over totalen worden gesproken, vindt de voorzitter. Dat was de afspraak bij het inzien van de telefoonlijsten. Het ging om het aangeven van trends, en dat kan de commissie nu dus doen. De voorzitter stelt voor om de tekst van zijn mail te gebruiken voor deze passage.
Sietze de Jong wil weten hoe het zit met de verschillen tussen de 10 telefoontjes in de concept-tekst en de aantallen waarover de voorzitter rept in zijn mail. De voorzitter geeft aan, dat het gaat om de gesprekken die daadwerkelijk inhoud hebben gehad, gezien de lengte van het contact. Van sommige is duidelijk, dat er geen contact tot stand is gekomen. [redacted] meent, dat de gegevens waarover de commissie nu beschikt voldoende zijn om over te kunnen rapporteren.
Afgesproken wordt, dat de secretaris een nieuw tekstvoorstel maakt voor de passage in paragraaf 3.6 en dat aan de leden rondmailt voor toetsing.

[redacted] zal naar aanleiding van een memo van Andries Visser over de relatie tussen het Handboek informatiebeveiliging en het Reglement bedrijfsmiddelen nog nagaan of dat consequenties heeft voor teksten. Hij zal aanvullingen aan de secretaris doorgeven.

De secretaris zal de overige wijzigingen doorvoeren en de eindredactie plegen. Alleen paragraaf 3.6 wordt nog rondgezonden aan de commissie. De definitieve versie niet meer.

2. Verslag van 24 juni 2009
Het verslag wordt ongewijzigd vastgesteld.
De voorzitter meldt, dat hij heeft gesproken met de DS n.a.v. haar briefje over het proces in en rond de hoorzittingen. Ze had o.a. kritiek op de wijze van vraagstelling, omdat de commissie daarin al conclusies formuleerde. De voorzitter heeft dit met haar uitgepraat en de zaak kan als afgedaan worden beschouwd.

3. Overzicht van kosten
BING heeft een urenverantwoording ingediend, die duidt op een behoorlijke kostenoverschrijding. Desgevraagd geeft [redacted] aan, dat de uiteindelijke rekening zal oplopen tot 80.000,- euro. De commissie wil graag weten wat daarvan de oorzaken zijn en meent, dat dit toch wel eerder had kunnen worden gemeld. Nu valt er niet veel meer van te vinden.
[redacted] geeft aan, dat er meer vergaderingen en meer interviews hebben plaatsgevonden dan gedacht. Ook het technische onderzoek was diepgaander dan tevoren nodig leek. De extra IT-kosten zijn echter al in een eerder stadium goedgekeurd. De overschrijding zit met name in de uren van [redacted] (ca. 90 uren extra). [redacted] geeft toe, dat BING daar wel eerder mee had moeten komen, maar er zat veel druk op het hele proces.
Afgesproken wordt, dat BING op korte termijn een duidelijke onderbouwing levert voor de oorzaken van de overschrijding. In het statenstuk voor PS zal de overschrijding worden gemeld.

De commissie is niet te spreken over de declaratie van KPMG. [redacted] De rekening is al betaald, maar de commissie wil toch een brief aan KPMG laten sturen om haar ongenoegen te laten blijken. De secretaris zal een concept-brief opstellen.

De declaratie van Van Luyn is akkoord.

4. Statenstuk 2009-390
De commissie kan zich vinden in het statenstuk en de voor te leggen besluiten aan PS. De geheimhouding wordt opgelegd mbt alle stukken in het dossier van de commissie waar het stempel 'vertrouwelijk' op staat.

5. Persconferentie en persbericht
Het persbericht is veel te lang en dient nog op vele punten te worden aangepast. De voorzitter stelt voor om teksten uit zijn voorwoord te gebruiken. Kwalificaties en terminologie moeten strikt sporen met de teksten in het rapport. Het persbericht wordt aangepast door SietzeJan Boer en daarna opnieuw rondgestuurd binnen de commissie *(NB: de voorzitter heeft aanpassing van het persbericht zelf ter hand genomen en rondgemaild, IR).*

De voltallige commissie is aanwezig op de persconferentie. De voorzitter zal het woord voeren. Hij zal daarin niet reageren op de artikelen van de hoofdredacteur van het DvhN. Daar staat de commissie boven.

De commissie dient om 9.15 aanwezig te zijn (0.19). Na afloop wil de voorzitter nog even kort met de commissie bijeen komen in 0.07.

6. Behandeling in PS op 2 juli a.s.
Zoals afgesproken zal de voorzitter hier wel ingaan op de hinder die de commissie heeft gehad van externe interventies.
Als er heel veel vragen komen vanuit de staten aan het adres van de commissie, dan wil de voorzitter eventueel een schorsing vragen om te kunnen overleggen met de commissie.

IR/ 29-06-09

5

KPMG Forensic
Postbus 74555
1070 DC Amsterdam

Burg. Rijnderslaan 10-20
1185 MC Amstelveen

Persoonlijk en Vertrouwelijk
Provincie Drenthe
Mevrouw I. Rozema
Griffier Proviniale Staten Drenthe
Postbus 122
9400 AC ASSEN

Amstelveen, 2 juni 2009

Declaratie Nummer AVNK00069311

(in Euro)

Declaratie voor kosten briefings conform toegezonden specificatie.

Honorarium	5.118,00
Reis, verblijf- en secretariaatskosten	465,00
Subtotaal	5.583,00
19 % BTW over 5.583,00	1.060,77
Totaal	6.643,77

Wij verzoeken u bovenstaand bedrag binnen 15 dagen te voldoen onder vermelding van declaratienummer AVNK00069311.

KOPIE

Ref.: FAPRD9[redacted]/MN/al

405

Datum binnenkomst	05 juni 2009
Boekstuknummer	2009 7577
Leveranciersnr.	
Team / behandelaar	SG. 700 954 L. Jeuring
Inkooporder nr.	

Projectgegevens *Alleen invullen bij geen inkooporder nummer*

Project	Taak	Kostensoort	Bedrag excl. btw
33000010	05	423184	5583,-

Grootboekgegevens *Alleen bij kostenplaatsen*

Prestatie	Kostensoort	Bedrag excl. btw

Omschrijving in adm.

Paraaf proj.leider | Paraaf budgethouder 11/6

Voor vragen met betrekking tot deze declaratie kunt u contact opnemen met onze centrale afdeling Credit Control.
Telefoon: 020 656 7676, fax: 020 656 7999, e-mail: creditcontrol@kpmg.nl

Bankrekeningen t.n.v. KPMG N.V.

Rabobank (Swift Code RABONL2U)	36.42.31.912
ABN AMRO Bank	54.03.33.859
Fortis Bank	83.19.58.162
ING Bank	69.64.60.149
BTW-nr	NL8034.17.597.B.01

KPMG Forensic
Postbus 74555
1070 DC Amsterdam

Burg. Rijnderslaan 10-20
1185 MC Amstelveen

Persoonlijk en Vertrouwelijk
Provincie Drenthe
Mevrouw I. Rozema
Griffier Proviniale Staten Drenthe
Postbus 122
9400 AC ASSEN

Amstelveen, 2 juni 2009

Declaratie Nummer AVNK00069311

(in Euro)

Declaratie voor kosten briefings conform toegezonden specificatie.	
Honorarium	5.118,00
Reis, verblijf- en secretariaatskosten	465,00
Subtotaal	5.583,00
19 % BTW over 5.583,00	1.060,77
Totaal	6.643,77

Wij verzoeken u bovenstaand bedrag binnen 15 dagen te voldoen onder vermelding van declaratienummer **AVNK00069311**

Ref.: FAPRD9[redacted]/MN/al

Voor vragen met betrekking tot deze declaratie kunt u contact opnemen met onze centrale afdeling Credit Control.
Telefoon: 020 656 7676, fax: 020 656 7999, e-mail: creditcontrol@kpmg.nl

Bankrekeningen t.n.v. KPMG N.V.

Rabobank (Swift Code RABONL2U)	36.42.31.912
ABN AMRO Bank	54.03.33.859
Fortis Bank	83.19.58.162
ING Bank	69.64.60.149
BTW-nr	NL8034.17.597.B.01

KPMG Forensic
Postbus 74555
1070 DC Amsterdam

Burg. Rijnderslaan 10-20
1185 MC Amstelveen

Uren en kosten specificatie briefings BING, Onderzoekscommissie en ovedracht digitale gegevens

KPMG Forensic

	[redacted]	[redacted]	IT-medewerkers	Uren	Bedrag
	Ass. Director	Manager	Adviseur		
Rate	*425*	*265*	*180*		
Briefings en diversen contacten BING	3,5	7,0		10,5	3.343
Overdracht digitale gegevens	0,5	2,5	5,0	8,0	1.775
Subtotaal	4,0	9,5	5,0	18,50	5.118
Reis, Verblijf en Secretariaatskosten					465
Totaal					5.583

Bankrekeningen t.n.v. KPMG N.V.

Rabobank	36.42.31.912
(Swift Code RABONL2U)	
ABN AMRO Bank	54.03.33.859
Fortis Bank	83.19.58.162
ING Bank	69.64.60.149

Voor vragen met betrekking tot deze declaratie kunt u contact opnemen met onze centrale afdeling Credit Control
Telefoon: 020 656 7676, fax: 020 656 7999, e-mail: creditcontrol@kpmg.nl

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
24 juni 2009

Aanwezig: Leo Bomhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester, [redacted] (BING), [redacted] (BING), [redacted] (SG/BC);
Inge Rozema (secretaris).

1. Mededelingen

De voorzitter stelt aan de orde de ingekomen brief van mevrouw Klip inzake het verslag van haar verhoor. De secretaris heeft de passage op blz. 4 nog nageluisterd en de weergave zoals die er oorspronkelijk stond klopt met wat ze heeft gezegd. Wel moeten de woorden "....in de slipstream van (een gesprek).." er nog tussen gevoegd worden. De voorzitter stelt voor om haar dit in een reactie te melden en ook aan te geven dat de commissie kennis neemt van haar overige aanvullende opmerkingen, maar daar nu niets meer mee kan. Als zij dat wil kan ze in de PS-vergadering van 2 juli een nadere toelichting geven.

De voorzitter en de secretaris hebben bij de CdK de telefoonlijsten bekeken van de dames Haarsma en Klip in de week vóór en de week ná 10-14 november. Daaruit bleek, dat de frequentie van telefoontjes van Klip met De Kleine in al die weken even groot was en dat Haarsma in de week ervoor niet met Martin de Bruin heeft gebeld, maar in de week erna ongeveer net zo vaak als in de lekweek. De voorzitter heeft de commissie hierover een mail gestuurd. Meer kan hij er om privacyredenen niet over zeggen.
Sietze de Jong is het er niet mee eens, dat er geen nader inzicht mag zijn in deze gegevens. Want het maakt nogal wat uit, of die hoge frequentie zich concentreert op 1 of 2 dagen of dat het gespreid over de hele week plaatsvindt. De voorzitter geeft aan, dat er elke dag zo'n beetje evenveel werd gebeld. [redacted] meent, dat de nu meegedeelde gegevens wat hem betreft voldoende zijn voor de rapportage.
Gea Smith begrijpt de onvrede van Sietze de Jong, maar deelt die niet. Wel heeft zij achteraf gezien het idee, dat de commissie in de hoorzittingen meer had door kunnen vragen. Margriet Stijkel beaamt dat. De voorzitter is het daar niet mee eens. Hij meent, dat op de cruciale punten voldoende is doorgevraagd.

De directeur-secretaris heeft een briefje aan de voorzitter geschreven met opmerkingen over het proces rond de verhoren. De voorzitter heeft dit nog niet goed kunnen lezen. Hij zal daar vrijdag a.s. in de commissie op terugkomen.

2. Vaststelling agenda
Agendapunt 4 (begroting en kosten) wordt doorgeschoven naar vrijdag 26 juni

3. Verslagen van 12, 17 en 18 juni 2009
De verslagen van 12 en 17 juni worden ongewijzigd vastgesteld. In het verslag van 18 juni wordt bij het punt Rondvraag nog toegevoegd, dat Sietze de Jong en Margriet Stijkel eveneens vinden dat een openbaar verhoor van De Kleine nog moet kunnen plaatsvinden.

5. Eerste concept van het rapport
Ko Vester heeft aarzelingen bij de titel. Het accent wordt op deze manier te zeer op het vinden van het lek gelegd en niet op de andere onderzoeksvragen. De voorzitter meent, dat een pakkende titel nodig is, en dat het onderzoek in de optiek van de buitenwacht toch vooral hierover gaat.

Algemeen: alle leden zijn vol lof over de vlotte leesbaarheid, de compleetheid, structuur en duidelijkheid van dit concept. Herman Beerda heeft wel kanttekeningen m.b.t. de conclusies. Die sporen niet altijd met wat we hebben gezien en zijn te weinig onderbouwd. Soms suggestief. Hij noemt enkele voorbeelden. Gea Smith vraagt zich af of die niet ingegeven zijn door politieke motieven? Herman Beerda meent van niet. Het gaat hem om de evenwichtigheid in het verhaal en om een adequate onderbouwing van uitspraken.
Hij blijft de verhouding tussen de eerste onderzoeksvraag en de rest scheef vinden, maar zo is het onderzoek nu eenmaal verlopen, dus als je dat in het rapport terugziet, is dat begrijpelijk.

Met betrekking tot de bijlagen vraagt Herman Beerda zich af of het advies van Elzinga er niet bij moet. De voorzitter meent van niet, omdat dit een advies aan PS was, op grond waarvan ook de onderzoeksvragen zijn aangepast. Ook Sietze de Jong vindt dat nu mosterd na de maaltijd. Gea Smith meent, dat het er wel bij hoort juist vanwege de invloed op de onderzoeksvraag.
[redacted] adviseert het niet te doen, omdat dat weer discussies kan uitlokken, die de aandacht van het rapport afleiden. Conclusie: het advies van Alzinga wordt niet als bijlage bijgevoegd
Het KPMG-rapport dient wel als bijlage te worden toegevoegd, om het geheel compleet te maken. De lijst met geïnterviewden en de lijst met gebruikte documenten wordt niet toegevoegd. Wel de lijst met gehoorde getuigen. De secretaris zal voor de bijlagen zorgdragen.

Het rapport wordt pagina voor pagina doorgenomen en van commentaar voorzien. Punten en komma's en taal- en typfouten zullen door de secretaris in de eindversie worden verbeterd.
De voorzitter zal zich nog buigen over het voorwoord.

De rapportage van Fox-IT over de technische gegevens, waarnaar wordt verwezen, is een vertrouwelijk rapport en zal nog vóór de vergadering van vrijdag aan de leden van de commissie worden toegezonden.

KPMG zal dinsdagochtend worden gebeld door de secretaris om ze te melden dat ons rapport openbaar wordt gemaakt die ochtend. Dan zijn ze geprepareerd op eventuele reacties.

6. Afspraken volgende vergadering
De volgende (en laatste) vergadering is **op 26 juni van 10.00 – 13.00 uur**.
Aan de orde is dan:

- Het kostenoverzicht en onderliggende facturen.
- Het tweede concept van het eindrapport ter definitieve vaststelling.
- De voorbereiding van de persconferentie en vaststelling van het persbericht.
- Het statenstuk bij het eindrapport.

- De bespreking in de fracties en de rol van de commissieleden daarbij.
- De mate van openbaarheid van (delen) van het onderzoeksdossier.

Openstaande afspraken

Datum afspraak	**Inhoud afspraak**	**realisatie**
24/6	De secretaris zorgt voor de bijlagen bij het rapport	26/6
24/6	BING zend het technische rapport vóór vrijdag aan de commissie	25/6
24/6	De secretaris voert de eindredactie (taaltechnisch) op het eindrapport	28/6
24/6	De secretaris belt dinsdag met KPMG om ze te attenderen op publicatie van ons rapport	30/6
24/6	[redacted] maakt een concept-persbericht	25/6

IR/ 25-06-09

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
18 juni 2009

Aanwezig: Leo Bomhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester, [redacted] (BING), [redacted] (SG/BC);
Inge Rozema (secretaris).
Afwezig: [redacted] (BING)

1. Mededelingen

Sietze de Jong meldt ongelukkig te zijn met de interventies van Henk Klaver. Maar hij is ook teleurgesteld in de commissie. Doen we nu echt aan waarheidsvinding? Halen we echt de onderste steen boven? Hebben we echt alle feiten gekregen? De gegevens zijn te laat aangeleverd. Dat heeft ons onder onnodige tijdsdruk gezet en belemmert ons in kwalitatief goed werken. Hij voelt zich soms als een roepende in de woestijn.
Leo Bomhof meent dat de commissie er alles aan heeft gedaan om te krijgen wat we hebben willen aan informatie. Hij zou niet weten hoe het anders had gemoeten.
Ge Smith vindt, dat de commissie goed bezig is. We doen aan waarheidsvinding, daarvan is ze overtuigd. Maar wel volgens de regels die gelden. En dat beperkt de commissie soms.
Margriet Stijkel sluit zich hierbij aan.
Herman Beerda meent, dat de informatie die we nu nog niet hebben, geen essentiële gegevens zijn, die iets zouden kunnen toevoegen. En sommige gegevens zijn er helaas gewoonweg niet (meer).
Ko Vester bewondert de diepgravendheid waarmee Sietze zich in het onderzoek heeft gestort. Maar hij is nog niet zover om te concluderen, dat we onvoldoende gegevens hebben om een kwalitatief goed rapport af te leveren.
[redacted] vindt als adviseur, dat de commissie op basis van deze gegevens een prima rapport kan schrijven.
Na enige verdere discussie concludeert de commissie, dat we veel gegevens te laat hebben gekregen, maar dat de verkregen informatie wel volledig was op grond van hetgeen we hebben gevraagd.

M.b.t. de reactie van Henk Klaver op de mail van de commissiesecretaris aan hem, m.b.t. terughoudendheid ten opzichte van de commissie: het gesprek met Ko Vester, waar Klaver op doelt, heeft wel plaatsgevonden, maar is op geen enkele wijze over de inhoud van het werk van de commissie gegaan. Alleen maar enkele opmerkingen, dat het wel veel werk was en dat de commissie het druk heeft. Dit benadrukt Ko Vester ten stelligste.
Dat Tanja Klip wist, dat zij door Margriet Stijkel zou worden bevraagd was geen geheim, want die lijst is voorafgaand aan de hoorzittingen al verspreid.

Margriet Benak heeft eerst Sietze de Jong gebeld en daarna met Leo Bomhof, met de vraag of de commissie wel aan waarheidsvinding doet. Leo Bomhof heeft uiteraard aangegeven, dat dat natuurlijk het geval is. En hij heeft haar verzocht om de commissie nou even met rust te laten, zodat ze haar werk gewoon kan afronden.

Dergelijke vragen en reacties wijzen erop, dat in het debat op 2 juli de schijnwerpers wel eens heel snel op de commissie zelf kunnen worden gericht, in plaats van op haar rapport. De werkwijze van de commissie en de degelijkheid van haar onderzoek kunnen ter discussie komen te staan.
Herman Beerda heeft het ongemakkelijke gevoel, dat er een campagne is gestart om de leden van de commissie in een verkeerd daglicht te stellen. Ook bij de CdK komen nota bene signalen binnen, dat wij ons werk niet goed doen. Hoe kunnen we ons daar nu tegen verweren?
Leo Bomhof meent, dat we dit gewoon langs ons heen moeten laten glijden. We moeten ons er in het geheel niet door laten beïnvloeden en er al helemaal niet op reageren. De commissie is een onafhankelijk, zelfstandig orgaan en zo moeten we ons blijven opstellen. Hij zal als voorzitter in het debat van 2 juli de criticasters van repliek dienen. Een beroep doen op de steun of 'bescherming' van de CdK, zoals wordt gesuggereerd, past daar niet bij. De CdK moet straks als voorzitter van PS tijdens het debat boven de partijen kunnen blijven staan.

Wel wordt afgesproken, dat Leo Bomhof en Herman Beerda gezamenlijk e.e.a. aan Tichelaar zullen melden, uitsluitend met als doel om hem op de hoogte te doen zijn.

Sietze de Jong heeft sterk de neiging om samen met Joma Kaal aan Klaver te melden, dat hij zich er verder niet meer mee moet bemoeien. Leo Bomhof meent, dat Sietze de Jong dat wat hem betreft best kan doen.

De secretaris meldt, dat zij n.a.v. de sms aan Gerard de Kleine namens de commissie, met hem telefonisch contact heeft gehad. Hij meldde, dat hij vond, dat Tanja Klip zelf de kans moest krijgen om haar uitspraken over de telefoontjes met De Kleine nader toe te lichten (en deels te herroepen). Er is in de 'slipstream van die privé-gesprekken' (zoals Tanja Klip het aanduidde) wèl inhoudelijk over het dossier gesproken, zegt De Kleine. Maar hij wil dat niet zelf in het openbaar aan de orde stellen, omdat hij met haar bevriend is.
De secretaris heeft dit aan de voorzitter gemeld. Hij heeft voorgesteld om De Kleine de suggestie aan de hand te doen, om Tanja Klip dan maar zelf te overreden om haar verklaring aan te vullen. Tevens moet de boodschap helder zijn, dat een besloten interview of verhoor niet aan de orde is, omdat de commissie daar niets mee kan. De secretaris heeft dit per sms weer overgebracht aan De Kleine.
Letterlijke tekst:
"Gerard, heb je dilemma afgestemd met cievz. Cie. begrijpt dit. Toch wil ze je niet besloten horen. Ze houdt je hartenkreet mbt Klip in het achterhoofd. Ze raadt je aan zelf met Klip contact te zoeken en haar te bewegen in PS-vergadering alsnog in te gaan op haar uitspraken over de 'slipstream'.
Vrgr, Inge"
De reactie van De Kleine per sms was vervolgens: *"Inge, helder, denk na over je waardevolle suggestie"*. Daarna heeft hij niet meer van zich laten horen.

Tijdens de vergadering belt Joma Kaal met Sietze de Jong met de mededeling, dat Henk Klaver haar heeft gezegd, dat de informant wel in een besloten zitting onder ede wil worden gehoord, en dat het verslag vervolgens mag worden gebruikt door de commissie voor het rapport.
De commissie is ontstemd over het feit, dat nu wéér via de lijn van Klaver wordt geïntervenieerd. Als De Kleine wat wil, dan dient hij zelf contact op te nemen met de commissie(secretaris). De voorzitter is bovendien heel stelling in de afwijzing van een besloten hoorzitting: hij kan het niet verantwoorden, waarom deze man besloten zou moeten worden gehoord.

3. Verslagen van 12 en 17 juni 2009
Deze worden doorgeschoven naar de volgende vergadering (24 juni).

4. Eerste verkenning conclusies en aanbevelingen
Na enige discussie is een belangrijke conclusie van de commissie, dat het aannemelijk is, dat het rapport (een kopie van de digitale definitieve versie) vanuit het provinciehuis naar buiten is gekomen, hoewel de theoretische mogelijkheid bestaat, dat dit door anderen (bv. Deloitte) is gedaan.

In het rapport zal duidelijkheid moeten worden gegeven over het hoe en waarom van de actie van [redacted] om met spoed een digitale versie te laten komen. Dat wekte in de staten van 18 maart argwaan op. Dit kan de commissie nader verklaren.

Voorts zal er iets moeten worden gezegd over de onvolledigheid van het KPMG-onderzoek.

Met betrekking tot de tweede onderzoeksvraag is het opmerkelijk te noemen, dat er toch veel rechtstreekse contacten plaats vinden tussen gedeputeerden en journalisten, zonder tussenkomst van de bestuursadviseur. Een aanbeveling zou kunnen zijn, om dat wel vaker via de geijkte wegen (de bestuursadviseurs) te laten verlopen.

[redacted] is al begonnen met schrijven. Hij denkt op basis van deze eerste verkenning een goede voorzet voor een eerste versie te kunnen maken. Die komt op dinsdag 23 juni naar de leden van de commissie toe. Indien de leden ondertussen nog nadere ideeën en suggesties hebben voor het rapport, dan kunnen die via de secretaris worden aangedragen.

7. Afspraken volgende vergadering
De volgende vergadering is **op 24 juni van 13.00 – 15.00 uur**.

De bespreking van de facturen van KPMG en Van Luyn is dan aan de orde. Evenals de urenverantwoording van BING t/m 12 juni.

Het eerste concept van het eindrapport zal dinsdag aan de leden worden gemaild door [redacted] Dit wordt dan in de vergadering van 24 juni besproken.

8. Rondvraag
De secretaris vraagt wat zij moet doen als Gerard de Kleine haar alsnog belt met het verzoek om een interview of verhoor. De commissie vindt in meerderheid, dat zijn beurt nu voorbij is. Ko Vester en Gea Smith vinden dat een openbaar verhoor nog tot de mogelijkheden moet kunnen behoren. De voorzitter is van oordeel, dat dat formeel nu niet meer kan: de hoorzitting is aangekondigd tot 18 juni 12.00 uur. Dat tijdstip is al gepasseerd.

Sietze en Margriet ook

IR/ 19-06-09

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de ingelaste bespreking
op 17 juni 2009

Aanwezig: Leo Bomhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester ;
Inge Rozema (secretaris).
Afwezig: [redacted] (BING)

De commissie is bijeen naar aanleiding van gebeurtenissen van de avond daarvoor. Sietze de Jong is gebeld door Henk Klaver met de volgende mededelingen:

- de informant heeft in een eerder stadium anderhalf uur met Leo Bomhof aan diens keukentafel in Zeijen gesproken.
- de informant wil nu toch met de commissie praten, naar aanleiding van de verhoren van die dag;
- de informant is inmiddels weer in dienst van zijn werkgever.

Sietze de Jong heeft daarover eerst met [redacted] en vervolgens met Inge Rozema contact gelegd. Daarna op hun advies ook met Leo Bomhof. Hij heeft aan Klaver het 06-nummer van de secretaris doorgegeven t.b.v. de informant als hij contact wil zoeken met de commissie. Klaver bevestigt per sms aan de secretaris, dat 'Gerard' haar de volgende ochtend zal bellen.

Sietze de Jong heeft woensdagochtend ook de andere leden van de commissie ingelicht over het bovenstaande telefoontje van Klaver.

Leo Bomhof geeft aan dat hij boos is over het feit, dat Sietze de Jong met de informatie niet meteen naar hemzelf is gekomen, maar eerst Kooman en de secretaris daarover heeft gebeld. Hij is ook ontstemd over het feit, dat Henk Klaver opnieuw intervenieert in het werk van de commissie. Als deze iets te melden heeft moet hij trouwens met Leo zelf contact opnemen en niet Sietze de Jong daarvoor gebruiken.

Sietze de Jong geeft aan er bewust voor gekozen te hebben om niet eerst met Leo Bomhof te bellen. De informatie betrof immers Leo zelf. Daar wilde hij eerst met anderen over klankborden. In combinatie met het gegeven, dat Leo afgelopen weekend ook contact heeft gehad met Tanja Klip (over de telecom-gegevens) zit e.e.a. hem niet lekker.
Margriet Stijkel vond het ook opvallend, dat Tanja Klip gisteren op de hoogte was dat de commissie over de telefoontjes met De Kleine vragen zou stellen.

Herman Beerda vraagt zich af of nu wordt gesuggereerd, dat Leo haar zou hebben ingelicht? De aanwezigen benadrukken stellig van niet.
Herman Beerda licht nogmaals toe, hoe die contacten met Haarsma en Klip afgelopen weekend zijn gelopen, nadat bleek dat Tichelaar niet bereikbaar was. We hadden toch juist afgesproken, dat we betrokkenen wel zouden inlichten over de telecom-bevindingen, om ze niet plots in het openbaar ermee te confronteren. De andere leden zijn het daarmee eens. Het was wellicht beter geweest, als Beerda met Klip had gebeld en Bomhof met Haarsma.

Leo Bomhof stelt de vertrouwensvraag. Hij wil weten of hij als voorzitter wel het vertrouwen geniet van de rest van de commissie. De commissie bevestigt dat het vertrouwen niet is geschonden.

Herman Beerda vindt, dat Sietze de Jong Henk Klaver had moeten afkappen zodra hij begreep, dat het over Eurochamp ging en niet over andere zaken. Sietze moet zichzelf niet in de positie van boodschapper brengen.

De commissie concludeert dat de heer Klaver uitsluitend contact kan hebben met de voorzitter of de secretaris, indien hij iets aan de commissie kwijt wil. De secretaris zal hem daarover een duidelijke mail sturen *(is gebeurd. Er is ook al antwoord binnen gekomen, IR)*

Voor alle duidelijkheid bevestigt Leo Bomhof nogmaals, dat hij geen inhoudelijk gesprek heeft gehad met Gerard de Kleine (noch met de informant) en zeker niet bij hem thuis.

Herman Beerda spreekt zijn ongenoegen uit over het gebeurde. Hij wordt bevestigd in zijn eerder geuite vermoeden, dat er aan de poten van de commissie wordt gezaagd. Hij vindt dat daarover iets moet worden gezegd in het rapport.

De vraag ligt nu voor hoe de commissie gaat reageren op de melding van De Kleine, dat hij een verklaring wil afleggen.
Beerda voelt er weinig voor. Hij heeft diverse kansen gehad, zowel als informant, als in de hoedanigheid van journalist van DvhN. We hebben hem aangeboden eventueel alleen in vertrouwen met BING te praten, we hebben hem uitgenodigd voor een interview en voor een verhoor. Dat heeft hij steeds afgehouden.
We hebben al eerder afgesproken, dat zijn anonimiteit als informant voor de commissie niet werkbaar zou zijn, net zoals KPMG daar last van had.
Gea Smith zou hem wel willen interviewen, maar dan op dezelfde wijze als de andere betrokkenen. En daarna een openbare hoorzitting.

Ondertussen komt een sms van De Kleine binnen voor de secretaris: hij zal niet verschijnen voor de commissie maar vraagt de commissie om mevrouw Klip nogmaals te bevragen op een concreet onderdeel van haar getuigenis (mbt de week van 17-22 november).

De commissie concludeert, dat zij met zo'n bericht niks kan. We doen daar dus niets mee. De secretaris zal de heer De Kleine melden, dat hij welkom is voor een interview (conform de werkwijze bij andere betrokkenen) en eventueel een openbaar verhoor. Wil hij dat niet, dan niet. *(bericht is aan De Kleine gestuurd (via sms). Hij heeft aangegeven niet in het openbaar te willen worden gehoord, IR).*

ONDERZOEKSCOMMISSIE EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG van de vergadering van 12 juni 2009

Aanwezig: Leo Bomhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester, [redacted] (BING);
Inge Rozema (secretaris).
Afwezig: [redacted] (BING)

1. Mededelingen

De secretaris meldt, dat de heer De Kleine haar die ochtend heeft gebeld, met de mededeling, dat hij zijn komst op de hoorzitting nog in beraad houdt. Hij zal daar uiterlijk woensdag op terugkomen.
De heer De Jong meldt, dat zijn fractievoorzitter hem heeft medegedeeld, dat de informant met De Jong zou willen praten. Dit heeft hij meteen doorgegeven aan de voorzitter en de heer Kooman. Hij is van oordeel, dat alleen de commissie als geheel met de informant kan praten.
De heer Bomhof wijst op het risico als de informant door de commissie in beslotenheid wordt gehoord. Als zijn anonimiteit blijvend gewaarborgd moet worden, schiet de commissie daar niets mee op in haar rapportage. Daar heeft KPMG ook last van gehad. Het is beter om de kaarten te zetten op De Kleine (er op hopend dat die als getuige op de hoorzitting wil verschijnen).
De heer Beerda krijgt het gevoel, dat er wordt gezaagd aan de poten van de commissie. Daar moeten we op bedacht zijn.
Conclusie:
De heer De Jong meldt (via de heer Klaver) aan de informant, dat hij niet als enige met hem wil spreken. Hij doet verder geen suggesties voor alternatieve mogelijkheden.

3. Verslag van 10 juni 2009

Het verslag wordt goedgekeurd, onder voorbehoud van nog een check door BING op correcte weergave van de technische bevindingen onder punt 4.
Naar aanleiding van het verslag : de heer Baas heeft toestemming gegeven voor gebruik van het verslag van zijn interview t.b.v. de rapportage.

4. Bevindingen mobiele telefonie gegevens

[redacted] zal alle gegevens over wie wanneer met wie heeft gebeld vermelden in de vragendossiers t.b.v. de verhoren. Opmerkelijke bevindingen zijn:
- gedeputeerde Klip heeft in de week van 10-14 november meerdere malen met De Kleine gebeld, soms drie keer per dag. O.a. ook na afloop van het Spaanse buffet. Zij heeft daarover in het interview niets gezegd.
- gedeputeerde Haarsma heeft met De Bruin gebeld na afloop van de GS-vergadering op dinsdag 11/11, maar vóór de persbriefing die middag.
- communicatieadviseur Van den Bosch belt die week slechts één maal met De Bruin.

De vraag ligt voor hoe we de betrokkenen met deze nieuwe gegevens confronteren. Plompverloren in de openbare verhoren, of wellicht nog tevoren?
De voorzitter stelt voor om hen er tevoren nog eens goed op te wijzen, dat ze bij zichzelf zorgvuldig moeten nagaan met wie ze zoal contact hebben gehad in die week. De voorzitter zal die boodschap via de CdK laten verlopen. Dat geldt dus zowel richting gedeputeerden als richting ambtenaren.

5. Voorbereiding hoorzitting
De vragenlijsten worden doorgenomen.
Bij de besloten zittingen is de inhoud van de verslagen geheim, conform de verordening. De voorzitter en enkele andere leden van de commissie vinden dat dit onvoldoende duidelijk is geweest. Anders hadden zij niet in besloten zittingen bewilligd. De commissie besluit om de getuigen te vragen toestemming te geven voor gebruik van hun verklaringen in het rapport.

De informatie uit de besloten interviews kan in het algemeen worden gebruikt, maar de commissie kan niet letterlijk naar deze verslagen verwijzen, noch getuigen confronteren met hetgeen zij daarin hebben gezegd. Die gesprekken zijn en blijven vertrouwelijk.
Er zal op de commissie worden gelet of zij zich aan de regels houdt.
De algemene mantra zal daarom zijn:
"Uit het onderzoek tot nu toe van de commissie is gebleken, dat.....".

6. Rapport
Op 24 juni zal een eerste versie van het rapport kunnen worden besproken. Indien mogelijk zullen eerste hoofdstukken al eerder worden rondgemaild. De leden dienen al wel op 19 juni een beeld te hebben van de te trekken conclusies en aanbevelingen.

7. Afspraken volgende vergadering

- De eerstvolgende vergadering is **op 16 juni** na afloop van de verhoren: gezamenlijk eten van 17.30 uur tot 19.00 uur bij Van der Valk.

- Er wordt op woensdag 17 juni NIET vergaderd.

- Daarna vergadert de commissie op **vrijdag 19 juni** van 10.00 – 13.00 uur over de conclusies en aanbevelingen voor het rapport (en over een titel).

- Voorts zijn als vergaderdata vastgelegd **woensdag 24 juni** van 13.00 – 15.00 uur;
- En **vrijdag 26 juni** van 10.00 – 12.00 uur ter finale bespreking van het rapport.

Openstaande afspraken

Datum afspraak	Inhoud afspraak	realisatie
12/6	Via CdK zal de voorzitter getuigen attenderen op voor zichzelf grondig nagaan van hun telefonische contacten in de betreffende week	13/6

paginanummer

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
10 juni 2009

Aanwezig: Leo Bornhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester, [redacted] (BC), [redacted] (BING) en [redacted] (BING); Inge Rozema (secretaris).

Afwezig: [redacted] (BING)

1. Mededelingen

De voorzitter deelt met de commissie de voorvallen in de media van afgelopen week. Wat betreft het telefoongesprek met de heer Klaver: dat is er geweest, zij het kort. De voorzitter heeft daarin zeker niet zelf aangestuurd op het indienen van een motie. Wel aangegeven, dat indien Klaver de vertraging in de rapportage aan de orde wilde stellen, dat wat hem betreft prima was, want de commissie wil daar best verantwoording over afleggen in PS.
Na afloop van PS heeft de voorzitter nagepraat over het debat met [redacted] Daar stond Ter Veer (DvhN) bij in de buurt. Die heeft hetgeen hij heeft opgevangen verkeerd als citaten in de krant opgenomen. Daar heeft [redacted] de verslaggever op aangesproken. De voorzitter heeft in een mail aan de commissie en PS e.e.a. toegelicht.

Op maandag jl. heeft de voorzitter n.a.v. vragen van Margriet Benak de namen van de genodigden voor de hoorzitting genoemd. Ook die van degenen die in een besloten zitting worden gehoord. De voorzitter is van oordeel, dat die namen niet geheim behoeven te zijn. Benak heeft er voor de radio echter een smeuïge voorstelling van gemaakt. Dat heeft intern in het provinciehuis tot reuring geleid.

Op dinsdag meldt de hoofdredacteur van het DvhN in zijn eigen krant, dat 'zijn' journalisten niet op de hoorzitting zullen verschijnen. De commissie heeft echter nog niet formeel een reactie van betrokkenen gekregen. De voorzitter is wel gebeld door De Kleine, die aangaf, dat hij onder andere omstandigheden wel had willen getuigen, maar nu in een arbeidsconflict zit met zijn werkgever en het niet in zijn belang vindt om dat te doen.

Tenslotte heeft de CdK de voorzitter aangesproken op het feit, dat hem ter ore is gekomen, dat na PS van 3 juni toch nog weer contact is geweest vanuit de commissie met het DvhN. De voorzitter benadrukt, dat dat niet kan en mag en vraagt de aanwezigen of dit gerucht klopt. De leden geven aan niet met het DvhN te hebben gesproken.

3. Verslag van 3 juni 2009

Het verslag wordt ongewijzigd vastgesteld. BING heeft contact gehad met Deloitte. Hun reactie was, dat er verder geen informatie meer zal worden verstrekt. De overige openstaande afspraken zijn uitgevoerd.

4. Tussentijdse bevindingen

[redacted] is aanwezig om verslag te doen van de bevindingen uit het technisch onderzoek.

De pc's van betrokkenen zijn onderzocht, alsmede de e-mail-omgeving en de logbestanden. KPMG heeft in het e-mail-verkeer uitsluitend gekeken naar bestanden van rond de 9,5 Mb. Dat bleek toch een te beperkte zoekvraag. Als de van Deloitte ontvangen mail met bijlage namelijk wordt doorgezonden naar iemand anders binnen het provinciehuis, wordt de dikke bijlage niet opnieuw aangehecht. Het (eventueel) doorgestuurde mailtje is dus veel kleiner van omvang.
Conclusie: i.t.t. KPMG, kunnen we (op grond van de omvang van het bestand) niet uitsluiten dat de bewuste e-mail is doorgezonden.

Er zijn drie omgevingen voor toegang tot de e-mail:
* de Drenthe Postoffice zelf (de server waarop al het externe en interne mailverkeer wordt opgeslagen. Als je ingelogd bent op een pc in het provinciehuis op @drenthe.nl, dan zit je in die postoffice).
* de inlogmethode vanuit huis met wachtwoord en token op thuisnetdrenthe.nl (VPN)
* inloggen op de webcliënt-omgeving. Dat is een internetomgeving.

Het onderzoek van de images van de diverse pc's heeft het volgende opgeleverd:
- pc van [redacted] er valt niets toe te voegen aan de bevindingen van KPMG. Er zijn geen printersporen, al zegt dat op zichzelf nog niets. Er is in november geen usb-stick in haar pc geplugd.
- pc van mevrouw Weistra: op haar pc is geen bestand van het rapport aangetroffen. Op 17/11 is zij ingelogd op het account van [redacted] Dat komt overeen met beider verklaringen.
- pc mevrouw Haarsma: deze heeft tussen 6 en 28 november niet aangestaan.
- pc de heer Van den Bosch: op zijn pc is wel een concept-versie van de samenvatting van het rapport aangetroffen, maar niet van het gehele rapport.

Netwerk-loginbestanden kunnen aantonen of er vanuit andere pc's onder eigen naam of dat van een ander is ingelogd. Die gegevens zijn echter niet meer beschikbaar.

Bevindingen o.g.v. de back-up (restore) van de mail-omgeving:
De restore is van belang om te kijken wie er in de mailbox van [redacted] kan kijken, of te zien of de mail is doorgestuurd. Er zijn geen dagtapes van deze back-ups. Wel een week-tape,gedateerd op 14 november. Alles van de week daarvoor kan worden gezien, behalve als iemand op 10 november iets heeft gedaan en dat vervolgens dezelfde of de volgende dag weer heeft uitgewist.

Het blijkt, dat [redacted] (secretaresse CdK) gemachtigd was om in de agenda en de mail van [redacted] te kijken én te schrijven. Voorts had [redacted] alle rechten op de pc van mevrouw Weistra (en van een aantal anderen).

Mevrouw Weistra heeft op 10 november om 21.45 uur (vanuit huis) ingelogd op de webcliënt-omgeving. In de pc van [redacted] is daarover vervolgens een notificatie-melding binnengekomen. Dat gebeurt automatisch, zodra er mail voor mevrouw Weistra in of uitgaat. Dit verklaart de connectie account Weistra ←→ mailbox [redacted] op de bewuste avond. I.t.t. eerdere vermoedens, is er dus niets bijzonders gebeurd.

Ook e-mails van betrokken personen aan de buitenwereld zijn gecheckt, maar daar zat niets bijzonders tussen.
Uit de toegangsregistratie blijkt, dat iedereen na half acht 's avonds het pand had verlaten.

Conclusie:

We kunnen niets naders concluderen over de vraag wie er aan het e-mail-bestand met bijlage van Deloitte in de pc van [redacted] heeft gezeten.
Het is niet uit te sluiten dat het bestand is geprint op 10/11 of daarna.
Het is niet uit te sluiten dat het bestand in die week is doorgestuurd naar een andere pc *binnen* het provinciehuis en daar vervolgens is gewist. (Als het naar buiten was gestuurd, dan was dat wel zichtbaar geweest.)

Bevindingen op basis van de interviews:
* interview met Van Nieuwpoort
Zijn verzoek om in het verslag de naam van de klokkenluider te schrappen zal de commissie niet inwilligen.
Wat toch bevreemding wekt, is dat hij op 10 november uiteindelijk niet de definitieve versie van het rapport krijgt en er ook niet naar vraagt. Hij staat opeens aan de zijlijn?

* interview met gedeputeerde Baas
Het verslag is goed bruikbaar voor de rapportage over de onderzoeksvragen 2 en 3 m.b.t. informatiebeveiliging. De secretaris zal aan de heer Baas het verzoek voorleggen namens de commissie om toestemming voor gebruik van het verslag t.b.v. het rapport.

5. Aanvullende interviews

Gezien de uitkomsten van het technisch onderzoek zijn aanvullende interviews niet meer nodig.

6. Voorbereiding hoorzitting
De vragen t.b.v. de hoorzittingen zullen a.s. vrijdag grondig worden doorgenomen. In het algemeen geldt voor deze vragen, dat het gaat om de hoofdpunten. Het gaat om het stellen van vragen ter openbare bevestiging van hetgeen we uit de interviews en het technisch onderzoek al weten, t.b.v. de rapportage. De vragen dienen scherp geformuleerd en toegespitst te zijn, zodat de bevraagden er
a) niet onderuit c.q. omheen kunnen in de beantwoording
b) niet de kans krijgen om breed uit te weiden over zaken die we niet willen horen.

Er kan in de vraagstelling niet worden geciteerd uit de verslagen van interviews. De onderwerpen die daarin aan de orde zijn geweest kunnen uiteraard wel worden aangestipt.

De vraag komt naar voren of het wenselijk is om alsnog De Kleine over te halen te komen getuigen. De komst van Van Luyn kan voor hem een nadere overweging zijn. De voorzitter voelt daar niet veel voor.

Communicatie: de commissie dient voorlopig een low profile aan te houden naar de pers toe. Rondom de hoorzittingen zullen geen interviews worden gegeven. Het doel van de hoorzittingen zal op internet en in de woordvoering nog eens helder worden verwoord. De commissie kan geen invloed uitoefenen op de getuigen, indien die wel interviews willen geven. We kunnen hen wel adviseren dat niet te doen. [redacted] zal met name richting ambtenaren deze boodschap overbrengen en hen voor en na de hoorzittingen desgewenst afschermen van de pers.

RTV Drenthe zal TV-opnamen maken, maar niet live uitzenden. Wel zal er op de radio zo nu en dan live verslag worden gedaan. Men gaat nog na of een internet-verbinding tot stand kan komen.

7. Rapport
De planning van publicatie en verspreiding wordt besproken. De commissie kan hiermee instemmen,

voorop gesteld, dat het rapport tijdig kan worden afgerond. Vooralsnog ziet de commissie op dat punt geen problemen meer. De persconferentie op dinsdag 30 juni zal om 9.30 uur worden gepland in zaal 0.19. De pers krijgt een half uur tevoren de tijd om het rapport in te zien.

8. Afspraken volgende vergadering

De eerstvolgende vergadering is op 12 juni om 10.00 uur.
De te bespreken onderwerpen zijn dan de voorbereiding van de hoorzitting (te stellen vragen en draaiboek) en de voorbereiding van het eindrapport.

Openstaande afspraken

Datum afspraak	**Inhoud afspraak**	**realisatie**
10/6	Baas vragen om toestemming gebruik verslag.	Verzoek is gedaan
10/6	SJ Boer zal ambtenaren inlichten over (niet) geven van interviews	

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
3 juni 2009

Aanwezig: Leo Bomhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester en [redacted] (BING);
Inge Rozema (secretaris).
Afwezig: [redacted] (BING)

1. Mededelingen

De voorzitter doet verslag van zijn gesprek van diezelfde ochtend met de heer Tichelaar, de heren Visser en Elema en mevrouw Imhof, in het bijzijn van de heer Kooman en mevrouw Rozema, m.b.t. de voortgang van het onderzoek en met name de vertraging in de oplevering van technische gegevens. De voorzitter heeft nogmaals de urgentie van oplevering benadrukt en afgesproken, dat zodra opnieuw kinken in kabels worden bespeurd, aan de bel wordt getrokken. De commissie kan zich geen verdere vertraging veroorloven. De voorzitter zal e.e.a. ook op deze wijze melden in de PS-vergadering van die middag.
Herman Beerda meent, dat de discussie in PS van die middag onhandig is. De commissie moet in alle rust haar werk kunnen doen en PS moeten zich daar niet mee bemoeien. Een vertraging van twee weken is toch niet zo uitzonderlijk. De planning was immers al aan de krappe kant. De andere leden beamen dit. Sietze de Jong herhaalt, dat hij het uitermate jammer vindt dat het nodig is gebleken om om uitstel te vragen.
De voorzitter benadrukt, dat de commissie er geen enkel belang bij heeft om de rapportage over de zomer heen te tillen, maar de kwaliteit blijft voorop staan.

3. Verslag van 27 mei 2009

Het verslag wordt ongewijzigd vastgesteld. BING heeft contact gehad met Deloitte. [redacted] heeft de voorgelegde vragen weer doorgespeeld aan de juridische afdeling. Er is dus nog niets uitgekomen.
Naar aanleiding van het verslag:
M.b.t. het artikel in Binnenlands Bestuur geeft de voorzitter aan, dat pas na de vorige vergadering bleek, dat ook [redacted] en Gert Udding door BB waren benaderd.
Margriet Stijkel wil weten of er nu wel of niet een extra interviewronde nodig is. Dat is wel het geval.

4. Tussentijdse bevindingen

Gezien het feit, dat de benodigde technische gegevens pas op 4 en 5 juni beschikbaar komen, is BING nog niet veel verder gekomen met nadere bevindingen. Duidelijk is dus, dat op 10 november vanaf een andere pc in het provinciehuis, onder het account van Selie Weistra is ingelogd en zo - via de machtigingsconstructie - in de mailbox van [redacted] is gekomen. Om 21.45 uur en om 22.25

uur. Zodra we weten wie er die avond in huis waren (uit de 'poortjes'gegevens) kan de groep waarop het onderzoek zich nader moet richten worden vastgesteld.

De Vodafone-gegevens van de mobiele telefonie zullen waarschijnlijk niet verder teruggaan dan drie of zes maanden. De vraag is of dan via het opvragen van facturen nog achter de gewenste gegevens kan worden gekomen. De provincie dient dan als klant om die gegevens te vragen en dat gaat geld kosten. Het kost dan ook weer extra tijd. De voorzitter betwijfelt of dit echt nodig is.

[redacted] heeft n.a.v. de e-mail van Sietze de Jong over de verschillen tusssen het concept-rapport en de definitieve versie e.e.a. bekeken. Het grootste deel van de verschillen is te verklaren of geeft geen aanleiding tot nader onderzoek. Hij adviseert om hier niet verder op door te rechercheren.

Bevindingen op grond van interviews:
* [redacted]
Wat opvalt is dat hij zegt geen reden te zien voor het lekken van het rapport. In de adviesnota aan GS over het Deloitte-rapport schrijft hij toch iets anders.

* [redacted]
Zij meldt als enige, dat op grond van de besprekingen van het kerngroepje memo's aan gedeputeerden zijn geschreven. Staan daar dan afspraken in? De anderen stellen, dat er geen afspraken uit die overleggen zijn vastgelegd. Dit is iets om nader aan mevrouw Weistra te vragen.
([redacted]

* de interviews met [redacted] en [redacted] leveren niets bijzonders op.
* [redacted] gaat uitgebreid op de gebeurtenissen op 10 november in. Is goed om te onthouden.

5. Aanvullende interviews
Op grond van de technische gegevens die we donderdag en vrijdag krijgen is nader aan te geven wie we voor aanvullende interviews moeten uitnodigen. De betrokkenen moeten wel tijdig op de hoogte worden gesteld. Het liefst al maandag de 8e juni. De interviews worden op vrijdag 12 juni 's morgens gehouden. De commissie machtigt de voorzitter om in overleg met Kooman en de secretaris de kring van te interviewen personen te bepalen.
Er moet goed worden nagedacht hoe we die interviews organiseren. Betrokkenen moeten tussentijds elkaar niet kunnen spreken. Het beste is, als we hen tegelijk in een wachtkamer kunnen zetten, maar dat zou wel eens heel lang kunnen gaan duren. De voorzitter en secretaris denken na over een oplossing.

6. Voorbereiding hoorzitting
[redacted] wordt aan de planningslijst toegevoegd. Op 18 juni om 9.00 uur. De verdere planning wordt goedgekeurd. De brieven met de oproep voor de hoorzitting kunnen donderdag 4 juni de deur uit. BING maakt een voorzet voor de te stellen vragen. De commissieleden (m.n. degenen die als eerste vragensteller zijn aangewezen) vullen dat zonodig aan.
Ko Vester wijst op de noodzaak om extra notulisten in te huren. De verslagen van de verhoren moeten er binnen twee à drie dagen liggen. De secretaris zal daarvoor zorg dragen.

7. Opzet rapport
De inhoudsopgave van het eindrapport is door [redacted] rondgemaild. De commissie is akkoord met deze indeling. BING kan beginnen met schrijven aan de paragrafen met feitelijkheden.
De voorzitter meent, dat het verslag van de PS-vergadering van 18 maart jl. ook zeker als bron moet

worden genoemd (en gebruikt).

8. Afspraken volgende vergadering

De eerstvolgende vergadering is op 10 juni om 11.30 uur.
De te bespreken onderwerpen zijn dan de nadere bevindingen op grond van de technische gegevens, de voorbereiding van de ingelaste interviews en van de hoorzitting en de opzet van het eindrapport.

Openstaande afspraken

Datum afspraak	**Inhoud afspraak**	**realisatie**
20/5	BING gaat na bij Deloitte wie evt. een versie van het rapport heeft gehad	Deloitte beraadt zich op antwoord
3 juni	Organisatie aanvullende interviews bepalen	
3 juni	De secretaris gaat na wie er op vakantie zijn	
	De secretaris regelt extra notulisten	

IR/ 04-06-09

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
27 mei 2009

Aanwezig: Leo Bomhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester en [redacted] (BING);
Inge Rozema (secretaris).
Afwezig: [redacted] (BING)

1. Mededelingen
Herman Beerda meldt, dat Binnenlands Bestuur met Eddy Veenstra en met hem heeft gebeld over het onderzoek. Hij heeft naar de voorzitter verwezen. Leo Bomhof heeft echter geen telefoontje gehad. Wel van Margriet Benak, die wilde weten wanneer de hoorzitting zal zijn.

3. Verslag van 20 mei 2009
Het verslag wordt ongewijzigd vastgesteld. BING heeft contact proberen te leggen met Deloitte, maar dat is nog niet gelukt.
Naar aanleiding van het verslag: Sietze de Jong vindt de dreiging met een kort geding door Van Luyn in november 2008 wel een punt om nog nader te bevragen bij medewerkers van de provincie.
De extra vergaderingen van de commissie op 12 en 19 juni starten om 10.00 uur en zullen naar verwachting tot 13.00 uur duren.

4. Tussentijdse bevindingen
* Aandachtspunten mbt het interview met A. Imhof:
Op blz. 10 meldt ze dat op 4 november ook in GS is gesproken over het Eurochamp-rapport, dat toen net in concept was verschenen. Is daar een besluitenlijstje van of heeft ze daar aantekeningen van? Wat is daar toen besproken?
Wat opvalt, is dat Van Nieuwpoort niet door haar op de kamer is geroepen met de vraag of hij gelekt heeft, maar de andere medewerkers van het kerngroepje wel. Dat is nog een aanvullende vraag voor haar.
Mevrouw Imhof merkt ook nog op, dat haar woorden "een handjevol rapporten" letterlijk in de krant stonden daarna. Heeft de heer Klaver dat aan de krant doorgespeeld?

* Aandachtspunten mbt interview met S. Weistra:
Op blz. 8 zegt ze toe, dat de commissie een mailtje van Deloitte aan haar kan krijgen. Dat is nog niet gebeurd.
Margriet Stijkel vond haar antwoorden vaak ontwijkend. Is er sprake van een selectief geheugen? Mevrouw Weistra zou nog eens goed moeten worden bevraagd.

* Aandachtspunten mbt interview met T. Klip:
Het sms-je aan de heer Klaver kwam dus van haar. [redacted] vindt dat een aanwijzing voor de vigerende cultuur binnen het provinciebestuur. Binnen het college lijkt men elkaar daar niet over aan te spreken, maar er wordt wel over ge-sms't met een statenlid.
Mevrouw Klip sprak over de tam-tam. Daar zouden we haar nog eens over moeten bevragen.

Herman Beerda meent dat de commissie zich teveel op het vinden van het lek focust. Ook de wijze waarop er op (in zijn ogen onbelangrijke) details wordt gefocust, duidt daarop. Hij heeft daar toenemende moeite mee. De onderzoeksopdracht voor de commissie was een andere en de buitenwereld zal de commissie daarop beoordelen.
Leo Bomhof vindt de zoektocht naar het lek een belangrijk onderdeel van de onderzoeksvraag. Dat was in het debat in PS op 18 maart ook de kern. Na het advies van Elzinga is dat breder getrokken, maar de kern blijft daarmee onverminderd overeind staan. Dat neemt niet weg, dat er tijdens de interviews wel degelijk is ingegaan op de andere onderzoeksvragen.
Gea Smith is het eens met Leo Bomhof. De commissie is op een goede manier bezig.

Herman Beerda vindt het met name van belang hoe de commissie de vraagstelling tijdens de hoorzitting gaat insteken. Daar moet uit blijken dat alle onderzoeksvragen aan bod komen en het zal om de hoofdzaken moeten gaan. Hij begrijpt ook wel dat de politiek zich vooral zal interesseren voor de vraag naar het lek, maar er is ook een bredere kring, die naar deze commissie kijkt, waaronder BZK. Zo'n analyse van zojuist over de vigerende cultuur binnen het provinciebestuur is uiteraard wel relevant voor ons onderzoek. Het rapport zal op deze aspecten voldoende evenwichtig moeten zijn.

Sietze de Jong vindt, dat gezien de discussie in PS, de commissie op de goede weg zit. Maar als er nu helemaal niets uitkomt, dan vindt hij dat de commissie beter ten halve kan keren dan ten hele dwalen, dus zouden we dan de opdracht moeten teruggeven.
Daar zijn de anderen het niet mee eens. Ook al vinden we het lek niet, dan is het rapport toch waardevol. De commissie kan aantonen dat we alles hebben gedaan om de waarheid boven tafel te krijgen, dus als dat niet lukt, zegt dat ook wat. Voorts zijn onze waarnemingen over de vigerende cultuur c.a. en het omgaan met integriteit ook van belang.

* Bevindingen op grond van technische analyse van BING
[redacted] meldt, dat ze opvallende dingen zijn tegengekomen. Op de avond van 10 november is er hoogstwaarschijnlijk geprobeerd in de mailbox van [redacted] te komen. Dat lijkt ook te zijn gelukt. Er is nog nader onderzoek en analyse nodig om precies te kunnen nagaan wat er is gebeurd. Daar heeft BING de technische gegevens voor nodig, die nog onderweg zijn vanuit de provinciale IT-afdeling.
Niemand van de geïnterviewden heeft daar echter iets over gezegd tot nu toe. Dat roept toch vragen op.
[redacted] adviseert om na afronding van de nadere analyse nog een extra interviewronde met een beperkte groep in te lassen over dit gegeven, alvorens met de hoorzittingen te beginnen.

Na enig beraad concludeert de commissie, dat het verstandig is om nu te beslissen om de hoorzittingen toch nog een week uit te stellen. Dat betekent, dat alles een week opschuift en dat de commissie aan PS om uitstel van rapportage zal verzoeken. Publicatie van het rapport kan dan nog steeds voor het reces plaatsvinden, maar behandeling in de staten zal dan later moeten.
De nieuwe data voor de hoorzitting zijn 16 juni de gehele dag en 18 juni 's ochtends.

5. Voorbereiding hoorzitting

* de planning wordt aangepast aan de nieuwe data. [redacted] wordt er alsnog aan toegevoegd voor een half uur in besloten setting. Mevrouw Haarsma zal als laatste worden gepland (ervan uit gaande, dat de beide journalisten niet komen).
* het persbericht is akkoord. Er worden geen namen in genoemd, behalve die van de beide gedeputeerden. Als journalisten ernaar vragen, dan kan er wel mededeling van worden gedaan.
* de brieven met de oproep voor de hoorzitting worden zowel per aangetekende post als gewone post als per mail verzonden.
* er is steeds één vragensteller per verhoor. De anderen kunnen zonodig aanvullende vragen stellen. Leo Bomhof is steeds als voorzitter degene die inleidt en uitleidt en de eed afneemt.
* er is gelegenheid voor het maken van foto's totdat de eed is afgelegd. Daarna moeten fotografen zich terugtrekken. Camera's mogen slechts vanaf een vaste positie filmen.
Bij Paul van den Bosch zullen camera-opnamen worden verboden. Ook de internet-uitzending zal dan worden stilgezet.
* er is geen apart persmoment voorzien na afloop van de hoorzitting.
* het draaiboek is verder akkoord.
* de structuur voor de verhoren is ook akkoord.

6. Opzet rapport

[redacted] heeft een inhoudsopgave gemaakt. Die zal hij rondmailen voor commentaar. In de volgende vergadering zal daar dieper op worden ingegaan. BING zal langzamerhand moeten beginnen met schrijven.

7. Afspraken volgende vergadering

De eerstvolgende vergadering is op 3 juni om 11.30 uur.
De te bespreken onderwerpen zijn dan de nadere bevindingen op grond van de technische gegevens, de voorbereiding van de ingelaste interviews en van de hoorzitting en de opzet van het eindrapport.

Openstaande afspraken

Datum afspraak	**Inhoud afspraak**	**realisatie**
20/5	BING gaat na bij Deloitte wie evt. een versie van het rapport heeft gehad	
27/5	Brief aan PS verzoek om uitstel	28/5
27/5	Nieuwe data hoorzitting 16 en 18 juni	
27/5	BING mailt opzet rapport rond	= gebeurd

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
20 mei 2009

Aanwezig: Leo Bomhof (voorzitter), Sietze de Jong, Gea Smith, Margriet Stijkel, Ko Vester, Michel Berends (plv), [redacted] (BING) en [redacted] (BING); Inge Rozema (secretaris).
Afwezig: Herman Beerda

1. Mededelingen
De voorzitter deelt mee, dat Herman Beerda hem heeft gemeld niet bij de vergadering noch bij de interviews aanwezig te kunnen zijn. De secretaris meldt, dat de commissie complimenten krijgt voor de wijze waarop de geïnterviewden zijn bejegend vorige week.

3. Verslag van 6 mei 2009
Het verslag wordt ongewijzigd vastgesteld. De afspraken zijn alle inmiddels gerealiseerd.
Deloitte heeft per e-mail te kennen gegeven, dat zij niet willen meewerken aan een interview.

4. Tussentijdse bevindingen
* Aandachtspunten mbt het interview met H. Klaver:
Wijkt hetgeen Klaver over de mail van Westera heeft gezegd nu wel of niet substantieel af van hetgeen hij in de PS-vergadering van 18 maart heeft gezegd?
Het valt een aantal leden op, dat Klaver veel zijpaden bewandelt en zo nu en dan nogal insinuerend is.
De vraag is of hij contact heeft gehad met Van Luyn.

* Aandachtspunten mbt interview met P. Van den Bosch:
Komt vertrouwenwekkend over. Schuift de verdenking af op Van Luyn. Is kennelijk eerlijk over wat Haarsma weet en niet weet.

* Aandachtspunten mbt interview met A. Haarsma:
Was een defensief verhaal. Week niet af van wat we al wisten en wat ze in PS heeft gezegd. Sietze de Jong vond haar nogal fel afwijzend waar het ging om het vrijgeven van het verslag van haar interview met KPMG.

* Aandachtspunten mbt interview met B. Van Luyn:
Hij is geloofwaardig als hij zegt, dat áls hij het definitieve rapport had gehad, hij dat onmiddellijk openbaar zou hebben gemaakt. Hij was in het begin van het interview warrig. Slecht voorbereid.
Het kort geding waar hij over sprak, daar hebben we de mensen van de provincie niet over gehoord?
De Kleine en Van Luyn moeten veel contact hebben gehad in die weken.

De overige interviews zijn nog in de maak. Van de gesprekken met Weistra en Klip worden nog woordelijke verslagen gemaakt. De commissie geeft aan, dat dat ook dient te gelden voor de verslagen van de gesprekken met Imhof [redacted].

[redacted] vindt, dat de geluidsbestanden van de interviews nog niet te snel moeten worden gewist. Pas als het onderzoeksrapport gereed is, kunnen deze veilig worden vernietigd. Dit is niet geheel conform de afspraken met de geïnterviewden, maar de commissie vindt, dat terzake geen risico moet worden gelopen.

* Bevindingen van BING
BING heeft opnieuw met KPMG gesproken.
De beruchte dubbele pagina in het pdf-bestand blijkt een extra pagina te zijn als eerste bladzij van de bijlage bij het rapport. Die zit niet in de definitieve papieren versie. Het klopt dus, dat Klaver een kopie heeft van de pdf-versie, welke ook in de pc van [redacted] zit. De rare volgorde van de pagina's 66, 67 en 69 en het ontbreken van 68 in de kopie van Klaver is hoogstwaarschijnlijk te wijten aan slordig kopiëren en duidt niet direct op een tweede pdf-versie.

Een aantal feiten is niet in het rapport van KPMG terug te vinden (zoals de fax van 24/11 van De Kleine aan Van Luyn). Hiervan is KPMG wel op de hoogte, blijkt. Maar zij hebben bepaalde feiten niet opgenomen om de anonimiteit van de informant te waarborgen, dan wel het onderzoek geen persoonsgericht karakter te geven.
Het is niet met zekerheid te zeggen of de opdrachtgever daar de hand in heeft gehad. Een eerste versie van het KPMG-rapport is besproken in het Hof van Saksen, maar die versie is door KPMG daar ook weer ingenomen. De commissie beschikt nu over het tweede concept van 5 maart jl.

BING heeft voorts een aantal bevindingen op papier gezet. Dit overzicht is nog niet volledig.

* De commissie concludeert, dat het toch noodzakelijk is om de concept-versie van Deloitte van 3 november te krijgen. Deloitte heeft daar geen toestemming voor gegeven. Maar met een beroep op artikel 151b van de Provinciewet zal het college van GS per brief alsnog worden gevraagd het te overhandigen.

* BING zal nog eens bij Deloitte trachten na te gaan wie nog meer een concept-versie of een definitieve (digitale) versie van het rapport hebben gehad. De naam van de 'klokkenluider' bij Eurochamp valt. Deze mevrouw heeft (ook) connecties met een journalist bij het DvhN.

* De commissie besluit na enige discussie om niet het gespreksverslag van mevrouw Haarsma met KPMG op te vragen.

6. Voorbereiding hoorzitting
De hoorzitting wordt gepland op 9 juni 's morgens en 10 juni de gehele dag. De secretaris zal een voorzet maken voor de tijdsindeling en volgorde van getuigen.
De volgende getuigen worden opgeroepen: mevrouw Haarsma, mevrouw Klip, mevrouw Imhof, mevrouw Weistra, de heer Klaver, de heer Van Luyn, de heer Van den Bosch, de heer De Bruin en de heer De Kleine. Met betrekking tot [redacted] en de heer Van Nieuwpoort houdt de commissie nog een slag om de arm.
Aan [redacted] zal worden gevraagd, of het verslag van haar interview mag worden gebruikt voor het rapport. Daarmee vervalt dan de noodzaak tot een openbaar verhoor.
De heer Van den Bosch zal wel in het openbaar worden gehoord, maar de commissie zal de filmende en fotograferende pers verbieden om opnamen te maken. Alleen de schrijvende pers kan zijn werk

doen. Voor de overige getuigen vindt de commissie dergelijke maatregelen niet noodzakelijk.

Het protocol voor de openbare verhoren wordt goedgekeurd.
De brief met de oproep voor getuigen moet nog worden aangepast waar het de passage over het omgaan met de media betreft.

7. Afspraken volgende vergadering

De eerstvolgende vergadering is op 27 mei om 11.30 uur.
De te bespreken onderwerpen zijn dan de voorbereiding van de hoorzitting, de opzet van het eindrapport en de bevindingen op grond van de interviews en de technische gegevens tot nu toe.

Op vrijdag 12 juni om 10.00 uur wordt een extra vergadering van de commissie ingepland.
Op vrijdag 19 juni om 10.00 uur eveneens. Ter finalisering van het rapport.
Op 22 juni moet het rapport drukklaar zijn en op 23 juni wordt het verspreid naar de leden van PS.
Op 30 juni zou dan een extra PS-vergadering moeten worden gepland.

Openstaande afspraken

Datum afspraak	**Inhoud afspraak**	**realisatie**
20/5	Brief aan GS met verzoek om concept-rapport Deloitte	25/5
20/5	BING gaat na bij Deloitte wie evt. een versie van het rapport heeft gehad	
20/5	Tijdsplanning en gespreksvolgorde hoorzitting	27/5
20/5	Brief oproep hoorzitting aanpassen	27/5

IR/ 25-05-09

ONDERZOEKSCOMMISSIE EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
6 mei 2009

Aanwezig: Leo Bomhof (voorzitter), Sietze de Jong, Gea Smith, Tjerk Medemblik (plv), Philip Oosterlaak (plv), [redacted] (BING) en [redacted] (BING, vanaf 12.30 uur);
Inge Rozema (secretaris).

Afwezig: Herman Beerda, Margriet Stijkel en Renee Westerhof

1. Mededelingen

De voorzitter deelt mee, dat Herman Beerda contact heeft gehad met enkele media. Hij heeft hiervan melding gemaakt.
De heer [redacted] van BING zal rond 12.30 uur aanschuiven. Hij heeft de dag tevoren overleg gehad met de IT-specialist van KPMG en zal daar in de commissie verslag over doen.

3. Verslag van 28 april 2009

Het verslag wordt ongewijzigd vastgesteld. Naar aanleiding van het verslag wijst de voorzitter nog op een incongruentie tussen hetgeen KPMG heeft gezegd en wat mevrouw Haarsma op 18 maart in PS zei: heeft Deloitte nou met de directiesecretaresse gebeld of andersom? Zowel in de interviews als d.m.v. technisch onderzoek van telefoongegevens zal hierover duidelijkheid moeten komen.

De voorzitter heeft vorige week contact gehad met de heer Klaver over de informant. Klaver heeft toegezegd te willen bemiddelen bij de informant. Hoe dit afloopt is nog niet duidelijk.

4. Tussenrapportage BING

BING heeft een tussenrapportage opgesteld op basis van de deskresearch en daar adviezen aan toegevoegd m.b.t. de volgende fase. [redacted] licht toe, dat in de interviews duidelijkheid moet komen over de vraag hoe die handboeken en voorschriften over informatiebeveiliging en gebruik bedrijfsmiddelen nu in de praktijk werken. Is het alleen maar papier of wordt het echt nageleefd? Desgevraagd geeft [redacted] aan, dat hij van oordeel is, dat hij de documenten goed heeft kunnen beoordelen.
Hij is van mening, dat het toch relevant is, om de verschillen tussen de concepten en definitieve versie van het Deloitte-rapport te bestuderen.
Sietze de Jong vraagt zich af of het voldoende duidelijk is voor ambtenaren wanneer iets vertrouwelijk is en wanneer niet. Wanneer is precies sprake van schending van het ambtsgeheim? Staat dat ergens geregeld? De voorzitter meent dat er zoiets is als "professional judgement": een ambtenaar moet op zijn klompen aan kunnen voelen wanneer iets vertrouwelijk is en wanneer niet. Daar mag en kan men hem op aanspreken.

Er volgt een discussie over de positie van verschillende ambtenaren in de organisatie en hun onderlinge relaties. Sietze de Jong schetst dit schematisch op het white board.
Vervolgens komt naar voren hoe de commissie nu moet omgaan met het feit, dat inmiddels is uitgesproken, dat het Deloitte-rapport in termen van de WOB wel (passief) openbaar is. De voorzitter meent, dat de commissie hier niets mee kan. Op het moment van lekken ging het om een vertrouwelijk rapport en daar richt het onderzoek zich op. Wel kan de vraag worden gesteld of het college hier goed over is geadviseerd destijds (les voor de toekomst).

5. Planning en lijst interviews
De heer Klaver heeft verzocht om later op de middag te mogen worden geïnterviewd. Aangezien Martin de Bruin heeft laten weten niet te komen, kan Klaver om 19.00 uur worden 'besteld'. Van De Kleine en Van Luyn is nog niets vernomen. De secretaris zal De Kleine nogmaals een brief sturen, maar dan op zijn huisadres. Van Luyn heeft laten weten nog contact op te nemen (*inmiddels aangegeven dat hij graag later in de week wil komen, IR*).

De interviewlijst van KPMG laat een aantal namen zien, die de commissie niet heeft uitgenodigd. Na enig beraad wordt besloten om de gedeputeerden Munniksma en Bats alsnog uit te nodigen. De anderen (ambtenaren) niet. P. Sijpersma is hoofdredacteur van het DvhN. Hij kan eventueel worden uitgenodigd na de interviews van de eerste week, als daar dan nog aanleiding toe bestaat.
De voorzitter heeft met Herman Beerda gesproken over de vraag of gedeputeerde Baas ook zou moeten worden bevraagd, in het kader van de bredere onderzoeksvraag van de commissie naar het (informatie)beveiligingsbeleid van de provincie. Hij stelt voor dit wel te doen. De commissie gaat hiermee akkoord.
De planningslijst wordt aangepast aan de laatste stand en z.s.m. aan de leden gestuurd.

6. Voorbereiding interviews
BING heeft per te interviewen persoon een vragenlijst gemaakt. De vragen worden ter vergadering hier en daar aangevuld. Voor het overgrote deel kan de commissie zich in de opzet en inhoud van de vraagstelling vinden. De lijsten zijn soms wel erg lang en de commissie vraagt zich af of er tijd genoeg is per gesprek. Dat is afwachten. Vragen kunnen eventueel wat geclusterd worden in de gesprekken.

De voorzitter heeft een voorstel gemaakt voor de werkverdeling per interview. Drie leden van de commissie doen het interview. De nummer 1 stelt primair de vragen, de andere 2 vullen hem of haar aan. De overige aanwezige leden onthouden zich van vraagstelling of commentaar. Eventueel per briefje mogelijke opmerkingen doorgeven. Afgesproken wordt, dat aan het eind van elk gesprek even wordt geschorst om overleg te hebben of er zaken vergeten zijn.
De voorzitter is bij (bijna) elk gesprek één van de drie vragenstellers. Hij acht dit aangewezen, om op deze wijze als voorzitter de geïnterviewden welkom te kunnen heten en enige uitleg te geven. Alleen bij de interviews met gedeputeerden Klip en Bats vindt hij dat (als partijgenoot) niet passend.
De rol van BING is die van "ogen en oren", maar men kan ook aanvullende vragen stellen als dat nodig wordt geoordeeld. Met name scherp zijn op informatie die aanvullend gebruikt kan worden in de nog komende gesprekken en de commissie daarop attenderen.

De secretaris heeft vanuit een eerder onderzoek nog een structuur van een interview op papier staan. Daarin staan aandachtspunten op een rijtje voor de wijze waarop een gesprek wordt geopend, wat er moet worden toegelicht aan de geïnterviewde en een paar standaard slotvragen. Als houvast gedurende het gesprek. De commissie neemt dit over.

7. Afspraken volgende vergadering

Na afloop van de interviews op vrijdag 15 mei (dus circa 15.00 uur) zal de commissie nog (kort) bijeenkomen om alle interviews na te bespreken en op grond daarvan te bepalen welke personen zullen worden opgeroepen voor de (openbare) hoorzitting. De oproep daartoe dient ruim tevoren aan de betrokkenen te worden toegestuurd (maandag 18/5 of dinsdag 19/5).

De eerstvolgende reguliere vergadering is dan op 20 mei om 11.30 uur.

8. Rondvraag

De heer [redacted] doet verslag van zijn bevindingen op grond van bestudeerd materiaal en zijn gesprek met de IT-specialist van KPMG:

Complicatie zat meteen al in het feit, dat KPMG geen gegevens wilde overdragen, omdat de opdrachtgever daarvoor geen toestemming heeft gegeven. Alles was alleen ter inzage. De commissie gaf aan, dat die toestemming er wel snel moet komen, anders zal de commissie andere wegen moeten bewandelen om dit gedaan te krijgen.

[redacted] heeft het KPMG rapport beoordeeld op tactiek en techniek en ook op de vraag of de conclusies konden zijn gebaseerd op de aangedragen gegevens. Daarover heeft hij ook vragen gesteld. De door KPMG gebruikte logging-gegevens zijn nodig om dat goed te kunnen beoordelen. De logging bestreek zowel e-mail verkeer intern⇔extern als intern⇔intern. Bij de intern⇔extern logginglijsten zat dus ook de mail van Deloitte aan de directiesecretaresse. KPMG heeft de logging gecheckt vanaf een aantal dagen vóór 10 november tot een paar weken erna.

Relevant is, dat het e-mail-systeem Groupwise, waar de provincie mee werkt, *bijlagen* bij een e-mail maar één maal fysiek bewaart in het systeem. Dan is dus de vraag of bij het eventueel doorsturen van die mail met bijlagen opnieuw een bestand van 9.5Mb wordt gevonden, of dat dit dus veel kleiner is. Dit is door KPMG niet gesignaleerd, omdat dit bij hen niet bekend bleek.

KPMG heeft gezocht op de omvang van het bestand én op een lijst met steekwoorden. KPMG weigert deze steekwoordenlijst te geven.
Voorts heeft KPMG niet gekeken naar de webmail-middelen van de directiesecretaresse, hoewel daarvan wel sporen te vinden moeten zijn, indien daar gebruik van is gemaakt. Ook naar gebruik van chatmail als MSN e.d. is niet gekeken.

Tussen elke PC en de daaraan gekoppelde printer zit een printserver. Daar is door KPMG niet naar gekeken. Wel naar de printer zelf, maar daarop is niets gevonden aan sporen. Mede omdat het al twee maanden na dato was. De harde schijf van de printer is door KPMG niet doorgelicht.
➔ [redacted] betwijfelt zelf ten zeerste of de kans om nu, een half jaar na dato, nog iets te vinden op de printer-server of de harde schijf van de printer wel aanwezig is.

KPMG was nogal stellig in de mening, dat er geen externe (usb-)media aangesloten zijn geweest op de betreffende PC. Bij navraag was naar de mening van [redacted] de argumentatie daarvoor niet bevredigend.

Zijn **conclusie** is, dat BING het technisch IT-onderzoek grondiger kan dan KPMG, maar of je dan alsnog wat vindt, is zeer de vraag. Want na een half jaar is er al veel aan relevante data verdwenen. Van PC's die je nu pas gaat veiligstellen zijn de sporen nu 100 maal kleiner dan een week geleden.

Vanuit de commissie zijn op grond van dit relaas nog vele vragen. Een deel daarvan kan worden beantwoord door de afdeling Automatisering van de provincie met wie de commissie diezelfde middag nog overleg heeft.

De commissie **concludeert** dat KPMG steken heeft laten vallen. De indruk bestaat, dat er sprake is van 'grote stappen, snel thuis'. De vraag is of dit het gevolg is van zelfrestrictie of van aanwijzingen door de opdrachtgever.
De commissie (c.q. BING) moet in die omissies voorzien, mits er een redelijke kans aanwezig wordt geacht, dat het iets kan opleveren. Dus:

1. de gegevens van KPMG loskrijgen (m.n. logging gegevens)
2. data verzamelen over aanwezigheidsregistratie (tussen 10/11 en 13/11) en over telefoonverkeer in die periode
3. mail-back-ups uitvoeren
4. veiligstellen van nog andere PC's is niet meer de moeite

Afspraak: BING maakt een lijstje met acties die in hun ogen nuttig en nodig zijn, met daaraan gekoppeld een tijdsplanning en kosten. Daar kan de commissie dan (snel) haar fiat op geven.

Na afloop van de vergadering gaan een aantal leden en de heren van BING op bezoek bij de heer Visser (CS) en de heer Kremers (AUT) voor nadere informatie over de IT bij de provincie.

Openstaande afspraken

Datum afspraak	**Inhoud afspraak**	**realisatie**
6/5	Voorzitter neemt nogmaals contact op met Klaver om naam van informant te achterhalen	29/4
28/4	Secretaris nodigt De Kleine, mdw. Deloitte en informant uit	✓
6/5	Toestemming directie vrijgeven gegevens van KPMG afdwingen	✓
6/5	Vervolmaken vragenlijsten interviews door BING	✓
6/5	Uitnodigen gedeputeerden Baas, Bats en Munniksma voor interview	7/5

Vertrouwelijk

15

Samenvatting relevante nieuwe bevindingen:

Ten aanzien van de eerste onderzoeksvraag

- Het is nog steeds zeer aannemelijk dat het de digitale definitieve versie van het rapport betreft die is uitgelekt naar het DvhN (en vervolgens doorgespeeld naar de heer Klaver). Dit vanwege het lay out verschil en de blanco pagina na bladzijde 45 in de versie van de heer Klaver. Daarnaast is inmiddels vastgesteld dat de 'dubbele' pagina in het rapport, zoals door KPMG is gesteld, de eerste bladzijde van de bijlage betreft. Deze betreffende pagina zit wel in de digitale versie, maar niet in de papieren versie van het definitieve rapport;
- De concept versie van het rapport zou geen paginanummering bevatten (blijkens het interview met de heer Van Luyn). Dit moet nog worden gecontroleerd. De heer De Kleine van het DvhN heeft op 24 november 2008 een kopie van bladzijde 17 (dus met paginanummering) aan de heer Van Luyn gestuurd als bewijs van het in bezit zijn van de krant van de definitieve versie van het rapport;
- Het concept rapport zou 86 pagina's bevatten, het definitieve rapport bevat 91 pagina's. Onduidelijk is waaruit dit verschil bestaat. Door een aantal geinterviewden is gesuggereerd dat het enige verschil slechts één alinea betreft, met als onderwerp 'visolie';
- Op en rond 10 november 2008 is er meerdere malen emailcontact geweest tussen de provincie en Deloitte. Hierover heeft KPMG niets gerapporteerd. Digitaal onderzoek moet uitwijzen wat er in deze emails heeft gestaan;
- Uit de interviews is gebleken dat in ieder geval drie personen op 10 november 2008 weet hadden van het bestaan van een digitale versie van het rapport: [redacted] mevrouw Weistra en de heer Van de Bosch;
- Op 10 november 2008 is er 's avonds een bijeenkomst geweest van de 'kerngroep Eurochamp'. Daarbij is 's avonds pizza gegeten. Geen van de aanwezigen kan zich herinneren of daarbij is gesproken over de digitale versie;
- Uit het interview met de heer Van Luyn is gebleken dat de journalisten De Kleine en De Bruin op een gegeven moment op gespannen voet met elkaar hebben gestaan. Het sturen van een fax door de heer De Kleine aan de heer Van Luyn met een bladzijde uit het rapport zou daar het gevolg van zijn;
- De heer Van Luyn zegt dat hij de concept versie d.d. 4 november nooit heeft ontvangen en de definitieve versie pas omstreeks 27 november 2008;
- Uit het vooronderzoek is gebleken dat de heer De Kleine 'van de zaak is gehaald'. Ook zou hij een tijdje thuis hebben gezeten. Aannemelijk is het dat het de heer De Kleine is geweest die een email van de heer Westera heeft doorgespeeld aan de heer Klaver. In die email wordt gesproken over het beschermen van de bron van de krant. Deze email was door de heer Westera gestuurd aan de hoofdredactie, aan de heer De Bruin en aan de heer De Kleine. De heer Westera heeft over het uitlekken van deze email gebeld met de heer Van de Bosch. De heer Klaver heeft deze email voorgelezen aan de commissie;
- De heer De Kleine heeft op 26 november 2008 een email gestuurd aan de heer Van de Bosch waarin hij zijn dank uitspreekt voor de informatie die hij

van de heer Van de Bosch heeft ontvangen over het wespennest van Eurochamp. Tevens schrijft hij letterlijk: 'let op uw saeck';

- De heer Klaver heeft een sms'je ontvangen van de mevrouw Klip, waarin onder meer is gesteld: 'Martin de Bruin onderhoudt nauwe contacten met de afdeling communicatie en is behulpzaam bij het bedenken van scenario's. Vreemd op zijn zachtst gezegd.';
- De heer Van de Bosch en mevrouw Haarsma wijzen in hun interviews nadrukkelijk naar advocaat Van Luyn als degene die het rapport zou kunnen hebben gelekt;
- De heer Van Luyn stelt dat als hij het rapport in handen zou hebben gehad, hij het zeker zou hebben laten lezen door journalisten. Dit vanwege het feit dat zijn cliënt door het rapport er juist beter van af zou komen. Daarnaast was hij naar eigen zeggen niet gehouden aan geheimhouding;
- In de oplegnotitie voor de GS vergadering van 11 november 2008 wordt gesproken over het risico van negatieve beeldvorming. Deze notitie is opgesteld op 7 november 2008 door [redacted] na afstemming met de heer Van de Bosch, [redacted] en [redacted]. Daaruit volgt dat er mogelijk een negatief beeld in de media zou kunnen ontstaan over de rol van de provincie in het Eurochampdossier. Daarbij wordt in de notitie aangetekend dat op basis van de analyse van Deloitte beweringen kunnen worden weerlegd. 'Echter omdat het rapport van Deloitte niet in openbaarheid kan worden gebracht en gedetailleerde informatie niet kan worden verstrekt, kunnen de media en de staten hier vragen over stellen.' Hieruit lijkt te volgen dat de provincie mogelijk een belang had dat het rapport zo snel mogelijk openbaar zou worden / c.q. in bezit zou komen van de media;
- De heer Klaver heeft in zijn interview aangegeven dat de door hem ontvangen 'dreigbrieven' zouden zijn geschreven door [redacted]. Hij heeft hiervan aangifte gedaan. De gedeputeerde de heer Bats, [redacted] een dreigbrief hebben ontvangen;
- KPMG geeft als reden voor het niet vermelden van een aantal feiten dat dit is gedaan ter bescherming van de identiteit van de informant en om te voorkomen dat het feitenonderzoek in een persoonsgericht onderzoek zou veranderen.

<u>Ten aanzien van de overige onderzoeksvragen:</u>

- Een aantal geïnterviewden geeft aan weinig kennis te hebben van het integriteitbeleid van de provincie. Bepaalde documenten zouden niet bekend zijn bij geïnterviewde medewerkers;
- Gedeputeerden hebben veelal rechtsreeks contacten met journalisten, soms door tussenkomst van hun communicatie/bestuursadviseur;
- Binnen het college spreekt men elkaar kennelijk niet aan op contacten met de pers, maar wordt er wel naar anderen toe over gesproken (bijv. sms'je van mevrouw Klip aan de heer Klaver);
- Het handboek informatiebeveiliging is niet 'vertaald' in een Jip en Janneke versie voor de medewerkers van de provincie;
- Bepaalde voorschriften ten aanzien van informatiebeveiliging worden niet strikt nageleefd door medewerkers (vb: pauzeknop en opslaan wachtwoord op gezamenlijke schijf);

- Er bestaat een duidelijk verschil in beeldvorming tussen het management van de provincie en de uitvoerende ambtenaren over wijze waarop integriteit wordt vormgegeven binnen de provincie.

ONDERZOEKSCOMMISSIE EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
6 mei 2009

Aanwezig: Leo Bomhof (voorzitter), Sietze de Jong, Gea Smith, Tjerk Medemblik (plv), Philip Oosterlaak (plv), [redacted] (BING) en [redacted] (BING, vanaf 12.30 uur);
Inge Rozema (secretaris).

Afwezig: Herman Beerda, Margriet Stijkel en Renee Westerhof

1. Mededelingen

De voorzitter deelt mee, dat Herman Beerda contact heeft gehad met enkele media. Hij heeft hiervan melding gemaakt.
De heer [redacted] van BING zal rond 12.30 uur aanschuiven. Hij heeft de dag tevoren overleg gehad met de IT-specialist van KPMG en zal daar in de commissie verslag over doen.

3. Verslag van 28 april 2009

Het verslag wordt ongewijzigd vastgesteld. Naar aanleiding van het verslag wijst de voorzitter nog op een incongruentie tussen hetgeen KPMG heeft gezegd en wat mevrouw Haarsma op 18 maart in PS zei: heeft Deloitte nou met de directiesecretaresse gebeld of andersom? Zowel in de interviews als d.m.v. technisch onderzoek van telefoongegevens zal hierover duidelijkheid moeten komen.

De voorzitter heeft vorige week contact gehad met de heer Klaver over de informant. Klaver heeft toegezegd te willen bemiddelen bij de informant. Hoe dit afloopt is nog niet duidelijk.

4. Tussenrapportage BING

BING heeft een tussenrapportage opgesteld op basis van de deskresearch en daar adviezen aan toegevoegd m.b.t. de volgende fase. [redacted] licht toe, dat in de interviews duidelijkheid moet komen over de vraag hoe die handboeken en voorschriften over informatiebeveiliging en gebruik bedrijfsmiddelen nu in de praktijk werken. Is het alleen maar papier of wordt het echt nageleefd? Desgevraagd geeft [redacted] aan, dat hij van oordeel is, dat hij de documenten goed heeft kunnen beoordelen.
Hij is van mening, dat het toch relevant is, om de verschillen tussen de concepten en definitieve versie van het Deloitte-rapport te bestuderen.
Sietze de Jong vraagt zich af of het voldoende duidelijk is voor ambtenaren wanneer iets vertrouwelijk is en wanneer niet. Wanneer is precies sprake van schending van het ambtsgeheim? Staat dat ergens geregeld? De voorzitter meent dat er zoiets is als "professional judgement": een ambtenaar moet op zijn klompen aan kunnen voelen wanneer iets vertrouwelijk is en wanneer niet. daar mag men hem op aanspreken.

Er volgt een discussie over de positie van verschillende ambtenaren in de organisatie en hun onderlinge relaties. Sietze de Jong schetst dit schematisch op het white board.
Vervolgens komt naar voren hoe de commissie nu moet omgaan met het feit, dat inmiddels is uitgesproken, dat het Deloitte-rapport volgens de WOB wel (passief) openbaar is. De voorzitter meent, dat de commissie hier niets mee kan. Op het moment van lekken ging het om een vertrouwelijk rapport en daar richt het onderzoek zich op. Wel kan de vraag worden gesteld of het college hier goed over is geadviseerd destijds (les voor de toekomst).

5. Planning en lijst interviews
De heer Klaver heeft verzocht om later op de middag te mogen worden geïnterviewd. Aangezien Martin de Bruin heeft laten weten niet te komen, kan Klaver om 19.00 uur worden 'besteld'. Van De Kleine en Van Luyn is nog niets vernomen. De secretaris zal De Kleine nogmaals een brief sturen, maar dan op zijn huisadres. Van Luyn heeft laten weten nog contact op te nemen (*inmiddels aangegeven dat hij graag later in de week wil komen, IR*).

De interviewlijst van KPMG laat een aantal namen zien, die de commissie niet heeft uitgenodigd. Na enig beraad wordt besloten om de gedeputeerden Munniksma en Bats alsnog uit te nodigen. De anderen (ambtenaren) niet. P. Sijpersma is hoofdredacteur van het DvhN. Hij kan eventueel worden uitgenodigd na de interviews van de eerste week, als daar dan nog aanleiding toe bestaat.
De voorzitter heeft met Herman Beerda gesproken over de vraag of gedeputeerde Baas ook zou moeten worden bevraagd, in het kader van de bredere onderzoeksvraag van de commissie naar het (informatie)beveiligingsbeleid van de provincie. Hij stelt voor dit wel te doen. De commissie gaat hiermee akkoord.
De planningslijst wordt aangepast aan de laatste stand en z.s.m. aan de leden gestuurd.

6. Voorbereiding interviews
BING heeft per te interviewen persoon een vragenlijst gemaakt. De vragen worden ter vergadering hier en daar aangevuld. Voor het overgrote deel kan de commissie zich in de opzet en inhoud van de vraagstelling vinden. De lijsten zijn soms wel erg lang en de commissie vraagt zich af of er tijd genoeg is per gesprek. Dat is afwachten. Vragen kunnen eventueel wat geclusterd worden in de gesprekken.

De voorzitter heeft een voorstel gemaakt voor de werkverdeling per interview. Drie leden van de commissie doen het interview. De nummer 1 stelt primair de vragen, de andere 2 vullen hem of haar aan. De overige aanwezige leden onthouden zich van vraagstelling of commentaar. Eventueel per briefje mogelijke opmerkingen doorgeven. Afgesproken wordt, dat aan het eind van elk gesprek even wordt geschorst om overleg te hebben of er zaken vergeten zijn.
De voorzitter is bij (bijna) elk gesprek één van de drie vragenstellers. Hij acht dit aangewezen, om op deze wijze als voorzitter de geïnterviewden welkom te kunnen heten en enige uitleg te geven. Alleen bij de interviews met gedeputeerden Klip en Bats vindt hij dat (als partijgenoot) niet passend.
De rol van BING is die van "ogen en oren", maar men kan ook aanvullende vragen stellen als dat nodig wordt geoordeeld. Met name scherp zijn op informatie die aanvullend gebruikt kan worden in de nog komende gesprekken en de commissie daarop attenderen.

De secretaris heeft vanuit een eerder onderzoek nog een structuur van een interview op papier staan. Daarin staan aandachtspunten op een rijtje voor de wijze waarop een gesprek wordt geopend, wat er moet worden toegelicht aan de geïnterviewde en een paar standaard slotvragen. Als houvast gedurende het gesprek. De commissie neemt dit over.

7. Afspraken volgende vergadering

Na afloop van de interviews op vrijdag 15 mei (dus circa 15.00 uur) zal de commissie nog (kort) bijeenkomen om alle interviews na te bespreken en op grond daarvan te bepalen welke personen zullen worden opgeroepen voor de (openbare) hoorzitting. De oproep daartoe dient ruim tevoren aan de betrokkenen te worden toegestuurd (maandag 18/5 of dinsdag 19/5).

De eerstvolgende reguliere vergadering is dan op 20 mei om 11.30 uur.

8. Rondvraag

De heer [redacted] doet verslag van zijn bevindingen op grond van bestudeerd materiaal en zijn gesprek met de IT-specialist van KPMG:

Complicatie zat meteen al in het feit, dat KPMG geen gegevens wilde overdragen, omdat de opdrachtgever daarvoor geen toestemming heeft gegeven. Alles was alleen ter inzage. De commissie gaf aan, dat die toestemming er wel snel moet komen, anders zal de commissie andere wegen moeten bewandelen om dit gedaan te krijgen.

[redacted] heeft het KPMG rapport beoordeeld op tactiek en techniek en ook op de vraag of de conclusies konden zijn gebaseerd op de aangedragen gegevens. daarover heeft hij ook vragen gesteld. De door KPMG gebruikte logging-gegevens zijn nodig om dat goed te kunnen beoordelen. De logging bestreek zowel e-mail verkeer intern⇔extern als intern⇔intern. Bij de intern⇔extern logginglijsten zat dus ook de mail van Deloitte aan de directiesecretaresse. KPMG heeft de logging gecheckt vanaf een aantal dagen vóór 10 november tot een paar weken erna.

Relevant is, dat het e-mail-systeem Groupwise, waar de provincie mee werkt, *bijlagen* bij een e-mail maar één maal fysiek bewaart in het systeem. Dan is dus de vraag of bij het eventueel doorsturen van die mail met bijlagen opnieuw een bestand van 9.5Mb wordt gevonden, of dat die dus veel kleiner is. Dit is door KPMG niet gesignaleerd, omdat dit bij hen niet bekend bleek.

KPMG heeft gezocht op de omvang van het bestand én op een lijst met steekwoorden. KPMG weigert deze steekwoordenlijst te geven.
Voorts heeft KPMG niet gekeken naar de webmail-middelen van de directiesecretaresse, hoewel daarvan wel sporen te vinden moeten zijn, indien daar gebruik van is gemaakt. Ook naar gebruik van chatmail als MSN e.d. is niet gekeken.

Tussen elke pc en de daaraan gekoppelde printer zit een printserver. Daar is door KPMG niet naar gekeken. Wel naar de printer zelf, maar daarop is niets gevonden aan sporen. Mede omdat het al twee maanden na dato was. De harde schijf van de printer is door KPMG niet doorgelicht.
➔ [redacted] betwijfelt zelf ten zeerste of de kans om nu, een half jaar na dato, nog iets te vinden op de printer-server of de harde schijf van de printer wel aanwezig is.

KPMG was nogal stellig in zijn mening, dat er geen extern (usb-)media aangesloten zijn geweest op de pc. Bij navraag was naar de mening van [redacted] de argumentatie daarvoor niet bevredigend.

Zijn **conclusie** is, dat BING het technisch IT-onderzoek grondiger kan dan KPMG, maar of je dan alsnog wat vindt, is zeer de vraag. Want na een half jaar is er al veel aan relevante data verdwenen. Van PC's die je nu pas gaat veiligstellen zijn de sporen nu 100 maal kleiner dan een week geleden.

Vanuit de commissie zijn op grond van dit relaas nog vele vragen. Een deel daarvan kan worden beantwoord door de afdeling Automatisering van de provincie met wie de commissie diezelfde middag nog overleg heeft.

De commissie **concludeert** dat KPMG steken heeft laten vallen. De indruk bestaat, dat er sprake is van 'grote stappen, snel thuis'. De vraag is of dit het gevolg is van zelfrestrictie of van aanwijzingen door de opdrachtgever.
De commissie (c.q. BING) moet in die omissies voorzien, mits er een redelijke kans aanwezig wordt geacht, dat het iets kan opleveren. Dus:

1. de gegevens van KPMG loskrijgen
2. data verzamelen over aanwezigheidsregistratie (tussen 10/11 en 13/11) en over telefoonverkeer in die periode
3. mail-back-ups uitvoeren
4. veiligstellen van nog andere pc's is niet meer de moeite

Afspraak: BING maakt een lijstje met acties die in hun ogen nuttig en nodig zijn, met daaraan gekoppeld een tijdsplanning en kosten. Daar kan de commissie dan (snel) haar fiat op geven.

Na afloop van de vergadering gaan een aantal leden en de heren van BING op bezoek bij de heer Visser (CS) en de heer Kremers (AUT) voor nadere informatie over de informatisering bij de provincie.

Openstaande afspraken

Datum afspraak	**Inhoud afspraak**	**realisatie**
6/5	Voorzitter neemt nogmaals contact op met Klaver om naam van informant te achterhalen	29/4
28/4	Secretaris nodigt De Kleine, mdw. Deloitte en informant uit	
6/5	Toestemming directie vrijgeven gegevens van KPMG afdwingen	
6/5	Vervolmaken vragenlijsten interviews door BING	
6/5	Uitnodigen gedeputeerden Baas, Bats en Munniksma voor interview	7/5

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
28 april 2009

Aanwezig: Leo Bomhof (voorzitter), Herman Beerda, Sietze de Jong, Gea Smith, Ko Vester, [redacted] (BING) en [redacted] (BING); Inge Rozema (secretaris).
Afwezig: Margriet Stijkel en Renee Westerhof

1. Mededelingen
Renee Westerhof is getroffen door [redacted]. Hij zal voor langere tijd uit de running zijn, zo lijkt het. Ko Vester zal hem vervangen. De secretaris zal een bloemetje namens de commissie sturen.

De brief van de DS, waarin zij de vragen van de OR aan de commissie doorspeelt zal worden beantwoord. Een concept daartoe ligt voor. De commissie gaat akkoord met het antwoord. De heer Beerda merkt op, dat hij kan meevoelen met de OR waar het diens zorg rond het eventueel openbaar verhoren van ambtenaren betreft in het bijzijn van de media. Het is echter de vraag of de commissie na de interviews nog ambtenaren onder ede wil horen. En zo ja, dan kan de commissie beslissen om dit zonodig ook in beslotenheid te doen.
Afgesproken wordt, dat zodra de lijst met te horen personen gereed is, dit aan de DS zal worden gezonden.

3. Verslag van 22 april 2009
De voorzitter mist in het verslag onder punt 4 de afspraak, dat BING zich zal conformeren aan de planning van de commissie. Dat wordt nog toegevoegd. [redacted] onderschrijft dit, maar heeft slechts willen aangeven, dat ervaring leert, dat met name in de rapportagefase de commissie zelf veel tijd nodig heeft om tot conclusies en aanbevelingen te komen.

4. Eerste indrukken BING
- Vandaag is nog een pakket stukken aangeleverd uit de organisatie. Die zullen deze week nog worden doorgenomen en bevindingen terzake zullen voor de commissie worden samengevat. De secretaris zal nog checken of nu al het gevraagde binnen is en zo nee, wanneer dat verwacht kan worden.
Sietze de Jong heeft behoefte aan nader inzicht in de IT-structuur, hoe dat precies werkt in dit huis en de afspraken rond beveiliging, etc. Afgesproken wordt, dat BING eerst zal inventariseren waar nader naar gekeken moet worden en vervolgens hier in huis zal gaan rondkijken. Sietze de Jong en Ko Vester zullen dan meelopen.
- Volgende week zal er nadere duidelijkheid zijn over wat er aan aanvullend onderzoek nodig is, met daarbij een inschatting van de kans dat het dan ook wat nuttigs oplevert.
- BING schat in, dat een nader bekijken van de telefonische lijntjes naar het DvhN de moeite waard kan zijn.

- BING heeft een gesprek gehad met KPMG. Dat geeft hen de indruk, dat er nog aanvullend onderzoek mogelijk en nuttig is. De IT-expert heeft het rapport van KPMG gescreend en heeft daarover nog een aantal vragen. [redacted] wil graag de afspraak met KPMG maken om hun beider IT-forensics op korte termijn te laten overleggen.
- BING acht het de moeite om meer pc's te screenen dan alleen die van de directiesecretaresse. Welke personen wisten nog meer dat er een pdf werd verstuurd?
- het blijkt, dat het om 1 mailbericht gaat, waaraan 3 pdf-bestanden waren gekoppeld.
- de resultaten van nader onderzoek op IT-gebied zullen niet beschikbaar zijn vóór de interviews. Maar als daar relevante punten uit naar voren komen, dan kunnen betrokkenen zonodig aanvullend worden bevraagd of we bewaren dat tot de hoorzitting.
- [redacted] meldt nog, dat hij van KPMG heeft begrepen, dat de informant hoogstwaarschijnlijk wel genegen is om te praten. De voorzitter meent, dat we dan z.s.m. via statenlid Klaver contact moeten proberen te leggen en de informant moeten uitnodigen. Hij zal de heer Klaver bellen op zijn vakantie-adres.

De voorzitter onderschrijft de voorstellen van BING. Hij vindt het van belang, dat in de rapportage van de commissie ook de verheldering van onduidelijkheden uit het KPMG-rapport goed wordt weergegeven.

5. Planning en lijst interviews

De commissie is van oordeel, dat de heer De Kleine van het DvhN ook moet worden uitgenodigd voor een interview. Dat kan op maandag vóór het interview met Martin de Bruin.
De secretaris doet de suggestie om de heer Van Luyn eventueel telefonisch te interviewen. Daar is de commissie het niet mee eens. De heer Van Luyn moet op het provinciehuis worden uitgenodigd.
Voorts zal de medewerker van Deloitte, die de mail verstuurde ook worden uitgenodigd.
De commissie gaat voorts akkoord met de planning. Gea Smith zal op 11 mei overdag er niet bij kunnen zijn.
De voorzitter gaat een voorstel voor de werkverdeling over de commissieleden maken. Steeds drie leden stellen de vragen. De anderen horen slechts toe.

6. Voorbereiding interviews

Er zijn door de commissieleden geen aanvullende vragen of opmerkingen aangeleverd.
[redacted] wijst erop, dat de vragen nog teveel zijn gericht op onderzoeksvraag 1 en niet zozeer op onderzoeksvragen 2 en 3 uit de onderzoeksopdracht. De vragen dienen dus wat breder te worden getrokken: over het integriteits- en beveiligingsbeleid en de cultuur in de organisatie hoe daarmee omgegaan wordt. Over de contacten tussen bestuur en media eveneens.
Sietze de Jong stelt voor om aan de ambtenaren steeds te vragen hoe zij het integriteitsbeleid in hun dagelijkse werk vormgeven. Wat betekent voor hen het afleggen van de ambtseed?
Afspraak: BING zal de vragenlijsten aanpassen en vervolmaken. Tevens zal er per persoon een korte introductie aan worden toegevoegd. Dit is op 6 mei gereed.

In de vergadering van 6 mei zal ruim de tijd worden genomen om de interviews grondig voor te bereiden. Dan zullen ook alle juridische eventualiteiten aan de orde komen en afspraken worden gemaakt hoe daarmee om te gaan.

7. Briefing door KPMG

De heren [redacted] van KPMG zijn uitgenodigd om hun onderzoek nader toe te lichten en vragen van de commissie te beantwoorden. Laatstgenoemde heeft het onderzoek

concreet uitgevoerd samen met een collega.

Het soort onderzoek dat KPMG heeft uitgevoerd is een feitenonderzoek. D.w.z. het inzichtelijk maken van de feiten met als doel erachter te komen hoe iets is gebeurd en zo mogelijk door wie. De wie-vraag duidt dan wel op een persoonsgericht onderzoek en daar zijn weer andere vereisten voor. Zoals bekend is KPMG aan beantwoording van de wie-vraag niet toegekomen.

Er zijn door de opdrachtgever van KPMG geen beperkingen opgelegd aan de onderzoekers of het onderzoek. De opdrachtgever heeft in de loop van het onderzoek wel gevraagd om nogmaals met statenlid Klaver en met de informant te gaan praten. Dat heeft KPMG toen gedaan.

Er is met [redacted] van Deloitte gesproken. Er is naar het mailbericht gekeken, waar de 3 pdf's van het rapport aanhingen. Dat mailbericht bevatte geen bcc's. Het is verzonden door de secretaresse van [redacted]

Mevrouw Imhof en de heer Visser waren de aanspreekpunten voor opdrachtverlening en begeleiding van het onderzoek van KPMG. Mevrouw Klip is er pas in de rapportagefase bij betrokken geweest. Mevrouw Weistra was de ambtelijk opdrachtgever en aanspreekpunt voor het Eurochamp-onderzoek van Deloitte.

KPMG gaat ermee akkoord om de informatie die door de provincie aan KPMG is verstrekt in het kader van het onderzoek aan de commissie te overhandigen. Dat betreft dan met name technische (logging) gegevens. De besprekingsverslagen met de door hen geïnterviewden zijn vertrouwelijk.

KPMG kan de naam van de informant niet prijsgeven.
Men acht hem betrouwbaar, omdat zijn verhaal goed in het totale plaatje past. En deels op grond van een subjectief, maar door ervaring ontwikkeld professioneel oordeel. Zijn motieven stoelden op ethische gronden.
Waarom de informant naar de heer Klaver is gelopen en niet naar iemand anders, is een vraag waarover KPMG niet kan uitweiden.

Van de heer Klaver zijn de volgende gegevens verkregen: een kopie op papier van de pdf-file van het rapport, het bonnetje van de kopieerkosten, een logboekje c.q. dagboekje over de periode half oktober 2008-februari 2009. De heer Klaver heeft enkele mailberichten en de dreigbrieven die aan hem gericht zijn ter plekke aan KPMG voorgelezen.

Er is sprake van vier versies van het rapport van Deloitte: het concept voor hoor- en wederhoor, het definitief concept voor de opdrachtgever, het definitieve rapport op papier (blauwe kaft) en het definitieve rapport in pdf.
KPMG heeft zich niet in de verschillen tussen die versies verdiept, omdat al snel de focus lag op de pdf-versie.

Het concept-rapport van KPMG is besproken met Klip, Imhof en Visser. Er is commentaar geleverd op het gebruik van concrete namen (Leijssenaar, Van Luyn) Die moesten worden geschrapt. Ambtenaren moesten met hun functienaam worden vermeld in plaats van het vage 'een medewerker'.
In de eerste bullet van de conclusies is in de definitieve versie een datum gewijzigd. Er stond eerst "13 november". Daar is "27 november" van gemaakt. De eerstgenoemde datum kon onvoldoende hard gemaakt worden.

Gedurende het onderzoekstraject is intensief met de opdrachtgever gesproken over de diepgang

ervan. Hoeveel haal je overhoop? KPMG vond onvoldoende aanleiding om dieper te gaan dan ze hebben gedaan. Men gebruikte de methode van 'uitsluiting van mogelijkheden'. Het had wel breder gekund, maar de kosten daarvan wogen niet op tegen de minimaal geachte kans dat het wat zou opleveren.
Het e-mailverkeer via de server is wel geheel gecheckt. Ook het interne mailverkeer is gelogd.

KPMG heeft desgevraagd geen specifieke opmerkingen over de wijze waarop Drenthe met beveiliging omgaat. Het is een openbaar gebouw en sommige externen hebben pasjes waarmee ze zo in- en uit kunnen lopen.

De directiesecretaresse heeft volgens KPMG aangegeven zich goed bewust te zijn van haar vertrouwelijke positie. Ze maakte melding van nieuwsgierige collega's, die haar bewust maken van de noodzaak om altijd de computer af te sluiten als ze wegloopt.
Ter verduidelijking: zij is *door Deloitte* gebeld, dat de definitieve rapporten pas later zouden worden aangeleverd en in datzelfde gesprek heeft zij toen gevraagd om dan alvast een pdf-versie te sturen.

KPMG zegt toe aan de commissie de lijst met geïnterviewde personen te zullen overhandigen.

KPMG gaat akkoord met de afspraak om de forensic IT-specialisten van BING en KPMG met elkaar te laten overleggen op zeer korte termijn.

8. Volgende vergadering
De volgende vergadering is op woensdag 6 mei van 10.30-13.30 uur. **NB: we beginnen dus eerder!!**
Zie ook onder punt 6 wat we dan aan de orde zullen hebben.

9. Rondvraag
Het concept-persbericht dat op verzoek van de voorzitter is gemaakt, wordt door de commissie akkoord bevonden. Het past in de lijn om zoveel mogelijk openheid van zaken te geven over het proces van het onderzoek.

Openstaande afspraken

Datum afspraak	**Inhoud afspraak**	**realisatie**
1/4	De commissie gaat een keer ter plekke de situatie in ogenschouw nemen.	
1/4 en 28/4	Geïnformeerd worden over het ICT-beveiligingsbeleid c.a. in het provinciehuis: BING en de leden De Jong en Vester nemen dit voor hun rekening	
28/4	Voorzitter neemt contact op met Klaver om naam van informant te achterhalen	29/4
28/4	Secretaris nodigt De Kleine, mdw. Deloitte en informant uit	
28/4	Voorzitter maakt voorzet voor werkverdeling interviews	6/5
28/4	Vervolmaken vragenlijsten interviews door BING	6/5

Tussenrapportage deskresearch Provincie Drenthe

BING

Datum

4 mei 2009

Aan

Onderzoekscommissie Eurochamp PS Drenthe

T.a.v. de secretaris, mevrouw I.M. Rozema

Van

[redacted] Directeur BING

Inhoudsopgave

PERSOONLIJK EN VERTROUWELIJK
Provincie Drenthe
Onderzoekscommissie Eurochamp PS Drenthe
T.a.v. de secretaris, mevrouw I.M. Rozema
Postbus 122
9400 AC ASSEN

Amersfoort, 4 mei 2009

Betreft: Rapportage deskresearch

Geachte Onderzoekscommissie,

Op uw verzoek hebben wij een deskresearch verricht. Deze dekresearch betreft ondersteuning van de commissie in de eerste fase van uw onderzoek naar de voortijdige verspreiding van een als vertrouwelijk bestempeld onderzoeksrapport. De opdracht voor ondersteuning van uw commissie is vastgelegd in uw opdrachtbrief van 21 april en onze offerte van 17 april jongstleden. Hierbij rapporteren wij onze bevindingen.

1. BING

BING biedt gespecialiseerde adviesexpertise en onderzoeksexpertise aan.
Het bureau richt zich daarbij exclusief op de overheid, wat borg staat voor specifieke branchekennis, verdieping van ervaringen en de mogelijkheid om duurzame relaties met de doelgroep te onderhouden. BING is een initiatief van de Vereniging van Nederlandse Gemeenten (VNG).

2. Aanleiding en doel van opdracht

Provinciale Staten (PS) van Drenthe hebben besloten om een onderzoek in te stellen op grond van artikel 151a van de Provinciewet naar de voortijdige verspreiding van een als vertrouwelijk bestempeld onderzoeksrapport. Provinciale staten hebben daartoe op 8 april jl. een onderzoekscommissie geïnstalleerd.

De centrale vragen in het onderzoek zijn:

- wie is verantwoordelijk voor de voortijdige verspreiding van het rapport van Deloitte en op welke wijze is dat geschied;
- waren er bij de provincie Drenthe organisatorische en/of 'bestuurlijk-culturele' factoren die de voortijdige verspreiding hebben bevorderd;
- in hoeverre moet het gevoerde bestuur worden aangepast om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen.

De eerste fase van het onderzoek is met name de fase van deskresearch. Doelstelling van deze fase is het verzamelen en analyseren van beschikbare informatie. Deze fase dient uit te monden in een advies waarin

onder meer moet worden aangegeven op welke punten in de tweede fase zich het nader onderzoek zou moeten toespitsen.

3. Door BING verrichte werkzaamheden

Wij hebben onder meer de volgende werkzaamheden verricht:

- Kennisname en analyse van het KPMG rapport;
- Kennisname en analyse van het verslag van het debat op 18 maart 2009 in Provinciale Staten;
- Kennisname en analyse van de van toepassing zijnde regelgeving en procedures en andere relevante documenten.

4. Kader

In dit hoofdstuk wordt kort het kader geschetst dat relevant is voor de beantwoording van de onderzoeksvragen. Dit kader bestaat uit een juridisch kader, de relevante wet- en regelgeving, en een beleidskader. Tot dit beleidskader behoren diverse documenten die door de provincie ten aanzien van het onderwerp informatie en informatiebeveiliging zijn opgesteld.[1]

4.1 Juridisch kader

Wij vermelden hier de wettelijke artikelen die - gelet de casus - het meeste relevant zijn.
Op basis van artikel 125a lid 3 van de Ambtenarenwet is een ambtenaar verplicht tot geheimhouding van hetgeen hem in verband met zijn functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt. Een breder kader wordt geschetst door artikel 125ter: 'Het bevoegd gezag en de ambtenaar zijn verplicht zich als een goed werkgever en een goed ambtenaar te gedragen.'

Op basis van artikel 55 van de Provinciewet kunnen Gedeputeerde Staten (GS) geheimhouding opleggen omtrent de inhoud van stukken die aan hen worden overgelegd.

Een schending van de geheimhouding kan een strafbaar feit opleveren. In artikel 272 van het Wetboek van Strafrecht is de schending van de geheimhouding geregeld. De tekst van het artikel luidt als volgt:

Artikel 272
1. Hij die enig geheim waarvan hij weet of redelijkerwijs moet vermoeden dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.
2. Indien dit misdrijf tegen een bepaald persoon gepleegd is, wordt het slechts vervolgd op diens klacht.

[1] Als bijlage bij deze rapportage is een document bijgevoegd met alle geraadpleegde documenten

4.2 Integriteitcode

De provincie Drenthe beschikt over zowel een ambtelijke gedragscode (Gedragscode ambtelijke integriteit) als een code voor de bestuurders; de Drentse gedragscode integriteit voor de CvdK, GS en PS.

4.2.1 Bestuurlijke gedragscode

De integriteitcode voor de statenleden en leden van GS van de Provincie Drenthe is vastgesteld door PS op 3 september 2003.
In de integriteitcode worden een aantal kernbegrippen genoemd. Dit zijn: dienstbaarheid, functionaliteit, onafhankelijkheid, openheid, betrouwbaarheid en zorgvuldigheid.
Deze kernbegrippen worden in de integriteitcode gezien als toetssteen voor de in de integriteitcode opgenomen gedragsafspraken. De leden van het college van GS en PS worden geacht de regels na te leven. Wanneer zij zich er niet aan houden, kan dat - blijkens de tekst van de code - gevolgen hebben voor hun functioneren en voor hun positie.

Voor deze casus is met name artikel 4 van de code van belang. In dit artikel, getiteld 'Informatie', staat het volgende:
Artikel 4.1 Een bestuurder gaat zorgvuldig en correct om met informatie waarover hij uit hoofde van zijn ambt beschikt. Hij verstrekt geen geheime informatie.

Artikel 4.2 Een bestuurder verstrekt informatie, tenzij deze geheim of vertrouwelijk is en het geven van informatie niet mogelijk is op grond van de Wet openbaarheid van bestuur.

Artikel 4.3 Een bestuurder maakt niet ten eigen bate of ten bate van zijn persoonlijke betrekkingen gebruik van in de uitoefening van het ambt verkregen informatie.

In de inleiding van de bestuurlijke gedragscode staat dat er voor ambtenaren tevens een beroepscode is opgesteld, waar integriteit een belangrijk deel van uitmaakt. De voorliggende code en de beroepscode voor ambtenaren zijn op elkaar afgestemd. Er staan geen tegenstrijdige bepalingen in, zo staat er geschreven.

4.2.2 Ambtelijke gedragscode

De Gedragscode ambtelijke integriteit is vastgesteld bij besluit van GS van 18 maart 2003. In de code worden de volgende zes kernbegrippen van ambtelijke integriteit onderscheiden: dienstbaarheid, professionaliteit, onafhankelijkheid, verantwoordelijkheid, betrouwbaarheid en zorgvuldigheid.
In de code zelf komt het onderwerp omgaan met informatie niet terug. Wel bestaat er bij de provincie een document getiteld 'Omgaan met provinciale informatie' **[datum opnemen].** Hierin wordt gesteld dat zorgvuldig moet worden omgegaan met informatie. Voor vertrouwelijke stukken geldt dit – volgens de tekst van het document – nog eens extra. Tevens staat in het document letterlijk: 'Lekt informatie bijvoorbeeld via de pers uit, dan kun je hier als medewerker persoonlijk op worden aangesproken.'

4.3 Beleidskader

Tot het beleidskader behoren een aantal documenten. De meest relevante documenten worden hieronder besproken.

4.3.1 Reglement gebruik bedrijfsmiddelen (2006)

In het Reglement gebruik bedrijfsmiddelen staat de procedure omschreven omtrent beschikbaarheid, gebruik, controle en bewaring van bedrijfsmiddelen. Artikel 2 t/m 6 worden als relevant beschouwd voor het onderzoek en zullen hieronder worden toegelicht.

In artikel 2 van het reglement staat dat gedragingen worden toegerekend aan diegene die op de computer is ingelogd. De tekst van het artikel luidt als volgt:

Artikel 2.

1. De directie kan de beschikbaarheid van bedrijfsmiddelen beëindigen of beperken wanneer een medewerker de bedrijfsmiddelen gebruikt op een wijze die in strijd is met dit reglement.
2. Een medewerker die de beschikking heeft over e-mailfaciliteiten is verplicht zijn postbus regelmatig te controleren of te doen controleren. De directie kan hiervoor nog nadere aanwijzingen geven.
3. Gedragingen worden toegerekend aan degene die op de computer is ingelogd.
4. Het installeren van software en applicaties is niet toegestaan, tenzij vooraf toestemming is verleend door de directie. Deze toestemming wordt alleen verleend als wordt voldaan aan de geldende rechten en eventuele licenties worden betaald.

In artikel 4 van het reglement staat dat het een medewerker niet is toegestaan om door het gebruik van bedrijfsmiddelen, schade te berokkenen aan de provincie Drenthe als instantie, haar werknemers en/of aan derden. De tekst van het artikel luidt als volgt:

Artikel 4.

1. De gebruiker mag alleen gebruikmaken van de bedrijfsmiddelen die beschikbaar worden gesteld door de provincie Drenthe. Uitzonderingen op deze bepaling zijn slechts mogelijk met schriftelijke toestemming van de directie. Aan deze toestemming kunnen voorwaarden worden verbonden.
2. Het is de gebruiker niet toegestaan om door middel van het gebruik van bedrijfsmiddelen zich zodanig te gedragen dat:
- de goede naam van de provincie kan worden geschaad;
- het ongestoord functioneren van de technische infrastructuur van de provincie in gevaar wordt gebracht;
- de vertrouwelijkheid van gegevens kan worden geschaad;
- het strijdig is met geaccepteerde omgangsvormen of goede zodon, belastend is voor de goede werksfeer dan wel beledigend is voor medewerkers en/of derden;
- het onrechtmatig is of een strafbaar feit oplevert;
- het strijdig is met de CAP;
- de provincie op enigerlei andere wijze dan op vorenstaande genoemde wijzen kan worden geschaad, hetzij in financiële zin, hetzij anderszins.
3. Het gebruik van middelen gericht op het verhinderen van kennisname binnen de provinciale organisatie van de inhoud van berichten en bijlagen door anderen dan de opsteller is niet geoorloofd. Van deze bepaling kan door de directie ontheffing worden verleend. Aan de ontheffing kunnen voorwaarden worden verbonden.

4. Gebruik van bedrijfsmiddelen voor privé-doeleinden wordt toegestaan mits met mate, uitgedrukt in zowel tijd en kosten, en niet in strijd met dit reglement. Voor het privé-gebruik van bedrijfsmiddelen kan de directie een financiële vergoeding vragen.

In artikel 5 van het Reglement gebruik bedrijfsmiddelen (2006) staat omschreven hoe de observatie en controle van gebruiksmiddelen plaatsvindt en welk doel het dient. Er staat onder meer in dat de directie ten allen tijde opdracht kan geven tot observatie. In artikel 6 wordt nader ingegaan op de regels omtrent het bewaren van gegevens. In dit artikel staat onder andere vermeld dat e-mails bewaard worden overeenkomstig de termijnen van de Archiefwet.

4.3.2 Uitvoeringsprogramma Drenthe (2006-2007)

In dit uitvoeringsprogramma (getiteld: Welkom in digitaal Drenthe) staat omschreven welke stappen de provincie onderneemt om de inzet van IT te verbeteren. Hoofdstuk 2 van dit document is het informatiestatuut. In dit statuut wordt specifiek ingegaan op het onderwerp informatiebeveiliging. Hierin wordt gesteld dat de provincie werkt op basis van de Code voor Informatiebeveiliging en dat in de planperiode wordt gestreefd naar een volledige invulling daarvan. Daarnaast staat beschreven dat medewerkers als gebruikers van de IT-hulpmiddelen geen misbruik mogen maken van de aan hen toevertrouwde middelen en gegevens. Zij mogen deze middelen slechts gebruiken voor hun werkzaamheden voor de provincie.

4.3.3 Beleidskader informatiebeveiliging provincie Drenthe (februari 2009)

In het Beleidskader informatiebeveiliging provincie Drenthe (getiteld: Veilig, integer en vertrouwd: hoe is onze informatie beveiligd?) wordt beschreven hoe ambtenaren van de provincie Drenthe dienen om te gaan met informatiebeveiliging.
In het beleidskader worden de volgende definities gehanteerd:

*'**Informatie** is een bedrijfsmiddel dat, net als andere belangrijke bedrijfsmiddelen, waarde heeft voor de organisatie en voortdurend op een passende manier beveiligd dient te zijn.*
Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden of in gesproken vorm). Welke vorm de informatie ook heeft of op welke manier ze ook wordt gedeeld of verzonden, ze dient altijd passend beveiligd te zijn.

***Informatiebeveiliging** bestaat uit het treffen van maatregelen die beogen te voorkomen dat onbevoegden vertrouwelijke gegevens kunnen bezitten, raadplegen of beschadigen.*
Informatiebeveiliging wordt gekarakteriseerd als het waarborgen van:
Veilige beschikbaarheid: geautoriseerde gebruikers hebben op de juiste momenten tijdig toegang tot informatie en aanverwante bedrijfsmiddelen;
Integriteit: correctheid en volledigheid van informatie en de verwerking daarvan;
Vertrouwelijkheid: informatie is alleen toegankelijk voor degenen, die hiertoe geautoriseerd zijn en daarmee op de juiste wijze omgaan'.

Als uitgangspunt voor het informatiebeveiligingsbeleid wordt door de Provincie Drenthe de Code voor Informatiebeveiliging (NEN/ISO 270001 en 270002) gehanteerd. In deze code worden de volgende tien categorieën noodzakelijke beveiligingsmaatregelen onderscheiden:

1. Beveiligingsbeleid
2. Beveiligingsorganisatie
3. Classificatie en beheer van bedrijfsmiddelen
4. Beveiligingseisen ten aanzien van personeel.
5. Fysieke beveiliging en beveiliging van de omgeving
6. Beheer van communicatie- en bedieningsprocessen
7. Toegangsbeveiliging
8. Aanschaf, ontwikkeling en onderhoud van systemen
9. Continuïteitsmanagement
10. Naleving.

In het handboek Informatiebeveiliging worden deze bovenstaande onderwerpen en de regelingen omtrent naleving meer in detail behandeld.

4.3.4 Handboek Informatiebeveiliging (2005)

Dit document geldt als bijlage bij het Beleidskader informatiebeveiliging en is bestemd voor de afdeling automatisering van de provincie Drenthe. De tien beveiligingsmaatregelen, zoals in de vorige paragraaf beschreven, worden hierin uitgebreid behandeld. Met name wordt ingegaan op de richtlijnen, procedures en werkwijzen van de beveiligingsmaatregelen. Deze maatregelen gelden als basisnorm waaraan de provincie Drenthe zich minimaal wil houden om veilig, integer en vertrouwd met informatie om te gaan.
In deze paragraaf wordt stilgestaan bij drie relevante hoofdstukken uit dit handboek.

Hoofdstuk 5: Classificatie en beheer bedrijfsmiddelen
In dit hoofdstuk wordt beschreven op welke wijze informatie geclassificeerd kan worden en welke typen er bestaan. Op deze manier wordt het duidelijk welke toegangsrechten er verbonden zijn aan een bepaalde classificatie,zoals vertrouwelijkheid. De volgende typen classificaties worden onderscheiden:

- ***Openbaar***
  Informatie die voor derden toegankelijk is (lezen). Wijzigen van deze informatie kan uitsluitend door medewerkers van de Provincie (eigenaar) plaats vinden.

- ***Niet Openbaar,*** *onderverdeeld in:*
  - *Intern gebruik:*
    Alle interne informatie die uitsluitend voor medewerkers van de provincie Drenthe toegankelijk is. Op basis van functie worden toegangsrechten tot deze informatie toegekend.
  - *Vertrouwelijk:*
    Informatie die uitsluitend voor een beperkte groep medewerkers van de provincie toegankelijk is. Bij de informatie dient aangegeven te worden wie toegang heeft tot de informatie.
  - *Persoonlijk:*
    Informatie uitsluitend bestemd voor de geadresseerde.

In dit hoofdstuk staat beschreven hoe informatie gelabeld dient te worden:
'Labelen en verwerken van informatie

- *Voor alle informatiesystemen wordt de geldende classificatie van informatie vastgesteld.*
- *Informatie zonder label wordt als "Intern gebruik" behandeld.*
- *Documenten met vertrouwelijke en persoonlijke informatie dienen op de voorpagina en in de koptekst voorzien te zijn van het label.'*

Hoofdstuk 8: Beheer van communicatie- en bedieningsprocessen; Onderwerp: Beleid ten aanzien van e-mail
In dit hoofdstuk wordt het beleid rondom het gebruik van e-mail beschreven. Hier wordt onder meer gesteld dat het niet toegestaan is om vertrouwelijke informatie te verzenden via de e-mail. Daarnaast wordt gesteld dat de provincie de e-mail alleen voor informele communicatie mag gebruiken.

Hoofdstuk 12: Naleving; Onderwerp: Beveiliging van bedrijfsdocumenten
In dit hoofdstuk wordt onder meer ingegaan op welke wijze bedrijfsdocumenten dienen worden beschermd tegen verlies, diefstal, vernietiging en vervalsing.
Naast de classificatie en labelling van informatie zoals beschreven in hoofdstuk 5, worden er extra maatregelen ondernomen om informatie optimaal te beveiligen. Deze maatregelen staan als volgt beschreven:

- *'Vertrouwelijke informatie dient in afgesloten kasten te worden bewaard na werktijd en bij het verlaten van de werkruimte*
- *Belangrijke systeeminformatie (systeemtoegang) dient centraal in een afgesloten ruimte bewaard te worden.*
- *Applicatiebeheerders beheren systeemdocumentatie van de diverse informatiesystemen. Deze documentatie bestaat uit:*
  - *Documentatie inzake de logische werking;*
  - *Documentatie inzake de technische werking;*
  - *Contracten e.d. met de leverancier(s) van de applicatie (archief);*
  - *Kwaliteitsgegevens over het systeem (meta-informatie);*
- *Bij het gebruik van elektronische opslagmedia worden maatregelen getroffen die ervoor zorgen dat de informatie leesbaar blijft (zowel de media zelf, als het gegevensformaat) gedurende de gehele bewaarperiode, teneinde te voorkomen dat de informatie verloren gaat ten gevolge van toekomstige technologische veranderingen. Deze maatregelen met betrekking tot de houdbaarheid van gegevens betreffen uitsluitend actuele systemen.'*

5. KPMG rapport

Het KPMG rapport naar het 'lekken' van het Eurochamprapport dient als basis voor het onderzoek van de provinciale onderzoekscommissie. In dit hoofdstuk worden de belangrijkste bevindingen van het KPMG rapport besproken.

5.1 Onderzoeksvraag en conclusies KPMG

De onderzoeksvraag voor het onderzoek van KPMG luidde als volgt:

'Is het definitieve rapport van Deloitte Forensic Services inzake Stichting Eurochamp Foundation voortijdig verspreid vanuit het Provinciehuis? Zo ja, op welke wijze, wanneer en door wie?'

De conclusie van KPMG is dat het definitieve rapport van Deloitte buiten het Provinciehuis terecht is gekomen, voordat het openbaar is gemaakt op 27 november 2009. KPMG heeft niet kunnen vaststellen op welke wijze dit is gebeurd en door wie.

KMPG heeft in haar rapport de belangrijkste feiten samengevat op een rijtje gezet. Deze luiden als volgt:

- 'De versie van het rapport die is verspreid voordat het rapport openbaar is gemaakt op 27 november 2008 betreft het definitieve *'Rapport inzake onderzoek naar de Stichting Eurochamp Foundation'*. Het rapport heeft het referentienummer 3112182270/2111.
- De versie die de heer Klaver in zijn bezit heeft vanaf 21 november 2008, betreft de digitale (pdf-) versie van voornoemde rapportage.
- De digitale (pdf-) versie van de rapportage is in de periode tussen 10 en 16 november niet verder per e-mail verspreid.
- De informant heeft verklaard dat hij de wetenschap heeft dat een exemplaar van het rapport in ieder geval op de ochtend van 13 november in het bezit is van Dagblad van het Noorden.
- Het Dagblad van het Noorden heeft aangegeven inzage te hebben gehad in de rapportage. Dit is in een redactioneel commentaar in Dagblad van het Noorden bevestigd. Niet is aangegeven welke versie van het rapport door Dagblad van het Noorden is ingezien.'

5.2 Uitgelekte versie

Door de onderzoekers van KPMG is vastgesteld dat er een aantal versies van het Deloitte rapport in omloop zijn geweest. Dit betreffen de volgende vier versies:

1. Een concept versie die in het kader van hoor en wederhoor aan de advocaat van een betrokkene in het Eurochamponderzoek is voorgelegd.
2. Een concept versie met nummer 3112182270/2135 die op 3 november 2008 per e-mail is verstuurd naar de provincie en op basis waarvan op 4 november 2008 overleg tussen de provincie Drenthe en Deloitte heeft plaatsgevonden.
3. De digitale versie van het definitieve rapport met nummer 311218227/2111 die op 10 november 2008 door Deloitte per email is verstuurd aan de secretaresse van de directie van de provincie, [redacted]
4. De ingebonden versie van het definitieve rapport met nummer 311218227/2111 die op 10 november 2008 door Deloitte per koerier aan de provincie is verzonden.

Door de onderzoekers van KPMG is vastgesteld dat het de digitale versie van het definitieve rapport (hierboven genoemd onder drie) betreft die uiteindelijk 'gelekt' is naar de buitenwereld, hoewel het woord 'lekken' niet als zodanig benoemd is. Het verschil tussen deze versie en de onder vier genoemde versie betreft volgens KPMG een lay out verschil. Tevens bevat de digitale versie van het definitieve rapport abusievelijk één pagina twee maal. Dit is bij de ingebonden versie niet het geval.

5.3 Kennis van de digitale versie

Volgens KPMG is de digitale versie van het definitieve rapport door Deloitte op 10 november 2008 om 14.11 uur verzonden aan de secretaresse van de directie van de provincie Drenthe, [redacted] Dit is gebeurd naar aanleiding van een telefoongesprek tussen een medewerker van Deloitte en [redacted]

Door Deloitte is er op 10 november 2008 telefonisch contact opgenomen met de provincie om mede te delen dat het rapport die middag per koerier aan de provincie zou worden verzonden. Door [redacted] is, volgens het onderzoek van KPMG, vervolgens uit eigen initiatief aangegeven dat zij ook graag een digitale versie van het rapport zou willen ontvangen. Deze versie is uiteindelijk om 14.11 uur die dag verzonden aan haar. Deze digitale versie van het rapport was volgens KPMG opgeknipt in drie aparte PDF-bestandjes, die als bijlagen bij één email zijn verzonden aan [redacted] Zij heeft deze email bewaard in een archief map van haar emailprogramma.
KPMG heeft niet kunnen achterhalen/vaststellen of de digitale versie tussen 10 en 13 november 2008 (de datum waarop de krant volgens de informant over een exemplaar van het rapport beschikte) verder digitaal is verspreid en/of gekopieerd op een externe mediadrager.
[redacted] zou in het interview met KMPG hebben gezegd dat haar inloggegevens van haar computer op dat moment bij niemand bekend zouden zijn geweest. Pas op 17 november 2008 zou zij deze gegevens hebben verstrekt aan de plaatsvervangend directeur. Op die datum heeft de plaatsvervangend directeur het rapport doorgezonden aan de landsadvocaat.
De gedeputeerde mevrouw Klip zegt tijdens het debat van 18 maart 2008 dat [redacted] twee andere medewerkers heeft geautoriseerd om toegang te krijgen tot haar inloggegevens (zie hoofdstuk 6). Dit komt niet overeen met de verklaring van [redacted]

Uit het KPMG rapport wordt niet duidelijk wie nu precies op de hoogte waren van het feit dat [redacted] een digitale versie van het rapport had ontvangen. In het rapport van KPMG staat hierover het volgende:
'*Er zijn volgens een aantal geïnterviewden een paar medewerkers en/of gedeputeerden op de hoogte dat het rapport op 10 november 2008 per mail is ontvangen van Deloitte.*'

De mogelijkheid bestaat dat de directie (directeur/secretaris en directeur/plaatsvervangend secretaris) hiervan op de hoogte was. Het was immers hun secretaresse die dit document in haar bezit had gekregen. Mogelijk zou ook de communicatie-adviseur van mevrouw Haarsma, de heer Van de Bosch, alsmede mevrouw Haarsma zelf hiervan op de hoogte kunnen zijn. Mevrouw Haarsma ontkent tijdens het debat dat later is gevoerd in PS, dat zij hiervan op de hoogte was.
Vermeldenswaard is dat mevrouw Haarsma op maandagmiddag 10 november 2008 op pad was met de plaatsvervangend secretaris van de provincie, mevrouw Weistra (dit staat overigens niet in het KPMG rapport, maar is mondeling medegedeeld). Mevrouw Weistra heeft diezelfde avond op het provinciehuis de doos met ingebonden rapporten in ontvangst genomen van de beveiliging van het provinciehuis, waarna de ongeopende doos in een afgesloten kast is opgeborgen.

Ook kan nog worden opgemerkt dat op 11 november 2008 een bespreking heeft plaatsgevonden over het Eurochamprapport. Bij die bespreking waren volgens KPMG aanwezig mevrouw Haarsma, de heer Van de Bosch, mevrouw Weistra en een vertegenwoordiger van Deloitte. Volgens het KPMG rapport zou uit de interviews met de betrokkenen zijn gebleken, dat deze bespreking heeft plaatsgevonden aan de hand van het concept rapport en dus niet op basis van het de dag daarvoor binnengekomen definitieve rapport.

5.4 Statenlid de heer Klaver

De fractievoorzitter van het CDA in PS, de heer Klaver, heeft een belangrijke rol gespeeld in de totstandkoming van het onderzoek van KPMG, als ook in het onderzoek zelf. De heer Klaver heeft in een schrijven (vermoedelijk aan GS) d.d. 21 november 2008 het verzoek gedaan tot het doen van een onderzoek naar de verspreiding van het Eurochamprapport. De inhoud van dit rapport zou volgens hem reeds bekend zijn bij de regionale media. De heer Klaver zou deze informatie hebben ontvangen van een informant, waarover in de volgende paragraaf meer.

De heer Klaver zou, blijkens het KPMG rapport, in de middag van 21 november 2008 van zijn informant te horen hebben gekregen dat de informant in de ochtend van 13 november 2008 de beschikking zou hebben gekregen over een versie van het Eurochamprapport. De heer Klaver heeft op vrijdagmiddag 21 november 2008 van zijn informant een kopie van deze versie van het rapport in zijn bezit gekregen.
Naast dit document, zou de heer Klaver ook meerdere e-mails in handen hebben gekregen. Uit één van die e-mails zou blijken dat het Dagblad van het Noorden 'een bron op hoogste bestuursniveau' van de provincie uit de wind wil houden. Dit heeft de heer Klaver tijdens het debat op 18 maart 2008 in PS verklaard. Tevens zou de heer Klaver in november en december 2008 een aantal anonieme brieven hebben ontvangen omtrent zijn rol in deze kwestie. KPMG heeft hiernaar verder geen onderzoek gedaan. De heer Klaver heeft hiervan aangifte gedaan bij de politie.

5.5 Rol informant

Het onderzoek van KPMG is mede gebaseerd op de verklaringen van een informant. KPMG heeft uitvoerig met deze informant (het betreft een man, afgaande op de mondelinge mededelingen van KPMG) gesproken De onderzoekers van KPMG betitelen de informatie van de informant als betrouwbaar. Letterlijk schrijven zij:
'*De bevindingen in deze rapportage zijn mede gebaseerd op vertrouwelijke informatie die wij van deze informant ter beschikking hebben gekregen. Wij achten de van deze informant verkregen informatie, op grond van de samenhang met andere voor het onderzoek beschikbare informatie, betrouwbaar.*'

De onderzoekers van KPMG kunnen (of willen) niet vertellen waarom deze informant zich tot de heer Klaver heeft gericht. Dit zou mogelijk de identiteit van de informant kunnen onthullen.

Over de persoon van de informant gaan inmiddels diverse geruchten rond. Daarbij wordt gesuggereerd dat de informant werkzaam zou zijn bij het Dagblad van het Noorden. Vooralsnog zijn deze geruchten echter niet bevestigd. Eén van de twee journalisten die verslag heeft gedaan van de bevindingen van het Eurochamprapport, zit momenteel ziek thuis. Gesuggereerd is dat dit te maken zou hebben met de kwestie van het lekken. Officieel wordt echter gesteld dat de journalist om gezondheidsredenen thuis zit.

Wat volgens KPMG vaststaat, is dat de informant de wetenschap heeft dat het Dagblad van het Noorden op de ochtend van 13 november 2008 in het bezit was van een exemplaar van het Eurochamprapport. Op 12 november 2008 zou de informant te horen hebben gekregen dat er een definitief rapport beschikbaar was.

De informant heeft zijn wetenschap op 21 november 2008 doorgespeeld aan de heer Klaver. Volgens KPMG heeft er een ontmoeting plaatsgevonden, waarbij door de heer Klaver een kopie is gemaakt van het rapport dat in het bezit was van de informant. De versie die in het bezit was van de informant betrof een print van de digitaal verzonden definitieve versie van het rapport.

5.6 Dagblad van het Noorden

Uit het KPMG rapport volgt dat twee journalisten van het Dagblad van het Noorden zich hebben bezig gehouden met het Eurochamprapport. Dit zijn de journalisten de heer De Bruin en de heer De Kleine. Hieronder wordt in chronologische volgorde hun betrokkenheid toegelicht.

Volgens KPMG heeft de heer De Bruin op 12 november 2008 een bezoek gebracht aan de advocaat van een van de betrokkenen van het Eurochamponderzoek. De journalist heeft hierover later aangegeven dat hij bij dit bezoek inzage heeft gehad in de versie van het rapport die de advocaat in zijn bezit had. Door de

advocaat wordt deze inzage ontkend. Uit het KMPG rapport volgt dat de advocaat, in ieder geval op dat moment, geen versie van het definitieve rapport in zijn bezit had, maar 'slechts' een gedeeltelijke concept versie die hem in het kader van hoor en wederhoor was verstrekt. Naar aanleiding van dit bezoek zou de heer De Bruin het artikel '*Jan heeft geen strafbare feiten begaan'* hebben geschreven dat op 15 november 2008 is gepubliceerd.

Eveneens op 12 november 2008 was de heer De Bruin, volgens KPMG, aanwezig op een avondbijeenkomst op het provinciehuis. Hij zou daarbij hebben gesproken met de gedeputeerde mevrouw Haarsma. Mevrouw Haarsma zou naar aanleiding van dit 'gesprek' het idee hebben gekregen dat de journalist in het bezit zou zijn van het Eurochamprapport. Op een later moment heeft zij volgens KPMG de journalist hierover aangesproken en hem hierop bevraagd. De journalist zou daarbij hebben aangegeven dat hij inzage had gehad, maar dat hij zijn bronnen niet bekend zou kunnen maken.

Op donderdagmiddag 13 november 2008 heeft mevrouw Haarsma een gesprek gehad met journalist De Bruin. Bij dat gesprek was ook haar communicatieadviseur de heer Van de Bosch aanwezig. Bij dat gesprek zou, volgens het KPMG rapport, zijn gesproken over de 'wijze van aanbesteding', zoals die in het Eurochamprapport naar voren komt. (Op dat moment is de krant, volgens de informant, reeds in het bezit van het definitieve rapport.)

Op 15 november 2008 wordt in de krant het artikel '*Het rapport over opkomst en ondergang van Eurochamp'* gepubliceerd. In dat artikel wordt volgens KPMG gemeld dat de journalisten inzage hebben gehad in het Deloitte rapport over Eurochamp.

Op woensdag 19 november 2008 hebben de heren De Bruin en De Kleine volgens het KPMG rapport een bezoek gebracht aan de advocaat van een van de betrokkenen van het Eurochamprapport. Niet duidelijk wordt of dit dezelfde advocaat betreft als de eerdergenoemde advocaat.
Twee dagen later, op 21 november 2008, meldt de informant zich bij de heer Klaver.

5.7 Bevindingen digitaal onderzoek

Door KPMG is een forensisch IT onderzoek uitgevoerd. Daarbij heeft KPMG, zoals eerder opgemerkt, niet kunnen vaststellen of de digitale versie tussen 10 november 2008 14.11 uur en 13 november 2008 (de datum waarop de informant over deze versie beschikte en ook de krant over een versie (dezelfde?) beschikte) verder digitaal is verspreid en/of gekopieerd op een externe mediadrager.
Daartoe is onder andere de computer van [redacted] onderzocht. Daarbij heeft men niet kunnen vaststellen of zij tussen 10 november 2008 en 13 november 2008 de betreffende digitale versie heeft uitgeprint. Andere computers zijn niet onderzocht.
Tevens is door KPMG het e-mailverkeer aan de hand van logginggegevens onderzocht. Daarbij heeft men niet kunnen vaststellen dat andere medewerkers van de provincie en/of leden van GS de betreffende versie van het rapport tussen 10 en 16 november 2008 per email hebben ontvangen. KPMG concludeert dat de digitale (pdf-)versie van het rapport in de periode tussen 10 en 16 november niet verder per e-mail verspreid is

6. Debat in provinciale staten

Op 18 maart 2009 is in Provinciale Staten gesproken over het rapport van KPMG. Tijdens dit debat is besloten tot het instellen van een provinciale onderzoekscommissie. In het debat zijn een aantal zaken aan de orde gekomen die van belang zijn voor het onderzoek van de provinciale onderzoekscommissie. Dit betreft met name uitlatingen van leden van GS.

Mevrouw Haarsma heeft tijdens het debat gereageerd op een groot aantal vragen die haar zijn gesteld door leden van de PS.
Over het gesprek met de journalist De Bruin op woensdagavond 12 november 2008 heeft zij het volgende verklaard:
'Ik stond in de rij met mijn bordje, voor of naast mij – dat weet ik niet meer precies – stond collega Klip en aan de andere kant stond de journalist. De journalist stelde mij verschillende vragen, waarop ik geen antwoord heb gegeven en vervolgens heb ik tegen mevrouw Klip gezegd: "Het lijkt wel alsof het rapport bij het Dagblad van het Noorden is." Dat heb ik aan mevrouw Klip gemeld.
Vervolgens heb ik mijn bordje leeggegeten en daarna ben ik 's avonds met de fractievoorzitter naar huis gereden en heb ik nog eens over alles nagedacht. De volgende ochtend heb ik in aanwezigheid van mijn bestuursadviseur een afspraak menen te moeten maken met het Dagblad van het Noorden. De reden hiervoor was dat wij beiden vonden dat het in de media voornamelijk nog ging over het aanbestedingsbeleid, terwijl de echte inhoud volledig uit het zicht was verdwenen. Mijn communicatie-adviseur en ik hebben met de journalist een gesprek gehad, in welk gesprek mijn eerste vraag aan hem was of er een rapport in het bezit was van het Dagblad van het Noorden. De journalist heeft geantwoord dat er geen rapport in het bezit van het dagblad was, dat ook hij geen rapport had, maar dat hij wel inzage in het rapport had gehad. Hij wist ook feilloos aan te geven wanneer dat was – het staat ook in het KPMG-rapport – want hij was woensdagochtend in Almere of Lelystad - waar precies weet ik niet meer – op bezoek geweest bij de advocaat van de heer Leijssenaar. Dat is wat de journalist mij heeft verteld.'

Over het opvragen van een digitale versie van het rapport verklaart zij het volgende:
'Ik kom bij een essentieel deel van het verhaal, het pdf-bestand. Op 14.11 uur is een pdf-bestand ontvangen. De heer Klaver heeft gevraagd op wiens verzoek en op wiens initiatief dit bestand is opgevraagd. Ik heb hiernaar uiteraard navraag gedaan bij de directie en mij is verteld dat de directie de secretaresse heeft gevraagd nog eens met Deloitte te bellen of de provincie het definitieve rapport daadwerkelijk die dag zou ontvangen. Wij vonden het nodig over het definitieve rapport te beschikken omdat wij voornemens waren om, zodra het college hierover de daaropvolgende dinsdag een besluit zou hebben genomen, aangifte te doen bij het OM.'

(...)

'De opdracht was niet te vragen of een pdf-bestand opgestuurd kon worden, maar wanneer het rapport binnen zou komen. Het antwoord was dat dit waarschijnlijk aan het eind van de dag zou zijn. Daarop heeft de secretaresse met de beste bedoelingen gevraagd het rapport per e-mail te sturen. Dat is gebeurd en die e-mail is om 14.11 uur ontvangen.
Dan is natuurlijk de volgende vraag wie wisten dat dit e-mail bericht zou binnenkomen, maar....'

(...)

'Wie wist dat het pdf-bestand bij de provincie is terechtgekomen? Dat waren een aantal medewerkers, een paar collegeleden en de directie. Ik kan naar eer en geweten zeggen dat ik het niet wist.'

Deze verklaring van mevrouw Haarsma komt niet geheel overeen met hetgeen door KPMG aan de onderzoekscommissie is verteld. Volgens KPMG heeft Deloitte gebeld met de provincie en heeft de secretaresse toen uit eigen beweging gevraagd naar een digitale versie van het rapport. Later tijdens het debat spreekt mevrouw Haarsma over medewerkers en/of gedeputeerden.

Mevrouw Haarsma stelt in het debat dat zij wel op de hoogte was van het feit dat het rapport van Deloitte op 10 november 2008 zou binnenkomen:
'Ik wist dat de doos binnen kwam, want ik had die dag met de plaatsvervangend directeur een bespreking bij de NAM in Assen en toen wij op het provinciehuis terug kwamen, was de doos gearriveerd. De plaatsvervangend directeur heeft toen gezegd de doos bij haar in de kast te zetten, omdat de volgende dag de besluitvorming op basis van de oplegnotitie zou plaatsvinden. Het was daarna aan de directie om op enig moment, omdat het in de aanloop naar de aangifte toch wel relevant werd de doos eens te openen, te openen. Daar heb ik mij niet mee bemoeid. '

Mevrouw Haarsma verklaart over haar gesprek met de journalist De Bruin op 13 november 2008 het volgende:
'Het volgende punt dat ik wil bespreken is de verwevenheid. De heer Klaver heeft gevraagd hoe het in dit huis met die verwevenheid zit. Net als hij vinden wij het belangrijk ons product goed te verkopen en wij – en ik spreek expres in de wij-vorm – vinden dat wij op een correcte en integere manier met de pers omgaan. Dat is het waardeoordeel dat ik namens het college kan geven.
Ik kom op 13 november, dat datum waarop ik in aanwezigheid van mijn bestuursadviseur een gesprek heb gehad met de journalist. Er is toen uitvoerig gesproken over het feit dat mij was opgevallen dat het eigenlijk alleen nog maar over de aanbestedingsregels ging en niet meer over waarvoor het onderzoek was gestart, namelijk de vraag wat er onrechtmatig was gebeurd. Het was niet zo dat wij de aanbestedingsregels onbelangrijk vonden, integendeel, maar de kern waarop het onderzoek zich diende te richten waren de handelingen die in onze optiek niet door de beugel konden. Dat heb ik met de pers besproken, niet meer en niet minder en dat gesprek heeft pakweg drie kwartier geduurd. '

(...)

'Dat is heel simpel. Ik heb net al gezegd dat ik met de communicatieadviseur had besproken dat de zaak wel een gekke wending nam, omdat het bericht alleen ging over de aanbesteding, terwijl het volgens ons ook om heel andere zaken ging. Wij besloten een afspraak met het Dagblad van het Noorden te maken om ook die kant van de medaille te laten zien.'

Mevrouw Haarsma stelt hier dat er in een bericht voornamelijk alleen nog maar wordt gesproken over de aanbestedingsregels. Onduidelijk is aan welk bericht zij refereert. Op het moment van het gesprek met de journalist is het artikel over het rapport nog niet verschenen. Wellicht refereert zij aan andere berichten in de media. De onderzoekscommissie dient mevrouw Haarsma hierover tijdens het voorgesprek nader te bevragen.

Mevrouw Klip reageert in het debat onder meer op een vraag van de heer Klaver of de secretaresse van de directie haar inloggegevens heeft gedeeld met anderen:
'Mijnheer de voorzitter. Ik heb nog twee vragen van de heer Klaver openstaan.

De eerste ervan was of de betreffende medewerker van het directiesecretariaat haar wachtwoord ook aan anderen heeft gegeven, met andere woorden of ook anderen in de bestanden op de computer van de bewuste medewerker van het directiesecretariaat kunnen komen.
Op pagina 15 van het rapport van KPMG staat dat die medewerkster haar wachtwoord heeft gegeven aan de directeur/plaatsvervangend secretaris zodat die het bestand naar haar eigen computer kon overbrengen om het vervolgens te verzenden naar de landsadvocaat. Verder heeft deze medewerker van het directiesecretariaat twee mensen gemachtigd om via hun eigen e-mailaccount in haar bestanden te komen. Het gaat dan om haar kamergenoot en de secretaresse van de CvdK.'

Uit dit antwoord volgt dat er mogelijk twee mensen zijn die in de periode tussen 10 en 13 november 2008 reeds in de bestanden van [redacted] konden komen, te weten de kamergenoot (onduidelijk is wie dit is) van [redacted] en de secretaresse van de Commissaris van de Koningin. Dit gegeven volgt niet uit het KPMG rapport.

Tijdens het debat laat gedeputeerde mevrouw Klip zich ook uit over het integriteitbeleid van de provincie en het onderwerp informatiebeveiliging:
'Voorzitter. Ik kom op mijn andere verantwoordelijkheid: de portefeuille personeel en organisatie. Waar gaat dat over? Het gaat daarbij om de besteding van personeelsbudgetten, samen met de portefeuillehouder financiën, het gaat over organisatieontwikkeling en reorganisatie en het gaat dan inderdaad ook over integriteitbeleid. Het Rijk heeft het integriteitsbeleid hoog in het vaandel en hetzelfde geldt voor deze provincie. Dit betekent dat wij allerlei dingen uit een voorschriftenlijst van het Rijk moeten implementeren in onze organisatie. Ik noem er een paar. Het gaat over gedragscodes, over noodzakelijke onderzoeken bij werving en selectie, het gaat over het kwalificeren van kwetsbare functies en de mogelijk niet integere relatie waarvan tussen bepaalde bevoegdheden en functies sprake kan zijn, het gaat over het afleggen van de ambtseed of –belofte, het gaat over het inventariseren van nevenwerkzaamheden, het gaat over relatiegeschenken en zo kan ik nog wel even doorgaan.
Implementeren is een en op een puntje na hebben wij dit allemaal al geruime tijd geleden gedaan. In alle monitoringsrapportages van het Ministerie van BZK scoren wij heel hoog. Maar dat is niet alles, want wij moeten die integriteit ook levend houden. Er moet voor gezorgd worden dat ambtenaren zich er voortdurend bewust van zijn. Dat betekent dat wij rond het afleggen van de ambtseed een programma organiseren dat er op gericht is dat mensen zich hiervan bewust zijn. Dat gebeurt via programma's op internet en via gesprekken binnen de verschillende teams.
Toch – en dat hebben wij de staten ook op papier laten weten – lijkt het ons naar aanleiding van de huidige situatie niet alleen verstandig maar ook noodzakelijk ons integriteitsbeleid nogmaals tegen het licht te houden. Daarbij kan gedacht worden aan nog dwingender gesprekken van managers en aan het incorporeren van bepaalde integriteitsaspecten in de individuele werkplannen van medewerkers. Daarvoor kunnen allerlei vormen gevonden worden en wij starten daar ik zou bijna zeggen morgen mee.
Daarnaast houden wij ook – dit hebben wij de staten ook laten weten – het huidige beleid op het gebied van informatiebeveiliging en fysieke beveiliging – het gaat dan om het gebouw – opnieuw tegen het licht.
Collega Baas, kenner op dit gebied en bovendien verantwoordelijk portefeuillehouder, zal daar straks meer over zeggen. Want de opmerking dat de vertrouwelijkheid van onze provinciale informatie gewaarborgd moet zijn, is volstrekt terecht. Maar – en dat is niet een maar van "ach, het doet er niet toe," maar dat is de maar van de realiteit – wij kunnen als openbaar bestuur in een openbaar, of bijna openbaar toegankelijk gebouw zowel fysiek als digitaal geen vesting worden.
Integriteit zit tussen de oren. Wij hebben als bestuur en als directie de verantwoordelijkheid om zowel via de structuur, waarvan ik zojuist een aantal voorbeelden heb genoemd, als via een permanent proces van bewustwording en bewust houden, ervoor te zorgen dat die integriteit ook tussen de oren blijft zitten.
Uiteindelijk moet dit ertoe leiden – maar in deze mensenwereld blijft dat een utopie – dat integriteit een

vanzelfsprekendheid is. Daar zetten we erg op in en daar gaan we naar aanleiding van deze gebeurtenis nog strakker op inzetten.
Voorzitter. Ik kom op de vragen die gesteld zijn aangaande de medewerker van het secretariaat.
Wij hebben een hele reorganisatie en een organisatieontwikkeling achter de rug. Wij proberen – de staten zijn daarover de afgelopen jaren voldoende bijgepraat – onder mijn bestuurlijke verantwoordelijkheid een provincie voor de toekomst te worden. Dat betekent niet binnenskamers heel goed zijn in je eigen vakgebied, maar van buiten naar binnen samen met de buitenwereld zorgen dat die ontwikkelingen tot stand gebracht worden waar de maatschappij om vraagt. Dat betekent dat wij steeds de nadruk leggen op proactieve ambtenaren, ambtenaren die meedenken met het bestuur en zo zelf nadenken over wat er nodig zou zijn.
Natuurlijk is er een grens aan proactief handelen en – ik moet nu even gaan voorlezen wat ik al eerder aangeleverd heb gekregen – de vraag of een ambtenaar, in dit geval een medewerker van het directiesecretariaat op eigen houtje een vertrouwelijk pdf-file kan aanvragen, moet ik als volgt beantwoorden. Ik citeer: "Iedere ambtenaar is bevoegd en bekwaam voor zijn functie en wordt geacht keuzes te maken die passen bij en vallen binnen de verantwoordelijkheid en bevoegdheid van de functie." Dat is een citaat uit de Collectieve arbeidsvoorwaarden van de provincies (CAP) die gelden voor alle 12 provincies en zijn vastgelegd in CAO-afspraken.
Deze keuze van de medewerker van de directiesecretariaat valt binnen die kaders.'

De gedeputeerde de heer Baas heeft zich in het debat ook uitgelaten over het onderwerp informatiebeveiliging:
'Mijnheer de voorzitter. Ik wil nog graag een aantal aanvullende opmerkingen maken, die betrekking hebben op het door ons gevoerd informatiebeleid, ook in relatie tot de zaak die vanmiddag zo nadrukkelijk speelt. Daarbij wil ik ook van mijn kant nog eens benadrukken – het wordt bijna saai – dat ook informatiebeveiliging valt of staat met de zorgvuldigheid en integriteit waarmee iedereen in deze organisatie daarmee omgaat. Er kunnen nog zoveel voorschriften, maatregelen, protocollen en procedures gemaakt worden, als er niet op een goede manier invulling aan wordt gegeven, is het risico dat er dingen fout lopen, altijd aanwezig. Ook dit is mensenwerk en fouten zijn nooit en in geen enkele organisatie uit te sluiten. Dit is uiteraard geen excuus dat het is voorgevallen; het is ernstig genoeg dat het is gebeurd en dat dit nu zoveel van onze tijd kost.
De huidige maatregelen die binnen de provincie Drenthe gelden met betrekking tot de informatiebeveiliging zijn vastgelegd in ons Handboek informatiebeveiliging. Dit handboek is gebaseerd op de binnen de gehele overheid geldende code voor informatiebeveiliging. Die code dateert uit de jaren tachtig/negentig van de vorige eeuw en die geldt binnen de rijksoverheid en de provinciale en gemeentelijke overheden als basis voor alles wat op het gebied van informatiebeveiliging in dit land moet worden gedaan. Binnen de provincie is dat verankerd in het Informatiestatuut.
Het Handboek informatiebeveiliging schrijft voor de informatiebeveiliging multidisciplinair te benaderen en integraal in de organisatie te beleggen in termen van verantwoordelijkheden. Dat wordt nader uitgewerkt in concrete maatregelen, gerubriceerd op onderwerp. De relevante onderwerpen op het gebied van toegang tot en verspreiding van informatie zijn als volgt in dat handboek vastgelegd.
- *Toegang tot informatie wordt bepaald door enerzijds de authenticatie en anderzijds de autorisatie van personen.*
- *Voor wat betreft de vaststelling van identiteit en de bevestiging daarvan, de authenticatie, zijn de maatregen in dat Handboek informatiebeleid vastgelegd en geïmplementeerd. Iedereen heeft een gebruikersnaam en een wachtwoord en die combinatie is altijd noodzakelijk om in de pc te komen en buiten het provinciehuis is er zelfs nog een token nodig om toegang tot het systeem te krijgen.*
- *De toegang tot de informatie binnen de systemen, de toegangsrechten, dus de autorisatie, is geregeld op grond van de functie die een medewerker heeft. Iemand die bij bodem werkt, komt niet in het deel dat bestemd is voor de treasury.'*

(...)

'Ik ga verder.
Dit noemen wij het rol-gebaseerde autorisatiemodel. De verantwoordelijkheid voor de juiste toegangsrechten ligt bij het functioneel beheer.
Er is een heel proces voor de uitgifte en het beheer van gebruikersnamen, wachtwoorden en toegangsrechten. Het toont allemaal aan dat het in dit huis conform alle overheidsregels is geregeld, maar – alweer – het gaat er ook om in hoeverre daar zorgvuldig, verantwoord en integer gebruik van wordt gemaakt.
Dat geldt ook voor het afdrukken van informatie op printers; alle decentrale copyers en printers hebben de mogelijkheid om met een persoonlijke code te printen en daar de printen af te halen, dit alles om te voorkomen dat ook onbevoegden documenten kunnen printen waarover zij niet de beschikking behoren te krijgen.
Het informatiebeleid is ontzettend afhankelijk van alle ontwikkelingen op ict-gebied en die ontwikkelingen gaan heel snel. In 1997 zaten we nog in de tijd van de visstick en nu inmiddels in de tijd van de usb-stick. Dat vergt een doorlopende aanpassing van het systeem. De code voor informatiebeveiliging van overheidswege is in 2007 weer geactualiseerd; het beleidskader informatiebeveiliging van dit huis is daarop gebaseerd en is inmiddels door de directie vastgesteld. De basisnormen en maatregelen voor informatiebeveiliging zijn ook afgerond, maar die hebben wij nog even aan KMPG om advies voorgelegd, want wij willen voldoen aan de modernste en nieuwste eisen op het gebied van ICT, die van ons worden verlangd.
Hoe het zit met de fysieke toegang tot het gebouw weten de statenleden als geen ander. Er is alleen toegang tot het provinciehuis, althans dat gedeelte dat buiten het openbare gedeelte van de hal ligt, te verkrijgen door middel van een toegangspas. De gebruikers van het gebouw zijn in verschillende categorieën ingedeeld: bestuur, medewerkers in vaste dienst, medewerkers in tijdelijke dienst, staten- en commissieleden, leveranciers, bezoekers en dienstverleners. Zij zijn allemaal geautoriseerd op het niveau dat voor hun werk noodzakelijk is. Ook dat is allemaal keurig vastgelegd in ons autorisatiereglement.
Voor alle gebruikers geldt draagplicht van de pas.'

Over het rapport op de computer van [redacted] zegt de heer Baas onder meer nog het volgende:
'Het is in ieder geval zo dat de bijlage bij de e-mail niet apart op de pc is opgeslagen. Het rapport is dus gewoon als bijlage bij de e-mail in het bestand blijven zitten.
Maar ik moet nu even op mijn gezonde boerenverstand afgaan en dat is veel slechter dan dat van een hacker: als ik thuis op de pc van de betrokken secretaresse wil inloggen, moet ik beschikken over zowel haar password en gebruikersnaam als haar token. Om die drie hindernissen te overwinnen, moet je toch heel wat mans zijn en wat mij betreft is het haast onmogelijk dat te doen.
Voor wat de heer Vester aangeeft met betrekking tot het gebruik van een usb-stick en printers, zitten op het huidige systeem geen programma's. '

7. Aandachtspunten vervolgonderzoek

De informant beschikte over de digitale versie van het definitieve rapport. Uit het KPMG onderzoek blijkt niet dat dit ook de versie is waarover het Dagblad van het Noorden beschikte. Dat is echter wel waarschijnlijk, aangezien de informant heeft bevestigd dat hij de wetenschap heeft dat een exemplaar van het rapport op de ochtend van 13 november in het bezit is van Dagblad van het Noorden. Het 'lekken' moet hebben plaatsgevonden tussen maandag 10 november 2008 14.11 uur (het moment van ontvangst van het digitale rapport) en donderdagochtend 13 november 2008 12.00 uur, het moment dat het rapport volgens de informant in het bezit is van het Dagblad van het Noorden.

Uit het KPMG rapport wordt niet duidelijk wie, naast [redacted] in de betreffende periode kennis heeft van de ontvangst/het bestaan van een digitale versie van het rapport. Dit is het eerste punt van aandacht voor het vervolgonderzoek van de onderzoekscommissie: vaststellen (door middel van interviews) wie binnen de provincie kennis had van het bestaan van een digitale versie van het rapport in de periode 10 tot en met 13 november 2008.

Uit het onderzoek van KPMG is niet vast komen te staan of het rapport in de periode 10 tot en met 13 november 2008 verder digitaal is verspreid en/of gekopieerd op een externe mediadrager. Ook is niet duidelijk geworden wie mogelijk toegang hadden tot de computer van [redacted]
Dit betreft het tweede aandachtspunt voor het vervolgonderzoek: vaststellen (door middel van interviews) van de kring van personen die in de betreffende periode toegang hadden tot de computer of de e-mail van [redacted] en het eventueel nader onderzoeken van de computers van deze betreffende personen.

De bestudering door een forensisch IT expert van BING van de resultaten van het digitale onderzoek van KMPG zou mogelijk nieuwe aanknopingspunten kunnen opleveren voor nader te doen forensisch IT onderzoek. Wellicht dat hiermee nieuwe informatie kan worden verkregen over de eventuele verspreiding van het Eurochamprapport in de periode 10-13 november 2008. Op dit moment zijn deze gegevens nog niet bekend. De bestudering van het materiaal van KPMG en de resultaten van het door BING te verrichten aanvullend forensisch IT onderzoek vormen daarmee het derde aandachtspunt voor het vervolgonderzoek van de onderzoekscommissie.

Andere aandachtspunten voor het vervolgonderzoek, gericht op de lekvraag, zijn kort samengevat:

- Zo mogelijk controleren van de informatie van de informant en het vaststellen van de betrouwbaarheid van de informant;
- Verkrijgen en bestudering van andere 'bewijsstukken' zoals de uitgelekte emails die heer Klaver in zijn bezit zou hebben en waaruit zou blijken dat het Dagblad van het Noorden een hooggeplaatste bestuurder uit de wind zou willen houden;
- Vaststellen door middel van interviews van de motieven voor mevrouw Haarsma en haar communicatieadviseur om actief de pers op te zoeken (benaderen van de heer De Bruin) om te praten over een op dat moment nog vertrouwelijk rapport;
- Bestudering van de verschillen tussen de concept versie van het rapport en de definitieve versie van het rapport;
- Bestudering van de verschillen tussen de concept versie van het rapport die de advocaat in zijn bezit heeft gehad in het kader van hoor en wederhoor en de andere versies van het rapport;
- Bestudering van verslag van PS bijeenkomst op 11 november 2008 waarin geheimhouding over rapport Eurochamp zou zijn opgelegd

Naast bovengenoemde aandachtspunten, dient er in het vervolgonderzoek ook nadrukkelijk te worden stilgestaan bij de beantwoording van de tweede en derde onderzoeksvraag:

- waren er bij de provincie Drenthe organisatorische en/of 'bestuurlijk-culturele' factoren die de voortijdige verspreiding hebben bevorderd?
- in hoeverre moet het gevoerde bestuur worden aangepast om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen?

Voor de beantwoording van deze vragen, dienen - naast de bestudering van de relevante documenten (zie hoofdstuk 4)- in de interviews vragen te worden gesteld aan zowel bestuurders als ambtenaren over zaken als:

- Hoe worden contacten met journalisten onderhouden?
- Is men op de hoogte van wet- en regelgeving op dit gebied?
- Wordt er in werkoverleggen en in GS/PS bijeenkomsten stilgestaan bij onderwerpen als contacten met de pers, informatiebeveiliging, vertrouwelijkheid van documenten?
- Hoe wordt het afleggen van de eed/gelofte door werknemers ervaren?
- Leeft integriteit als onderwerp binnen de provincie?
- Waaruit blijkt dat, welke concrete aandacht krijgt het?
- Wat zou er volgens de mening van betrokkenen dienen te veranderen om het risico van nieuwe incidenten te beperken?

8 Tot slot

Wij vertrouwen hiermede aan het eerste deel van onze opdracht te hebben voldaan.

Hoogachtend,

[redacted]
Directeur

BIJLAGE I:

Lijst van geraadpleegde documenten

1. KPMG rapport, Onderzoek naar mogelijke voortijdige verspreiding rapport Eurochamp, 10 maart 2009.
2. Schriftelijke weergave debat in PS op 18 maart 2009.
3. Reglement gebruik bedrijfsmiddelen (2006)
4. Uitvoeringsprogramma Drenthe (2006-2007), Welkom in digitaal Drenthe.
5. Beleidskader informatiebeveiliging provincie Drenthe (februari 2009), Veilig, integer en vertrouwd, hoe is onze informatie beveiligd?
6. Basisnorm maatregelen informatiebeveiliging (bijlage bij beleidskader informatiebeveiliging).
7. Handboek informatiebeveiliging (2005).
8. Diverse functiebeschrijvingen.
9. Gedragscode ambtelijke integriteit (maart 2003, laatste update 10 oktober 2008).
10. Drentse gedragscode integriteit voor de CvdK, GS en PS.
11. Organogram Provincie Drenthe.
12. Organisatiebesluit Provincie Drenthe 2008.
13. Meer samen, nóg sterker, Besturings- en managementconcept, oktober 2007.
14. *Het rapport over de opkomst en ondergang van Eurochamp*, Dagblad van het Noorden, 15 november 2008, door Gerard de Kleine en Martin de Bruin
15. *Advocaat: Jan heeft geen strafbare feiten begaan,* Dagblad van het Noorden, 15 november 2008.
16. *J'accuse!,* column van Denker (bronvermelding...)

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
22 april 2009

Aanwezig: Leo Bomhof (voorzitter), Margriet Stijkel, Jan Langenkamp, Herman Beerda, Sietze de Jong Renee Westerhof en [redacted] (Comm.).
Inge Rozema (secretaris).

3. Verslag van 8 april 2009
Het verslag wordt vastgesteld. In de komende verslagen zullen de openstaande afspraken steeds worden bijgehouden. Er moet een brief aan RTV-Drenthe worden gestuurd met het verzoek om een transcript van de column van de heer Denkers uit Cassata.

4. Kennismaking externe ondersteuning → BING volgt aule planning.
De heren [redacted] van BING schuiven halverwege de vergadering aan. Hen wordt gevraagd een planning te maken van hoe zij het proces zien. Wat is wanneer gereed. Er zijn reeds per mail en worden ook ter plekke stukken aangereikt ter bestudering. Deze zullen nog worden aangevuld met de opgevraagde stukken bij de ambtelijke organisatie. De secretaris zal z.s.m. nagaan wanneer deze beschikbaar komen *(NB: dat is op zijn vroegst a.s. maandag, IR.)*
Het bureau wordt gevraagd de commissie te helpen te blijven focussen op de onderzoeksvragen en geen zijpaden te bewandelen. Van hen wordt verwacht dat zij bij de interviews en hoorzittingen aanwezig zijn en de commissie helpen bij de voorbereiding ervan. Tijdens de interviews mogen ook zij (aanvullende) vragen stellen. Ze kunnen tussendoor feedback geven op het verloop van de interviews. Een interviewtraining wordt niet nodig geacht.
De voorzitter zou graag al tijdig een voorlopige inhoudsopgave van het rapport van de commissie willen hebben, om een idee te krijgen hoe e.e.a. eruit ziet. Ook zal al aan de rapportage gewerkt worden gedurende de fasen 1 en 2, voorzover mogelijk.
De heren geven aan, dat zij het van belang vinden te weten wat KPMG wel en niet in zijn onderzoek heeft betrokken. Besloten wordt om KPMG uit te nodigen voor een briefing aan de commissie.

5. Plan van Aanpak
Het PvA wordt definitief vastgesteld.

6. Voorbereiding interviews
Over de definitieve **lijst van te interviewen personen** kan nu nog niets worden gezegd. Dat moet volgen uit de desk-research. De lijst die er nu ligt is een voorlopige. Maar de mensen die erop staan dienen in ieder geval te worden bevraagd, vinden de aanwezigen. Aanvullingen kunnen later eventueel nog komen. Daartoe zal de informant ook moeten behoren. I.v.m. voldoende voorbereidingstijd voor de geïnterviewden kunnen aanvullende mensen pas in de week van 18 mei worden geïnterviewd. De mensen op de voorliggende lijst kunnen nu worden uitgenodigd.

De opgestelde concept-uitnodigingsbrief wordt akkoord bevonden.

De leden van de commissie zullen de **concept-vragenlijst** bestuderen en hun commentaar en/of aanvullingen vóór de volgende vergadering aan de secretaris doorgeven. De heren van BING zullen op grond van hun deskresearch uiterlijk in de week van 6 mei nadere adviezen geven m.b.t. de vraagstelling.

M.b.t. **de planning** van de interviews is er discussie over de volgorde van bevraging: eerst de bestuurders en dan de ambtenaren of andersom. De heren van BING adviseren de bestuurders als laatste te plannen en ook voldoende tijd tussen de gesprekken te plannen voor korte evaluaties. De heer De Jong pleit voor meer gesprekken op de woensdag.
Drie leden van de commissie zullen steeds (in wisselende bezetting) de interviews afnemen. De anderen kunnen daar ook bij zijn (hoeft niet), maar dan "op de achterbank". De geïnterviewden moeten niet negen mensen tegenover zich hebben zitten.

Het **protocol** voor de interviews (= informatieve gesprekken) zal met de uitnodiging aan de geïnterviewden worden meegezonden. Er moet nog in worden verwerkt, dat de geluidsbestanden worden vernietigd, zodra het schriftelijke verslag is goedgekeurd (door beide partijen). Wat betreft de eventuele bijstand voor de geïnterviewden: die is toegestaan, maar dient niet in de plaats te treden van de geïnterviewde. M.a.w. hij mag niet namens de geïnterviewde antwoorden.

7. Communicatie
Het advies m.b.t. de communicatie door en rondom de onderzoekscommissie wordt akkoord bevonden. Op de website zal informatie verschijnen rond het proces van het onderzoek. Ook zal er een aantal informatieve documenten op worden geplaatst, zoals de verordening en het plan van aanpak.
De openbare hoorzitting zal via de webcasting op internet te volgen zijn.

8. Volgende vergadering
De volgende vergadering is op dinsdag 28 april van 17.00 – 19.00 uur. Daarna zal KPMG aanschuiven voor een briefing tot 20.00 uur (indien dat lukt).
De ChristenUnie zal dan verstek moeten laten gaan (zowel lid als plv.lid)

Openstaande afspraken

datum	afspraak	realisatie
1/4	De commissie gaat een keer ter plekke de situatie in ogenschouw nemen.	
1/4	Geïnformeerd worden over het ICT-beveiligingsbeleid in het provinciehuis	
22/4	Brief aan RTV-Drenthe met verzoek transcript column Denkers.	gereed 24/4
22/4	Vragenlijst per geïnterviewde becommentariëren c.q. aanvullen en aan secretaris doorgeven.	28/4
22/4	KPMG uitnodigen voor briefing.	28/4

→ doet BING advies ogv stukken.

Planning besloten interviews en (openbare) hoorzitting **VERTROUWELIJK**

Datum / Naam	Interviews maandag 11 mei 2009 (GS-kamer)	Interviews woensdag 13 mei 2009 (1.43 en 2.21)	Interviews vrijdag 15 mei 2009 (0.36)	Interviews aanvullend 18 mei 2009	Hoorzitting Donderdag 28 mei 2009	Hoorzitting Uitloop-datum 29 mei 2009
				PM		PM
Mw. A. Haarsma gedeputeerde			10.30 uur		ochtend	
H. Klaver Statenlid	11.00 uur					
Mw. T. Klip gedeputeerde			9.00 uur			
Mw. A. Imhof Dir.-secr.		14.00 uur				
Mw. S. Weistra Dir-plv.secr.		15.15 uur				
A. Visser Hoofd Concernstaf		17.00 uur				
[redacted] Secr. Haarsma	13.00 uur					
[redacted] Secr. CdK	13.45 uur					
[redacted] Plv. secr. DS	14.30 uur					
[redacted] Secr. DS	15.30 uur					
P. van de Bosch Comm.adv. Haarsma		9.00 uur				
[redacted] Beleidsmdw. sport		10.30 uur				
[redacted] Mdw concernstaf		11.30 uur				
[redacted] Mdw. BC		13.00 uur				
M. de Bruin Journalist	19.00 uur					
Hr. Van Luyn Advocaat	20.00 uur					
Deloitte mdws.		PM				
Informant				PM		

ONDERZOEKSCOMMISSIE EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG van de vergadering van 22 april 2009

Aanwezig: Leo Bomhof (voorzitter), Margriet Stijkel, Jan Langenkamp, Herman Beerda, Sietze de Jong Renee Westerhof en [redacted] (Comm.).
Inge Rozema (secretaris).

3. Verslag van 8 april 2009
Het verslag wordt vastgesteld. In de komende verslagen zullen de openstaande afspraken steeds worden bijgehouden. Er moet een brief aan RTV-Drenthe worden gestuurd met het verzoek om een transcript van de column van de heer Denkers uit Cassata.

4. Kennismaking externe ondersteuning
De heren [redacted] van BING schuiven halverwege de vergadering aan. Hen wordt gevraagd een planning te maken van hoe zij het proces zien. Wat is wanneer gereed. Er zijn reeds per mail en worden ook ter plekke stukken aangereikt ter bestudering. Deze zullen nog worden aangevuld met de opgevraagde stukken bij de ambtelijke organisatie. De secretaris zal z.s.m. nagaan wanneer deze beschikbaar komen *(NB: dat is op zijn vroegst a.s. maandag, IR.)*
Het bureau wordt gevraagd de commissie te helpen te blijven focussen op de onderzoeksvragen en geen zijpaden te bewandelen. Van hen wordt verwacht dat zij bij de interviews en hoorzittingen aanwezig zijn en de commissie helpen bij de voorbereiding ervan. Tijdens de interviews mogen ook zij (aanvullende) vragen stellen. Ze kunnen tussendoor feedback geven op het verloop van de interviews. Een interviewtraining wordt niet nodig geacht.
De voorzitter zou graag al tijdig een voorlopige inhoudsopgave van het rapport van de commissie willen hebben, om een idee te krijgen hoe e.e.a. eruit ziet. Ook zal al aan de rapportage gewerkt worden gedurende de fasen 1 en 2, voorzover mogelijk.
De heren geven aan, dat zij het van belang vinden te weten wat KPMG wel en niet in zijn onderzoek heeft betrokken. Besloten wordt om KPMG uit te nodigen voor een briefing aan de commissie.

5. Plan van Aanpak
Het PvA wordt definitief vastgesteld.

6. Voorbereiding interviews
Over de definitieve **lijst van te interviewen personen** kan nu nog niets worden gezegd. Dat moet volgen uit de desk-research. De lijst die er nu ligt is een voorlopige. Maar de mensen die erop staan dienen in ieder geval te worden bevraagd, vinden de aanwezigen. Aanvullingen kunnen later eventueel nog komen. Daartoe zal de informant ook moeten behoren. I.v.m. voldoende voorbereidingstijd voor de geïnterviewden kunnen aanvullende mensen pas in de week van 18 mei worden geïnterviewd. De mensen op de voorliggende lijst kunnen nu worden uitgenodigd.

De opgestelde concept-uitnodigingsbrief wordt akkoord bevonden.

De leden van de commissie zullen de **concept-vragenlijst** bestuderen en hun commentaar en/of aanvullingen vóór de volgende vergadering aan de secretaris doorgeven. De heren van BING zullen op grond van hun deskresearch uiterlijk in de week van 6 mei nadere adviezen geven m.b.t. de vraagstelling.

M.b.t. **de planning** van de interviews is er discussie over de volgorde van bevraging: eerst de bestuurders en dan de ambtenaren of andersom. De heren van BING adviseren de bestuurders als laatste te plannen en ook voldoende tijd tussen de gesprekken te plannen voor korte evaluaties. De heer De Jong pleit voor meer gesprekken op de woensdag.
Drie leden van de commissie zullen steeds (in wisselende bezetting) de interviews afnemen. De anderen kunnen daar ook bij zijn (hoeft niet), maar dan "op de achterbank". De geïnterviewden moeten niet negen mensen tegenover zich hebben zitten.

Het **protocol** voor de interviews (= informatieve gesprekken) zal met de uitnodiging aan de geïnterviewden worden meegezonden. Er moet nog in worden verwerkt, dat de geluidsbestanden worden vernietigd, zodra het schriftelijke verslag is goedgekeurd (door beide partijen). Wat betreft de eventuele bijstand voor de geïnterviewden: die is toegestaan, maar dient niet in de plaats te treden van de geïnterviewde. M.a.w. hij mag niet namens de geïnterviewde antwoorden.

7. Communicatie
Het advies m.b.t. de communicatie door en rondom de onderzoekscommissie wordt akkoord bevonden. Op de website zal informatie verschijnen rond het proces van het onderzoek. Ook zal er een aantal informatieve documenten op worden geplaatst, zoals de verordening en het plan van aanpak.
De openbare hoorzitting zal via de webcasting op internet te volgen zijn.

8. Volgende vergadering
De volgende vergadering is op dinsdag 28 april van 17.00 – 19.00 uur. Daarna zal KPMG aanschuiven voor een briefing tot 20.00 uur (indien dat lukt).
De ChristenUnie zal dan verstek moeten laten gaan (zowel lid als plv.lid)

Openstaande afspraken

datum	afspraak	realisatie
1/4	De commissie gaat een keer ter plekke de situatie in ogenschouw nemen.	
1/4	Geïnformeerd worden over het ICT-beveiligingsbeleid in het provinciehuis	
22/4	Brief aan RTV-Drenthe met verzoek transcript column Denkers.	
22/4	Vragenlijst per geïnterviewde becommentariëren c.q. aanvullen en aan secretaris doorgeven.	28/4
22/4	KPMG uitnodigen voor briefing.	28/4

ONDERZOEKSCOMMISSIE
EUROCHAMP- RAPPORT

VERTROUWELIJK

KORT VERSLAG
van de vergadering van
8 april 2009

Aanwezig: Leo Bomhof (voorzitter), Margriet Stijkel, Gea Smith, Herman Beerda, Sietze de Jong en Renee Westerhof.
Inge Rozema (secretaris).

3. Afsprakenlijstje van 1 april 2009
De afspraken zijn uitgevoerd. De secretaris heeft niet het goede contact bij Ernst & Young kunnen vinden t.b.v. de offerte-aanvraag. De expertise van E&Y ligt met name in accountancy en fiscaliteit. Dat is voor ons onderzoek minder relevant. De commissie gaat akkoord met drie offerte-aanvragen: aan BMC, BING en Berenschot.

4. Advies professor Elzinga
Het advies heeft geleid tot aanpassing van de onderzoeksopdracht. Een eventuele dader zal alleen als 'bijvangst' van het onderzoek naar voren kunnen komen. Het onderzoek zal op een meer indirecte wijze vorm moeten krijgen en breder worden getrokken. Men is het erover eens, dat die breedte wel binnen de perken moet blijven.
Er is discussie over de vraag of BZK nog moet worden ingeschakeld. Herman Beerda pleit daar sterk vóór. Leo Bomhof, Sietze de Jong en Renee Westerhof zijn van mening, dat de aangepaste onderzoeksopzet voldoende tegemoet komt aan eventuele bezwaren. De commissie heeft advies ingewonnen en daar naar geluisterd.
Geconcludeerd wordt, dat BZK niet om een toets wordt gevraagd, maar dat goed juridisch advies door het externe bureau zeer belangrijk zal worden.

5. Operationalisering onderzoeksvragen
Het huiswerk heeft een lange lijst (soms gedetailleerde) vragen opgeleverd. Deze zijn toegespitst op de eerste onderzoeksvraag. Vanwege de wijziging in de onderzoeksopdracht zullen ook de andere twee vragen nog moeten worden geoperationaliseerd. Herman Beerda meent, dat het externe bureau de commissie moet helpen om daar slim mee om te gaan. Dat geldt ook voor het gebruik van de al geïnventariseerde lijst met vragen. De aanwezigen zijn het daarmee eens.
De secretaris heeft een voorzet gemaakt met een aantal vragen op hoofdlijnen per onderzoeksvraag, om mee te zenden met de offerte-aanvraag. De commissie beschouwt dit als een voorlopige aanzet voor de operationalisering.

6. Offerte-aanvraag
Het voorliggende voorstel is akkoord. De onderzoeksvragen moeten nog worden aangepast aan de herziene opdracht van PS. De offertes moeten op maandag 20 april 10.00 uur binnen zijn. De secretaris maakt op basis daarvan een vergelijkende beoordelingstabel en mailt die rond aan de

leden. Zij reageren per omgaande, zodat op dinsdag 21 april kan worden gegund. Op 22 april zal het gekozen bureau in de vergadering van de commissie aanwezig moeten zijn.
Het rapport van KPMG wordt niet meegezonden, vanwege de beperking die er door KPMG is opgelegd voor gebruik door derden. De secretaris zal KPMG een brief schrijven namens de commissie om hen te informeren over het op handen zijnde onderzoek, waarbij hun rapport als uitgangspunt dient. Ook een brief met verzoek om image in stukken

7. Plan van Aanpak
Het PvA moet nog worden aangepast aan de nieuwe formulering van de onderzoeksopdracht. In de volgende vergadering de definitieve versie voorleggen en vaststellen.
Afgesproken wordt dat de secretaris de eerst aangewezene is om het budget in de gaten te houden en bij dreigende overschrijdingen tijdig aan de bel te trekken bij de commissie.

8. Volgende vergadering
De wekelijkse vergaderingen zullen voortaan van 11.30 uur tot uiterlijk 13.30 uur worden gepland. Dit is steeds in 0.07 met lunch. De eerstvolgende vergadering is niet op 15 april, maar op 22 april a.s.

Bijeenkomst met plaatsvervangend leden (na afloop PS)
Voorts aanwezig: Michel Berends, Joma Kaal, Ger Udding, Ko Vester, Tjerk Medemblik en Jan Langenkamp.

De commissie is nu formeel benoemd. De commissie wijst Renee Westerhof aan als plv. voorzitter.

De voorzitter stelt het Huishoudelijk Reglement aan de orde en wijst de leden en plv. leden op de afspraken daarin omtrent communicatie en vertrouwelijkheid. Inhoudelijke zaken uit de commissie kunnen niet in de fracties worden besproken, behalve tussen het lid en het plaatsvervangend lid van de commissie. De communicatie naar buiten loopt via de voorzitter.
Het Huishoudelijk reglement wordt vastgesteld.

Afgesproken wordt dat op gezette tijden een vergadering wordt belegd met de plv. leden erbij om hen even bij te praten. Voorts krijgen zij alle stukken in cc.
Vanwege de vertrouwelijkheid van de stukken wordt de plv. leden gevraagd hun privé-mail-adressen door te geven, zodat die voor verspreiding van stukken en ander mailverkeer van de commissie kan worden gebruikt.

IR/ 09-04-09

23

Voorlopige planning besloten interviews en (openbare) hoorzitting **VERTROUWELIJK**

Datum / Naam	Interviews maandag 11 mei 2009	Interviews dinsdag 12 mei 2009	Interviews woensdag 13 mei 2009	Interviews vrijdag 15 mei 2009	Hoorzitting donderdag 28 mei 2009	Hoorzitting uitloopdatum 29 mei 2009
						PM
Mw. A. Haarsma gedeputeerde	18.30 uur				ochtend	
Mw. T. Klip gedeputeerde	19.30 uur					
H. Klaver Statenlid	20.30 uur					
Mw. A. Imhof Dir.-secr.			15.00 uur			
Mw. S. Weistra Dir-plv.secr.			16.00 uur			
A. Visser Hoofd Concernstaf			17.00 uur			
[redacted] Secr. Haarsma		9.00 uur				
[redacted] Secr. DS		10.00 uur				
[redacted] Secr. CdK		11.00 uur				
[redacted] Plv.secr.DS		12.00 uur				
P. van de Bosch Comm.adv.Haarsma		13.00 uur				
[redacted] Beleidsmdw. sport				14.00 uur		
[redacted] Mdw concernstaf				15.00 uur		
[redacted] Mdw. BC				16.00 uur		
M. de Bruin Journalist		19.00 uur				
Hr. Van Luyn Advocaat Eurochampdirectie		20.00 uur				
Deloitte mdws.	17.00 uur					
de informant						

Kopie V.

ZWARTE TAS
VERTROUWELIJK

Agendapunt voor de vergadering van gedeputeerde staten van Drenthe

GS-stuk

24

Algemene gegevens	
Opsteller	Andries Visser, [redacted]
Afdeling	Concernstaf
Datum	donderdag 5 maart 2009
Uiterste behandeldatum in GS:	
Toelichting:	

Verantwoordelijk manager	
Andries Visser	
Akkoord:	*Bespreken:*
	Vi 4/3

Nr.	*Programma, prioriteit, resultaat in begroting*
nvt	nvt

Portefeuillehouder
Tanja Klip-Martin

Afgestemd met	*Afwijkende mening*
1.	
2.	
3.	

Paraaf Directeur-secretaris:
Annette Imhof

Archivering	
Datum:	*Registratienummer:*
10-3-09	nr. 4.4 / 2009002853
	nr.
	nr.

Communicatie	
Openbaar:	nee
Persbericht:	later?
OR-aangelegenheid:	nee
Bekendmaking:	
Niet van toepassing	

Onderwerp

Onderzoek naar mogelijke voortijdige verspreiding van het Deloitte rapport over Eurochamp

Advies

1. Kennisnemen van het eindrapport van KPMG
2. Het rapport met geleidebrief verzenden naar provinciale staten

Beslissing GS

(1) Conform, Brief I.h.p (2)

" ~~Brief naar PS toevoegt~~

Inleiding

Naar aanleiding van berichten over mogelijke onregelmatigheden in de bedrijfsvoering van de stichting EuroChamp Foundation heeft de provincie Drenthe een onderzoek laten uitvoeren door Deloitte Forensic & Dispute Services. Herhaalde berichten in de regionale media en vragen vanuit leden van provinciale staten leidden tot speculaties dat de inhoud van het definitieve onderzoeksrapport gedateerd op 10 november 2008 voortijdig is verspreid. Dat wil zeggen voordat u het rapport op 27 november 2008 openbaar maakte. U heeft besloten deze speculaties te onderzoeken. KPMG Forensic heeft dit onderzoek uitgevoerd.

De onderzoeksvraag luidde: is het definitieve rapport van Deloitte Forensic & Dispute Services inzake de stichting EuroChamp Foundation voortijdig verspreid vanuit het Provinciehuis? Zo ja, op welke wijze, wanneer en door wie?

Uit het rapport van KPMG blijkt dat er op 21 november 2008 een exemplaar voortijdig in handen is gekomen van een lid van provinciale staten (de heer Klaver). Dit is (aantoonbaar) de digitale (PDF) versie die op verzoek van een medewerker op 10 november van Deloitte is binnengekomen op het Provinciehuis. Volgens een anonieme informant is deze versie al op 13 november 2008 in diens (= de informant) bezit gekomen. De onderzoekers hebben dit geverifieerd. De onderzoekers achten de informant betrouwbaar gelet op de aan hen overlegde informatie en in relatie met de overige feiten, gevonden in het onderzoek. De ambtelijke opdrachtgevers zijn niet op de hoogte van de identiteit van de informant.
Uit de interviews en uit het onderzoek in de directe IT omgeving (wat betreft de toegang tot en de opslag van de PDF versie) is gebleken dat de PDF versie op één actie na, niet voor of op 21 november 2008 is doorgestuurd via enig mailverkeer. De ene getraceerde en bevestigde gebeurtenis vond plaats op 17 november 2008. De PDF versie is toen verstuurd naar de landsadvocaat. De onderzoekers hebben geen aanwijzingen dat deze actie in het kader van de voortijdige verspreiding relevant is.
De wijze waarop de PDF versie is verspreid is niet getraceerd. Er is niet gemaild. Uitprinten van de PDF versie of overzetten daarvan naar bijvoorbeeld een USB stick is niet te herleiden omdat daar geen loggegevens (gegevens die het digitale verkeer vastleggen) van zijn, anders dan toevallige resten van gegevens. En die zijn hier niet gevonden. Ook de interviews geven hier geen aanknopingspunt. Ook de vraag wie verantwoordelijk is voor de voortijdige verspreiding kan (daarom) niet door de onderzoekers worden beantwoord
De onderzoekers hebben aangegeven dat een nader grootschalig onderzoek naar de gehele IT omgeving of nadere interviews zeer waarschijnlijk niet zal leiden tot een antwoord op de vraag: op welke wijze en door wie het rapport voortijdig is verspreid.

Advies

1. Kennisnemen van het eindrapport van KPMG
2. Het rapport met geleidebrief verzenden naar provinciale staten

Beoogd effect

Provinciale staten zijn in staat zich een oordeel te vormen over de onderzoeksresultaten

Argumenten

1.1. Kennis van het rapport is nodig om een strategie uit te stippelen voor de behandeling in PS en qua publiciteit

In het rapport wordt gesteld dat het voortijdig in het bezit zijn van het rapport bij derden door een handeling vanuit het provinciehuis mogelijk is gemaakt. Op welke wijze is niet traceerbaar en door wie dit is gedaan is binnen de grenzen van dit onderzoek niet aantoonbaar. U kunt op basis van het rapport een aantal verdere scenario's bespreken als inzet naar PS.

- Het ene scenario is het hier bij te laten en het verlies (het geconstateerde lekken) te nemen, waarbij aangegeven kan worden dat er op het terrein van integriteit en informatiebeveiliging verdere maatregelen worden genomen (zonder een dichtgetimmerd provinciehuis na te streven)
- De andere lijn is om door te gaan met waarheidsvinding. Door het instellen van een vervolgonderzoek. Te denken valt aan een persoonsgericht onderzoek en/of een nader onderzoek naar de gehele IT omgeving. Ongeacht de kans op succes. Er wordt dan een sterk signaal afgegeven over de opvatting van GS over de integriteit van de organisatie.

2.1. PS informeren

Gelet op de toezegging van GS en de behandeling van het onderwerp in de PS vergadering van 17 december 2008 en de gewenste transparantie is integrale en openbare toezending gewenst. De wijze van behandeling wordt door PS overigens zelf bepaald.

Uitvoering

Tijdsplanning

Niet van toepassing.

Financiën

Kostenraming	2009	2010	2011	2012	2013
Totale kosten	€ 70.000	€ 0	€ 0	€ 0	0
Bijdragen van derden	€ 0	€ 0	€ 0	€ 0	0
Bruto kosten provincie	€ 70.000	€ 0	€ 0	€ 0	0
Baten Provincie	€ 0	€ 0	€ 0	€ 0	0
Netto kosten Provincie	€ 70.000	€ 0	€ 0	€ 0	0

Dekkingsplan

Middelen bestaand programma / prioriteit, te weten:accountantskosten

Personeel

Niet van toepassing.

Europese aspecten

Niet van toepassing.

Monitoring en evaluatie

Niet van toepassing.

Extern betrokkenen
KPMG Forensic (onderzoekers); kunnen eventueel in PS toelichting geven (advies: alleen op verzoek PS)

Communicatie
Voorgesteld wordt om op het tijdstip van zending naar PS ook een persbericht op te stellen met beknopte feitelijke informatie. En een persconferentie te overwegen.
Inmiddels is ook besloten de ongeschoonde versie van het Deloitte rapport op basis van de WOB (??) beschikbaar te stellen. De eventuele communicatie daarover moet (ook qua timing) afgestemd.

Bijlagen	**Meekopiëren**
1. Eindrapport	Ja
2. Geleidebrief	Ja
3.	Ja/Nee
4.	Ja/Nee
5.	Ja/Nee

Provinciehuis Westerbrink 1, Assen
Postadres Postbus 122, 9400 AC Assen
www.drenthe.nl
T (0592) 36 55 55
F (0592) 36 57 77

provincie Drenthe

25

Aan:
KPMG Forensic
T.a.v. [redacted]
Burgemeester Rijnderslaan 20
1185 MC AMSTELVEEN

Assen, 16 december 2008
Behandeld door A. Visser (0592) [redacted]
Ons kenmerk 51/Dir/2008015390
Onderwerp: Onderzoek verspreiding Deloitte-rapport EuroChamp

Vertrouwelijk

Geachte heer [redacted],

In een eerder gesprek met u of met medewerkers van uw organisatie hebben wij verkennend gesproken over de mogelijkheden die uw organisatie biedt voor het verrichten van onderzoek naar de mogelijk vroegtijdige verspreiding vanuit het Drentse Provinciehuis van het definitieve rapport van Deloitte Forensic Services over de stichting EuropChamp Foundation gedateerd op 10 november 2008. In deze brief laat ik u weten hoe wij verder gaan met het traject om te komen tot dit onderzoek.

Aanvraag offerte en plan van aanpak
Met deze brief vraag ik u een offerte te doen voor het uitvoeren van een onafhankelijk onderzoek naar de mogelijk voortijdige verspreiding van het definitieve Deloitte-rapport over EuropChamp. Gezien de aard van het onderzoek is hierbij snelheid geboden. Graag ontvang ik van u vrijblijvend een offerte met plan van aanpak voor een onderzoek dat voldoet aan onze onderzoeksopdracht. De onderzoeksopdracht treft u bijgevoegd aan.

Vertrouwelijk
Ik verzoek u vertrouwelijk met deze aanvraag om te gaan. Het al dan niet in de openbaarheid brengen van het onderzoek en de uitkomsten daarvan, ligt bij de provincie Drenthe. U onderhoudt uw contacten hierover alleen rechtstreeks met de opdrachtgever(s).

Onderzoek
Voor de inhoud van het onderzoek verwijs ik naar de onderzoeksopdracht. In dit document staat onder andere aangegeven wat de aanleiding van het onderzoek is, wat de centrale onderzoeksvraag is en welke aandachtspunten voor de provincie van belang zijn. Ook staat in de onderzoeksopdracht een passage over de aard en vorm van het onderzoek, de volgorde van onderzoek en de tijdsplanning.

Offerte op basis van uurtarief
Wij verzoeken u nadrukkelijk uw offerte in te dienen op basis van uurtarief. Dit gezien de aard van het onderzoek en de onzekerheden in de verschillende fases van het onderzoek over het verdere verloop daarvan.

Algemene inkoopvoorwaarden
Op de onderzoeksopdracht zijn de Algemene inkoopvoorwaarden van de provincie Drenthe van toepassing. Deze voorwaarden treft u als bijlage aan. Ik vraag u bij het opstellen van uw offerte met plan van aanpak alvast rekening te houden met onze Algemene inkoopvoorwaarden.

Meerdere aanvragen
Naast uw organisatie vragen wij ook twee andere externe organisaties om een offerte met plan van aanpak. In het kader van transparantie vinden wij het van belang u dit te laten weten.

Keuzecriteria
Gezien de aard van het onderzoek is het een voorwaarde dat uw organisatie bij het Ministerie van Justitie op de lijst van vergunninghouders voor het uitvoeren van dergelijke onderzoeken staat ingeschreven. Daarnaast zijn de belangrijkste criteria bij het maken van onze keuze voor een organisatie die het onderzoek gaat uitvoeren, met name de kwaliteit van het plan van aanpak, het uurtarief en de snelheid van onderzoek. Ook telt mee of wordt voldaan aan de algemene inkoopvoorwaarden van de provincie. Wij beoordelen en wegen de offertes en plannen van aanpak aan de hand van genoemde criteria.

Inzending
Als u ingaat op onze vraag, verzoek ik u uiterlijk 19 december 2008 17.00 uur uw offerte met plan van aanpak onder de vermelding van "vertrouwelijk" te doen toekomen aan de provincie Drenthe, ter attentie van de heer A. Visser, hoofd Concernstaf. Graag uw offerte met plan van aanpak per fax versturen naar faxnummer 0592-355299. Wij verzoeken u vlak vóór het verzenden van deze documenten contact op te nemen met de heer A. Visser. Inzendingen die nog na de inzendtermijn binnen komen, kunnen wij helaas niet meer meenemen bij het maken van de keuze voor de organisatie die onze opdracht uitvoert.

Vervolg
Naar aanleiding van de offertes met plannen van aanpak maken wij een keuze voor één externe organisatie. Die organisatie krijgt de opdracht van ons het onderzoek daadwerkelijk uit te voeren. Wij berichten u zo spoedig mogelijk over onze beslissing nadat wij onze keuze hebben gemaakt.

Opdrachtgevers/contactpersonen
De opdrachtgever namens het college van gedeputeerde staten is de Directeur-Secretaris, mevrouw J.M. Imhof. Gedelegeerd opdrachtgever is het hoofd van de Concernstaf, de heer A. Visser. De opdrachtgevers zijn de enige contactpersonen tussen u en de provincie Drenthe voor wat betreft deze aanvraag.

- Mevrouw J.M. Imhof, Directeur-Secretaris.
- De heer A. Visser, hoofd Concernstaf, telefoonnummer 0592-[redacted].

Als u nog vragen heeft naar aanleiding van deze brief kunt u met de heer Visser contact opnemen.

Tot slot
In deze brief hebben wij u gevraagd vrijblijvend een offerte met plan van aanpak bij ons in te dienen voor het uitvoeren van een onderzoek naar de verspreiding van het Deloitte-rapport over EuroChamp. Gezien ons eerdere gesprek ga ik ervan uit dat u positief tegenover deze vraag staat. Wij zien met belangstelling uw reactie tegemoet.

Hoogachtend,

A. Visser
Hoofd Concernstaf

Bijlagen:
- *Onderzoeksopdracht met bijlage*
- *Algemene inkoopvoorwaarden provincie Drenthe*

kopie

26

Vertrouwelijk

Onderzoek: Verspreiding Deloitte-rapport EuroChamp

Onderzoeksopdracht

Aanleiding

Naar aanleiding van berichten over mogelijke onregelmatigheden in de bedrijfsvoering van de stichting EuroChamp Foundation (directeur: de heer Leijssenaar) heeft de provincie Drenthe een onderzoek laten uitvoeren door Deloitte Forensic Services (FS). Herhaalde berichten in de regionale media en vragen vanuit leden van Provinciale Staten leiden tot speculaties dat de inhoud van het definitieve onderzoeksrapport gedateerd op 10 november 2008[1] (verder genoemd: het rapport) voortijdig is verspreid. Dat wil zeggen voordat het college het op 28 november j.l. openbaar maakte. Deze speculaties over het voortijdig verspreiden van het rapport vindt het college van Gedeputeerde Staten schadelijk voor de reputatie van de provincie. Het college heeft hierop het Openbaar Ministerie gevraagd of er aanleiding is strafrechtelijk onderzoek te doen naar het moment en de manier en door wie het definitieve rapport van Deloitte Forensic Services over de Stichting Eurochamp Foundation mogelijk eerder is verspreid. Het Openbaar Ministerie heeft laten weten hiervoor geen aanleiding te zien. Om een eind te maken aan de speculaties in de media hebben GS besloten een nader onderzoek te laten uitvoeren door een onafhankelijk bureau naar de manier, wanneer en door wie het rapport van Deloitte Forensic Services inzake de Stichting EuroChamp Foundation mogelijk eerder is verspreid.

Onderzoeksvraag

Voor het onderzoek is de volgende centrale onderzoeksvraag geformuleerd.

Centrale onderzoeksvraag

Is het definitieve rapport van Deloitte Forensic Services inzake de stichting EuroChamp Foundation voortijdig verspreid vanuit het Provinciehuis?
Zo ja op welke wijze, wanneer en door wie?

Aanvullende opmerking in relatie tot de onderzoeksvraag:

1. de provincie vindt het belangrijk dat 'kennis van' en 'betrokkenheid bij' het eventueel voortijdig verspreiden van het definitieve rapport een belangrijk aspect is bij de uitwerking van het onderzoek;
2. de provincie vindt het belangrijk dat de opmerkingen van de heer Klaver (fractievoorzitter van het CDA) dat hij aanwijzingen heeft dat vanuit de provincie het rapport eerder dan 28 november j.l (anders dan politie, SNN, Statengriffie en de landsadvocaat) is verstrekt, gestaafd worden;
3. de digitale en de papieren versie zijn door Deloitte aan de provincie verstrekt op 10 november j.l.
4. de provincie hecht eraan dat de twee betrokken journalisten van het Dagblad van het Noorden en de advocaat van de heer Leijssenaar bevraagd worden, in relatie tot beweringen en artikelen in de media

[1] Hier wordt bedoeld de digitale versie en de papieren versies van het definitieve rapport, beide ontvangen door de provincie op 10 november j.l.(dus geen concepten).

Vorm van onderzoek en rapportage
U bent in uw plan van aanpak in principe vrij om de onderzoeksopzet in uw offerte vorm te geven. De kwaliteit van uw aanpak is een gunningcriterium. Het onderzoeksrapport is een rapport met feiten en bevindingen die niet naar personen zijn te herleiden, tenzij dit noodzakelijk is voor de bewijsvoering van de mogelijke vroegtijdige verspreiding vanuit het Provinciehuis.
Na het staven van de beweringen gedaan door media en de heer Klaver kan het onderzoek afhankelijk van de uitkomsten van dat deelonderzoek worden bijgesteld en/of uitgebreid.
Er is regelmatig een voortgangsgesprek met de directeur –secretaris en het hoofd van de concernstaf van de provincie over de voortgang en de tussentijdse resultaten.

Opdrachtgever(s)
De opdrachtgever namens Gedeputeerde Staten is de Directeur-Secretaris, mevrouw J.M. Imhof; gedelegeerd opdrachtgever is het hoofd van de Concernstaf, de heer A. Visser. De opdrachtgevers zijn de enige contactpersonen tussen het onderzoeksbureau en de provincie voor wat betreft de uitvoering en de fasering van het onderzoek.

Tijdsplanning
Het onderzoek dient per direct te starten. Na een periode van maximaal zes weken verwachten wij een afgerond onderzoeksrapport. Tussenrapportages aan de opdrachtgevers zijn mogelijk.

kopie ✓

Vertrouwelijk
Zwarte Tas

Agendapunt voor de vergadering van gedeputeerde staten v 27

GS-stuk

Algemene gegevens	
Opsteller	[redacted]
Afdeling	Sociaal-Economische ontwikkeling
Datum	vrijdag 7 november 20088
Uiterste behandeldatum in GS:	
Toelichting:	

Verantwoordelijk manager	
Marcel-Armand van Nieuwpoort	
Akkoord:	*Bespreken:*
6/2	7/11/2008

Nr.	**Programma, prioriteit, resultaat in begroting**

Portefeuillehouder
Anneke Haarsma

Afgestemd met	**Afwijkende mening**
1. [redacted] BC	nee
2. [redacted] SEO	nee
3. Paul van den Bosch, BC	nee

Paraaf Directeur-secretaris:

Archivering	
Datum:	*Registratienummer:*
11-11-08	nr. 4.3/2008013336
	nr.
	nr.

Communicatie	
Openbaar:	nee
Persbericht:	nee
OR-aangelegenheid:	nee
Bekendmaking:	
Niet van toepassing	

Onderwerp

Onderzoekrapport Deloitte naar bedrijfsvoering Stichting EuroChamp

Advies

Bijopbergnota niet aangeboden PD

1. Kennisnemen van het onderzoeksrapport van Deloitte naar de Stichting Eurochamp.
2. Het voornemen aan Stichting Eurochamp kenbaar maken de subsidiebeschikkingen van in totaal € 360.000 toegekend uit::
   a. de reserve 'Versterking Economische Structuur' € 170.000,--;
   b. de reserve 'Mensen in het middelpunt, Parels van Drenthe' van totaal € 190.000,--,
   in te trekken.
3. Kenbaar maken aan Stichting EuroChamp dat, gelet op de voorgenomen intrekkingen, er rekening mee moet worden gehouden dat al uitbetaalde voorschotten van in totaal € 250.000,-- terug worden gevorderd.
4. Hiertoe bijgevoegd ontwerpbesluit aan Stichting Eurochamp vaststellen.
5. Aangifte doen bij het Openbaar Ministerie in verband met mogelijke strafbare feiten. Hiervoor de directeur plaatsvervangend secretaris mevrouw S. Weistra mandateren.

6. Verzoeken van derden om een exemplaar van het rapport van Deloitte te mogen ontvangen, af te wijzen op grond van de Wet openbaarheid van bestuur. en binnen deze kaders
7. Provinciale staten informeren met bijgevoegde brief. en over het verdere verloop rond informatieverstrekking afspraken te maken met het OM.

Beslissing GS

I.h.p.

Zie de hierbij gevoegde aanpassingen voor de brief.

Inleiding

Op 20 juni jl. is uw college op de hoogte gebracht van mogelijke financiële onregelmatigheden bij Stichting EuroChamp (hierna: EuroChamp). De onregelmatigheden zouden zijn begaan door de directie van EuroChamp. In maart 2006 heeft uw college een subsidiebedrag van € 360.000,-- verleend aan EuroChamp voor de periode 2006-2008. Doel van deze subsidie was:

- de stichting te professionaliseren en verder in de markt te zetten;
- het leggen van een structurele basis voor het organiseren van toekomstige topsportevenementen voor gehandicapten in Noord-Nederland;
- Noord-Nederland en Drenthe in het bijzonder promoten als topsportregio voor gehandicapten.

EuroChamp zou dit doen door middel van een drietal activiteiten:

- het ontwikkelen en organiseren van een World Serie of World games in Drenthe;
- het organiseren van training- en sportkampen en daaraan gekoppeld een regionaal facilitair netwerk in Drenthe;
- de organisatie van een internationaal congres op het raakvlak van de valide sport en de gehandicaptensport in Drenthe.

De verleende subsidie is opgebouwd uit twee delen. Er is voor € 190.000,-- subsidie verleend uit de Reserve mensen in het middelpunt, Programmalijn Parels van Drenthe en voor € 170.000,-- uit de Reserve versterking economische structuur. Het eerste deel is reeds voor 60% bevoorschot, het tweede deel voor 80% (bevoorschotting vindt plaats tot maximaal 80% van de verleende subsidie).

Naar aanleiding van informatie over mogelijke financiële onregelmatigheden bij EuroChamp hebben er op twee momenten overleggen met het bestuur van Eurochamp plaatsgevonden. Hierover is uw college nader geïnformeerd in eerdere GS-vergaderingen.

Op 21 juli jl. heeft uw college de resultaten van het boekenonderzoek, in opdracht van EuroChamp uitgevoerd door UNO bedrijfsadviseurs, ontvangen. Het rapport bevestigt dat financiële onregelmatigheden hebben plaatsgevonden bij EuroChamp. Het rapport stelt echter dat 'volledige kwantificering van de onregelmatigheden nader uitgebreid en diepgaand onderzoek vereist'.

Op basis hiervan heeft uw college opdracht gegeven aan Deloitte Forensic & Dispute Services om nader onderzoek te doen naar de bedrijfsvoering binnen de stichting EuroChamp. Inzet was dit onderzoek binnen een termijn van enkele weken af te ronden. Echter, door de geconstateerde complexe problematiek was er een langere onderzoeksperiode noodzakelijk. Het eerste conceptrapport over de bedrijfsvoering binnen EuroChamp is op 3 november jl. ontvangen.

Het onderzoeksrapport van Deloitte bevestigt de door UNO geconstateerde onregelmatigheden. Daarnaast is Deloitte op meer onregelmatigheden gestuit. Het onderzoeksrapport van Deloitte geeft een gedetailleerd beeld over de wijze waarop de bedrijfsvoering binnen de stichting Eurochamp heeft plaatsgevonden.

Advies

1. Kennisnemen van het onderzoeksrapport van Deloitte naar de Stichting Eurochamp.
2. Het voornemen aan Stichting Eurochamp kenbaar maken de subsidiebeschikkingen van in totaal € 360.000 toegekend uit::
   a. de reserve 'Versterking Economische Structuur' € 170.000,--;
   b. de reserve 'Mensen in het middelpunt, Parels van Drenthe' van totaal € 190.000,--,
   in te trekken.
3. Kenbaar maken aan Stichting EuroChamp dat, gelet op de voorgenomen intrekkingen, er rekening mee moet worden gehouden dat al uitbetaalde voorschotten van in totaal € 250.000,-- terug worden gevorderd.
4. Hiertoe bijgevoegd ontwerpbesluit aan Stichting Eurochamp vaststellen.
5. Aangifte doen bij het Openbaar Ministerie in verband met mogelijke strafbare feiten. Hiervoor de directeur plaatsvervangend secretaris mevrouw S. Weistra mandateren
6. Verzoeken van derden om een exemplaar van het rapport van Deloitte te mogen ontvangen, af te wijzen op grond van de Wet openbaarheid van bestuur.
7. Provinciale staten informeren met bijgevoegde brief.

Beoogd effect

- Een rechtmatige afrekening van de aan EuroChamp verleende subsidies
- Terugvordering van de verleende voorschotten aan de EuroChamp.

Argumenten

1.1. Het rapport geeft een gedetailleerd overzicht van de wijze waarop de bedrijfsvoering is uitgevoerd.

2.1. Uit dit rapport moet worden geconcludeerd dat er onvoldoende waarborgen zijn in de betrouwbaarheid van de bedrijfsvoering van EuroChamp.

Wij hebben gerede twijfels over de rechtmatigheid van handelen door medewerkers van EuroChamp. Het rapport van Deloitte laat een patroon van fouten cq. malversaties zien in de bedrijfsvoering van EuroChamp. Kort samenvattend kunnen genoemd worden:

- Aanbestedingsprocedures die niet correct zijn verlopen.
  Conform onze ASV en SNN voorwaarden moeten voor alle opdrachten boven € 25.000,-- aanbestedingsprocedures worden gevolgd. Deloitte laat een overzicht zien waarbij gegronde aanwijzingen zijn over de onjuistheid van de gevolgde aanbestedingsprocedures. Hierbij is antedatering en/of manipulatie van documenten niet uit te sluiten.
  Op basis van het rapport kan ook geconcludeerd worden dat EuroChamp op dit onderdeel foute informatie aan ons heeft verschaft in de verplichte voortgangrapportages over het project.
- Het doorberekenen van uurtarieven van medewerkers van een derde partij waar geen schriftelijke documenten (contracten of overeenkomsten) aan ten grondslag lagen.
- Facturen die door medewerkers onterecht zijn gedeclareerd bij EuroChamp.

2.2. De rechtbank Assen heeft EuroChamp op 23 september jl. failliet verklaard.

Door de rechtbank is inmiddels een curator aangewezen om alle financiële zaken af te wikkelen. De hoofddoelstelling van het project was om van Eurochamp een stabiele organisatie te maken waarbij

continuïteit in activiteiten gegarandeerd zou zijn. Het achterliggende doel was dat de stichting hiermee een stabiele financiële basis zou hebben na beëindiging van de subsidieperiode.

Op grond van bovenstaande argumenten bestaat voldoende aanleiding om de subsidieverleningsbeschikkingen in te trekken en de verleende voorschotten terug te vorderen.

2.3. *Het Samenwerkingsverband Noord Nederland heeft inmiddels de verleende van 328.000,-- op nihil vastgesteld en is overgegaan tot terugvordering.*

2.4. *Op grond van de Algemene wet bestuursrecht is uw college verplicht EuroChamp in de gelegenheid te stellen haar zienswijze naar voren te brengen voordat een definitief besluit wordt genomen over intrekking van de subsidieverleningen.*

Om deze reden is op dit moment nog sprake van een ontwerpbesluit.

3.1. *Volgens artikel 162 van het Wetboek van Strafvordering is uw college verplicht tot het doen van aangifte.*

Omdat uw college thans kennis heeft van mogelijke strafbare feiten binnen de EuroChamp is uw college verplicht tot het doen van aangifte.
Opgemerkt moet worden dat bij het doen van de aangifte het rapport van Deloitte wordt overgedragen aan het Openbaar Ministerie. Dit heeft als consequentie dat het onderzoeksrapport onderdeel zal uitmaken van een justitieel onderzoek.

4.1 *De Wet openbaarheid van bestuur (Wob) biedt de mogelijkheid om een verzoek om informatie te weigeren indien hierdoor de opsporing en vervolging van strafbare feiten zou kunnen worden gefrustreerd.*

Op dit moment hebben een schuldeiser van EuroChamp, te weten de heer R. Huijskens, en Dorhout Advocaten namens Creative Wave B.V. verzocht om een exemplaar van het rapport van Deloitte. De komende tijd zullen naar alle waarschijnlijkheid onder andere de curator van EuroChamp en de media om een exemplaar van het rapport van Deloitte verzoeken. Deze verzoeken worden primair geweigerd op bovengenoemde grond. Andere weigeringsgronden zijn dat verstrekking van het rapport zich niet verdraagt met de eerbiediging van de persoonlijke levenssfeer én dat sprake is van een document, opgesteld ten behoeve van intern beraad waar persoonlijke beleidsopvattingen zijn opgenomen.

5.1 *Uw college heeft toegezegd provinciale staten nader te informeren over de voortgang van het onderzoek.*

Middels bijgevoegde brief en bijbehorende bijlage worden provinciale staten op hoofdlijnen op de hoogte gebracht.
Indien provinciale staten om een exemplaar van het rapport vragen geldt het volgende. Op grond van de Provinciewet geeft uw college provinciale staten mondeling of schriftelijk de door een of meer leden gevraagde inlichtingen. Dit kan alleen worden geweigerd als dit in strijd zou zijn met het openbaar belang. De Provinciewet biedt dan de mogelijkheid om op grond van een belang, genoemd in artikel 10 Wob (in dit geval het belang van de opsporing en vervolging van strafbare feiten), een geheimhoudingsplicht op te leggen aan provinciale staten.

Uitvoering

Tijdsplanning
10/11 november 2008: informeren bestuur EuroChamp
12 november 2008: doen van aangifte
12 november 2008: provinciale staten informeren
tot ± 18 november 2008: EuroChamp in de gelegenheid stellen zienswijze naar voren te brengen
25 november 2008: definitief besluit omtrent de intrekking van de subsidieverlening

Financiën
Niet van toepassing.

Personeel
Niet van toepassing.

Europese aspecten
Niet van toepassing.

Monitoring en evaluatie
Het faillissement van Eurochamp zal consequenties hebben in de realisatie van de ambities van uw college op het terrein van gehandicapten(top)sport. Inhoudelijk is dit thans een permanent punt van aandacht en wordt er momenteel gekeken op welke wijze concreet inhoud gegeven kan worden om ambities van het college te verder vorm te geven. Een onderdeel hiervan kan zijn dat de activiteiten van Eurochamp eventueel worden overgedragen aan bestaande (sport)organisaties in Drenthe. Hierover vindt momenteel een oriëntatie plaats. Voorstellen hiervoor worden aan uw college later voorgelegd.

Extern betrokkenen
(curator van) Eurochamp, Samenwerkingsverband Noord-Nederland, Openbaar Ministerie

Communicatie
Persbericht, bijgevoegd.

Bijlagen	**Meekopiëren**
1. Onderzoeksrapport inzake stichting Eurochamp	Nee, ter inzage voor GS
2. Samenvatting onderzoeksrapport	Ja
3. Statenbrief	Ja
4. Ontwerpbesluit Eurochamp	Ja
5. Persbericht.	Ja

28

CONCEPT **VERTROUWELIJK**

Vertrouwelijk
Onderzoekscommissie Eurochamp
T.a.v. de secretaris, mevrouw I.M. Rozema
Postbus 122
9400 AC ASSEN

Amersfoort, 11 juni 2006

Betreft: Advies gebruik telecomgegevens

Geachte mevrouw Rozema,

Bijgaand vindt u zoals afgesproken met [redacted] een advies over het gebruik van facturen van telecomgegevens tijdens het onderzoek van de provinciale onderzoekscommissie Eurochamp.

1. Op 18 maart 2009 hebben PS van Drenthe besloten tot het instellen van een onderzoek op basis van artikel 151a Provinciewet. Onderzoeksvragen zijn:

- *wie is verantwoordelijk voor de voortijdige verspreiding van het rapport van Deloitte inzake Eurochamp en op welke wijze is dat geschied;*
- *waren er bij de provincie Drenthe organisatorische en/of 'bestuurlijk-culturele¿ factoren die de voortijdige verspreiding hebben bevorderd;*
- *in hoeverre moet het gevoerde bestuur worden aangepast om nieuwe situaties van schending van integriteit en van de regels inzake geheimhouding te voorkomen.*

2. In het kader van dit onderzoek dient zich de vraag aan of facturen met daarop het

telefoonverkeer van diensttelefoons in het onderzoek betrokken mogen worden.

3. Het onderzoek vindt zijn formeelwettelijke grondslag in artikelen 151a-f van de Provinciewet. Voor het inbreuken op grondrechten (ic het recht op privacy) is een formeelwettelijke grondslag vereist. Aan dit vereiste is derhalve voldaan.

4. De inzet van een enquête is een zwaar middel waarbij stevige onderzoeksbevoegdheden kunnen worden ingezet. In die zin reiken de bevoegdheden van een dergelijk onderzoek verder dan de bevoegdheden/methoden in een regulier ambtenaarrechtelijk integriteitsonderzoek. Denk daarbij aan de mogelijkheid tot het horen van getuigen onder ede en de medewerkingsplicht. Deze constatering over de positionering in het "juridische landschap" is van belang omdat bij het bepalen van de rechtmatigheid van de onderzoeksmethoden minimaal de norm genomen kan worden die in ambtenaarrechtelijke zaken door de bestuursrechter gehanteerd wordt. Omdat over gemeentelijke en provinciale enquêtes nauwelijks jurisprudentie voorhanden is, kan aansluiting gezocht worden bij de jurisprudentie over de rechtmatigheid van het gebruik van telefoonverkeer in reguliere disciplinaire onderzoeken. Aan het einde van deze notitie daarover meer.

5. De onderzoeksbevoegdheid van de Staten (151a-f) is in 2003 ingevoerd bij de Wet dualisering provinciebestuur (stb.2003,17).

6. In artikel 151a Provinciewet wordt een aantal vormvoorschriften gegeven. Kijkend naar de beschikbare stukken is aan deze vereisten voldaan.

7. Een van die vormvereisten betreft het stellen van nadere regels over de wijze waarop het onderzoek is ingericht voordat besloten wordt tot enig onderzoek. Deze regels dienen per verordening te worden vastgesteld.

8. Drenthe heeft reeds in 2003 een dergelijke verordening vastgesteld: de "Verordening Onderzoekscommissie" (inwerkingtreding: 2 juli 2003, Provinciaal Blad 2003,55)

9. Artikel 7 van de verordening ziet op de bevoegdheden van de onderzoekscommissie. De onderzoekscommissie is bevoegd tot het opvragen en inzien van alle schriftelijke informatie die zij voor haar onderzoek nodig acht, met inachtneming van de bepalingen van de Provinciewet ten aanzien van geheimhouding. Het onderzoek kan zich mede uitstrekken tot alle archieven van de provincie.

10. Artikel 7 van de Verordening geeft daarmee een nadere (een m.i. correcte) invulling van hetgeen gesteld is in artikel 151b Provinciewet. Dit artikel geeft –kort gesteld- de onderzoekscommissie de bevoegdheid om inzage te vorderen, afschriften te maken en kennis te nemen van alle bescheiden waarover de bestuursorganen van de provincie en personen die voor de provincie werken beschikken voor zover dat naar het redelijk oordeel van de commissie nodig is.

11. Bij "bescheiden" in het kader van een financieel onderzoek kun je denken aan facturen, bonnen, agendaposten, verslagen van bijeenkomsten etc.. De reikwijdte van de onderzoeksbevoegdheden blijkt uit een uitspraak van het College van Beroep voor het bedrijfsleven dat oordeelde over de wijze waarop een accountantsbureau onderzoek had gedaan naar de functionaliteit van de uitgaven van het Rotterdamse gemeentebestuur 1986-1999. Ook hier was sprake van een vergelijkbaar enquête door de Raad. Om de functionaliteit van dienstreizen te beoordelen droeg men kennis van persoonlijke agenda van de burgemeester en de afschriften van zijn creditcard.

12. Facturen van diensttelefoons zijn m.i. zonder meer aan te duiden als "bescheiden"in de zin van 151b Provinciewet.

13. De volgende vraag is of de commissie in redelijkheid kan oordelen of de telefoonlijsten voor het onderzoek van belang zijn. Daarbij dient mede in ogenschouw genomen te worden dat de onderzoeksvragen het kader vormen waarbinnen de commissie haar taak uitoefent. Er kunnen geen documenten worden opgevraagd die niet in relatie staan tot de onderzoeksvraag.

14. Mede gezien de onderzoeksvragen is het mijns inzien zonder meer verdedigbaar om zicht te krijgen op de telefonische contacten van betroken personen. Uit de telefoonlijsten kan immers blijken of ze contact hebben gehad met de media. Onderzoek van facturen van diensttelefoons is in dit verband te typeren als een passende en noodzakelijke onderzoeksmethode. Ook de Verordening sluit dit niet uit. De facturen maken onderdeel uit van de archieven van de provincie.

15. De grenzen van de vordering die de commissie kan doen, komen in beeld wanneer de belangen de Europese Unie en de Staat in het geding zijn (151b lid 2). Dat is hier niet aan de orde.

16. Omdat het gaat om een bestuursrechtelijke onderzoek dient ook de evenredigheid (3:4 Awb) in acht genomen te worden. Nu het niet gaat om het vorderen van lijsten van de prive-telefoons, kan het middel als evenredig beoordeeld worden. Overwogen kan worden de lijsten pas te vorderen als interviews/openbare hoorzittingen niet tot duidelijkheid hebben geleid. Het is mijns inziens zelfs verdedigbaar om te stellen dat het onzorgvuldig is om na te laten de lijsten te checken. Het belang van de waarheidsvinding vraagt daarom.

17. Sommige publieke rechtspersonen hebben ervoor gekozen om interne richtlijnen te stellen over het gebruik van informatie en communicatietechnologie bij interne onderzoeken. Of in de provincie Drenthe dergelijke interne voorschriften heeft is niet bekend. Het ontbreken ervan doet niets af aan de bevoegdheid om telefoonlijsten te gebruiken. Het gaat immers niet om een regulier intern onderzoek, maar een onderzoek ex. artikel 151a Provinciewet. Nadere spelregels omtrent het gebruik van ICT zouden in de verordening een plaats dienen te hebben.
Het bestaan van interne richtlijnen is in die zin relevant dat het gebruik van

telefoonlijsten minder discutabel zou maken.

18. Met het oog op dezelfde zorgvuldigheid (hoor en wederhoor) is het verstandig om de betrokken persoon de analyse van het telefoonverkeer voor te houden en de informatie niet slechts als sturingsinformatie te gebruiken. Het is mijns inziens ook passend om in het onderzoeksverslag verantwoording af te leggen over de gebruikte onderzoeksmethoden.

19. Kijkend naar de bestuursrechtelijke jurisprudentie ten aanzien van reguliere disciplinaire onderzoeken dan is het zgn. "zozeer indruist-criterium"de maatstaf voor het bepalen van de rechtmatigheid van de bewijsvergaring. Slechts wanneer de bewijsvergaring op een wijze heeft plaatsgevonden die zozeer indruist tegen hetgeen van een fatsoenlijk handelen overheid mag worden verwacht, komt onrechtmatigheid in beeld.

20. De jurisprudentie overziende brengt mij tot de conclusie dat het gebruik van telefoonlijsten in de regel als een rechtmatige onderzoeksmethode gezien wordt. Niet alleen het gebruik van lijsten, maar ook de analyse van telefoongesprekken zelve (ook privé) wordt door de bestuursrechter regelmatig gehonoreerd. In dit verband wijs ik o.a. op de volgende uitspraken met de volgende LJN-nummers: BH1794 (gebruik geluidsopnamen meldkamer politie) BB1512 (onderzoek door Hoffman naar gebruik diensttelefoon/schaduwen ambtenaar) AY8153 (analyse 69 privégesprekken en Sms-berichten). Nu in reguliere disciplinaire onderzoeken deze methoden zijn toegestaan, is het zonder meer verdedigbaar deze methoden ook toe te passen in een onderzoek als onderhavige.

Ik hoop u hiermee voldoende geinformeerd te hebben.

Met vriendelijke groet,

[redacted]

Vertrouwelijk: Stafgroep Automatisering

provincie Drenthe

Handboek Informatiebeveiliging

Inhoudsopgave

1 Reikwijdte

Het handboek informatiebeveiliging is bestemd voor de afdeling automatisering van de Provincie Drenthe en beschrijft de richtlijnen, werkwijzen en procedures ten aanzien van de informatiebeveiliging zoals die gelden voor de afdeling automatisering.

Doelstelling
De doelstelling van het handboek voor Informatiebeveiliging is om helderheid te verschaffen over het beleid en maatregelen met betrekking tot informatiebeveiliging. Het Plan is een naslagwerk voor lijnmanagement en medewerkers van de afdeling automatisering.

Uitgangspunten bij het beleid
Beleid laat zich omschrijven als het bewuste streven naar een optimale verhouding tussen het doel (een exclusieve, integere en beschikbare informatievoorziening) en de middelen, maatregelen om dat doel te bereiken. De uitgangspunten bij de inrichting van de informatiebeveiliging zijn dat bij alle maatregelen een afweging moet worden gemaakt tussen de beveiligingaspecten, gebruiksgemak, (afbreuk-)risico's en de kosten van de maatregel.

Daarnaast geldt dat altijd moet worden voldaan aan wettelijke voorschriften als die voor een bepaald onderdeel van de informatievoorzieningen zijn vastgesteld. Te denken valt aan de Wet Persoonsregistratie (privacywet).

De sleutelwoorden (richtlijnen) bij het ontwerpen en vaststellen van beveiligingsmaatregelen zijn:

Afdoende	***Sober***	***Werkbaar***

Inhoud van dit handboek

Het handboek is gebaseerd op de code voor informatiebeveiliging: 2000. De indeling van het handboek is conform de indeling van de code.

2 Termen en definities

2.1 *Informatiebeveiliging*

Hoofdstuk : Termen en definities Onderwerp **Informatiebeveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 2 paragraafnummer : 2.1

Doelstelling
Helderheid verschaffen over begrippen rond informatiebeveiliging

Gebruikte termen en definities
Informatiebeveiliging:
het behoud van de vertrouwelijkheid, integriteit en beschikbaarheid van informatie
Vertrouwelijkheid:
informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn
Integriteit:
de informatie en de verwerking daarvan is correct en volledig
Beschikbaarheid:
geautoriseerde gebruikers hebben op de juiste momenten tijdig toegang tot informatie en aanverwante bedrijfsmiddelen

Bedrijfsmiddelen
de in dit Handboek onderscheiden onderdelen van de gegevenshuishouding
Infrastructuur
ICT personeel, netwerkcomponenten, computers, mobiele computers, systeemsoftware
Kantoorautomatisering
Bedrijfsmiddelen voor kantoorwerk als Office pakketten, e-mail en Internet toegang
Gegevens
Digitaal opgeslagen (groepen van) gegevens (data) en metagegevens (gegevens over gegevens)
Applicaties
Toepassingen die ondersteuning geven aan de bedrijfsprocessen

Waar gesproken wordt over *Informatiesystemen* wordt een combinatie van bovenstaande bedoeld.

Auteur: A. Visser
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

2.2 Risicoanalyse

Hoofdstuk : Termen en definities Onderwerp **Risicoanalyse en risicomanagement**	Verwijzing naar Code IB Hoofdstuknummer : 2 paragraafnummer : 2.1

Doelstelling

Helderheid verschaffen over begrippen rond risicoanalyse en risicomanagement

Gebruikte termen en definities

Risicoanalyse

Inventariseren van de bedreigingen en de kwetsbaarheid van informatie en IT bedrijfsmiddelen; beoordelen van de ernst en de kans op het optreden daarvan

Risicocategorieën van IT bedrijfsmiddelen

Indeling ter bepaling van de afhankelijkheid van de bedrijfsmiddelen. De volgende indeling wordt gehanteerd:

a) *Bedrijfsmiddelen voor calamiteitenbeheersing*
bedoeld voor communicatie en coördinatie en informatie tijdens calamiteiten waarbij de provincie is betrokken, in welke rol dan ook.

b) *Bedrijfsmiddelen voor vitale bedrijfsinformatie*
betreft systemen die essentieel zijn voor de bedrijfsvoering (bedrijfskritisch)

c) *Bedrijfsmiddelen voor (overheids)communicatie*
betreft systemen die zorgen voor externe communicatie via diverse media, als Websites, e-mail en kantoorapplicaties

d) *Overige bedrijfsmiddelen*
niet bedrijfskritische systemen

De indeling kan gevolgen hebben voor normen op het terrein van kwaliteit, beschikbaarheid, maximale uitval en uitwijkmaatregelen.

Auteur: A. Visser
Versie: 0.1
Datum: 1 april 2005

Akkoord:	Geldig tot: 1 januari 2006

2.3 *Risicomanagement*

Hoofdstuk : Termen en definities Onderwerp **Risicomanagement**	Verwijzing naar Code IB Hoofdstuknummer : 2 paragraafnummer : 2.3

Doelstelling

Helderheid verschaffen over begrippen rond risicoanalyse en risicomanagement

Gebruikte termen en definities

Risicomanagement

vaststellen, beheersen en minimaliseren (of elimineren) van de beveiligingsrisico's die IT bedrijfsmiddelen kunnen treffen tegen aanvaardbare kosten en inspanningen.

Auteur: A. Visser
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

3 Beveiligingsbeleid

Hoofdstuk : Beveiligingsbeleid Onderwerp : **Beleidsdocument voor Informatiebeveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 3 paragraafnummer : 3.1

Doelstelling
Het bieden van sturing en ondersteuning van het management ten behoeve van informatiebeveiliging

Toelichting
In het Informatiestatuut van de provincie, gepubliceerd in het Informatieplan 2002 – 2005 (statenstuk 887) zijn de kaders ten aanzien van de informatiebeveiliging aangegeven (zie bijlage bij dit blad). Daarnaast wordt er voor wat betreft het gebruik van Internet, mail en ICT bedrijfsmiddelen gewerkt met spelregels, die worden gepubliceerd op Huisnet.

De sleutelbegrippen voor maatregelen in het kader van Informatiebeveiliging zijn: afdoende, sober en werkbaar.

Nog in te voeren maatregelen
Reglement bedrijfsmiddelen
Reglement telewerken

Documentverwijzing
- Informatieplan 2002 – 2005 (statenstuk 887)

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

4 Beveiligingsorganisatie

4.1 De organisatorische infrastructuur voor informatiebeveiliging

Hoofdstuk : Beveiligingsorganisatie Onderwerp **Managementforum voor informatiebeveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 4 paragraafnummer : 4.1.1

Doelstelling

Een managementkader dient vastgesteld te worden om de implementatie van informatiebeveiliging in de organisatie op gang te brengen en te beheersen.
Er dienen, onder leiding van het management, geschikte forums te worden samengesteld voor het goedkeuren van het beleid ten aanzien van informatiebeveiliging, voor het toekennen van verantwoordelijkheden en voor het coördineren van de implementatie van de beveiliging binnen de organisatie. Het kan nodig zijn om binnen de organisatie één of meer specialisten voor informatiebeveiliging aan te wijzen. Ook dient contact te worden gelegd met externe beveiligingsspecialisten, zodat men op de hoogte blijft van industriële trends, normen en beoordelingsmethoden en er geschikte contactpersonen aanwezig zijn in geval van beveiligingsincidenten. Het verdient aanbeveling de informatiebeveiliging multidisciplinair te benaderen, bijvoorbeeld door de medewerking en samenwerking van managers, gebruikers, beheerders, ontwerpers van toepassingsprogramma's, auditors en beveiligingspersoneel en specialistische kennis op het gebied van bijvoorbeeld verzekeringen en risicomanagement.

Toelichting

De stuurgroep Informatie Management heeft de verantwoordelijkheid voor het adviseren aan GS inzake informatiebeveiliging. Bestaand beleid en wijzingen daarop zijn eigendom van de voorzitter van deze stuurgroep. In de stuurgroep hebben vaste zitting directie (voorzitter), gebruikersorganisatie, beheerder van de geautomatiseerde informatiesystemen en dataopslag. Bij het organisatieonderdeel belast met het beheer van Informatiesystemen zal een medeweker worden belast met de uitvoering van het vastgestelde beveiligingsbeleid

Nog in te voeren maatregelen

NB: de directie moet nog tot de hierboven genoemde werkwijze besluiten.

Documentverwijzing

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

4.2 *Beveiliging van toegang door derden*

Hoofdstuk : Beveiligingsorganisatie Onderwerp **Managementforum voor informatiebeveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 4 paragraafnummer : 4.2

Doelstelling

De toegang tot de IT-voorzieningen van de organisatie door derden dient te worden beheerst.
Op plaatsen waar toegang door derden zakelijk gezien noodzakelijk is, dient door middel van een risicoanalyse te worden bepaald welke gevolgen dit heeft voor de beveiliging en welke maatregelen dienen te worden getroffen. Over deze maatregelen dient overeenstemming te worden bereikt en zij dienen te worden vastgelegd in een contract met de betrokken derden.
Bij toegang door derden kunnen ook andere partijen betrokken zijn. In contracten waarin aan derden toegang wordt verleend dient vastgelegd te worden of en welke andere partijen geautoriseerde toegang kan worden verleend alsmede de voorwaarden waarop zij toegang kunnen krijgen.
De Code kan worden gebruikt als basis voor dergelijke contracten. De Code is tevens te gebruiken als leidraad wanneer wordt overwogen om de informatieverwerking uit te besteden.

Toelichting

Toegang door derden tot het netwerk kan alleen na goedkeuring van de opdrachtgever van de externe partner. Door het aangaan van het contract geeft de opdrachtgever tevens goedkeuring aan het verlenen van toegang tot het interne netwerk voor de algemene toepassingen. Dat zijn de toepassingen Office (Word, Excel, PowerPoint), GroupWise (incl. internet e-mail), huisnet, Internet en tijdschrijven. De interne opdrachtgever dient hiertoe telefonisch een verzoek te richten aan de helpdesk waarbij ook wordt aangegeven voor welke periode de externe partner toegang wordt verleend. De helpdesk zal de aanvraag vastleggen en, indien gewenst, periodiek rapporteren aan de stuurgroep. Voor het verlenen van toestemming voor toegang tot databestanden zal de eigenaar van de databestanden toestemming moeten verlenen. Daartoe zal de opdrachtgever een schriftelijk verzoek doen bij de eigenaar waarbij naam, reden en periode wordt vermeld. Dit verzoek moet de eigenaar na goedkeuring doorsturen naar de Helpdesk.

Nog in te voeren maatregelen

Documentverwijzing

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

4.3 *Uitbesteding*

Hoofdstuk : Beveiligingsorganisatie Onderwerp **Uitbesteding**	Verwijzing naar Code IB Hoofdstuknummer : 4 paragraafnummer : 4.3

Doelstelling
Het handhaven van de beveiliging van informatie, wanneer de verantwoordelijkheid voor informatieverwerking is uitbesteed aan een andere organisatie.
Uitbestedingregelingen dienen in te gaan op de risico's, beveiligingsmaatregelen en procedures voor informatiesystemen, netwerken en /of werkstations in het contract tussen de partijen.

Toelichting

Uitbesteding van Informatieverwerking dient altijd te geschieden door het organisatieonderdeel belast met het beheer van de informatiesystemen. Dit organisatieonderdeel zal goedkeuring verlenen nadat een analyse is gemaakt over de impact. De analyse zal bestaan uit:

- vaststellen voor welke gegevens een goedkeuring zal worden gegeven
- vaststellen wie eigenaar is van de gegevens
- vaststellen van het risiconiveau, door de eigenaar aan te geven

Bij een laag risiconiveau zal het organisatieonderdeel zelfstandig de aanvraag accorderen en periodiek rapporteren over de gemaakte afspraken aan de stuurgroep IM. Bij een, naar de mening van het organisatieonderdeel, groot risiconiveau zal toestemming worden gevraagd aan de stuurgroep IM.

Nog in te voeren maatregelen

Documentverwijzing

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

5 Classificatie en beheer van bedrijfsmiddelen

Hoofdstuk : Classificatie en beheer bedrijfsmiddelen Onderwerp : **Verantwoording voor bedrijfsmiddelen**	Verwijzing naar Code IB Hoofdstuknummer : 5 paragraafnummer : 5.1 en 5.1.1

Doelstelling
Alle belangrijke informatiebedrijfsmiddelen dienen te zijn verantwoord en aan een "eigenaar" toegewezen. Het bepalen van de verantwoordelijkheden voor bedrijfsmiddelen draagt ertoe bij dat deze op de juiste manier beveiligd blijven.

Toelichting
Het eigendom van de bedrijfsmiddelen is als volgt belegd:

Bedrijfsmiddel	Eigenaar
Calamiteitensysteem	Hoofd kabinet
ProBiS	Concern Controller (Hoofd FC)
Afdelingssystemen	Lijn
Kantoorautomatisering	Stafgroep automatisering
Computersystemen (hardware en OS)	Stafgroep automatisering
Netwerkcomponenten	Stafgroep automatisering
Telefoniesystemen	Facilitaire groep

De taken zijn als volgt verdeeld:
Functioneel beheer, wordt uitgevoerd door de Eigenaar van de toepassing.
Definiëren functionaliteit van toepassing en vereiste SLA. Beslist omtrent nieuwe functionele eisen. Stelt eisen aan niveau van informatiebeveiliging en stelt autorisatie vast.
Applicatie beheer wordt uitgevoerd door de stafafdeling Automatisering.
Toekennen autorisaties (technisch uitvoerend). Installeren en inrichten van software op basis van eisen van functioneel beheerder.
Technisch beheer, wordt uitgevoerd door de Stafafdeling Automatisering
Beheer van netwerk; systemen en databases. Draagt zorg voor beschikbaarheid van technische middelen. Autorisaties tot netwerken; systemen en databases.

De automatiseringsbedrijfsmiddelen zijn geregistreerd in de configuratiedatabase van Assyst.

Nog in te voeren maatregelen
De verdeling van taken en bevoegdheden die er zijn voor de informatiefunctie moeten als uitvloeisel van het Integraalmanagement concept verder worden toegespitst.

Documentverwijzing

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Classificatie en beheer bedrijfsmiddelen Onderwerp : **Classificatie van Informatie**	Verwijzing naar Code IB Hoofdstuknummer : 5 paragraafnummer : 5.2

Doelstelling
Informatie dient te worden geclassificeerd, om de behoefte aan, de prioriteit en de mate van beveiliging aan te geven.

Huidige werkwijze

Classificatie
De volgende classificaties worden gehanteerd:

Openbaar
Informatie die voor derden toegankelijk is (lezen). Wijzigen van deze informatie kan uitsluitend door medewerkers van de Provincie (eigenaar) plaats vinden.

Niet Openbaar, onderverdeeld in:

Intern gebruik
Alle interne informatie die uitsluitend voor medewerkers van de provincie Drenthe toegankelijk is. Op basis van functie worden toegangsrechten tot deze informatie toegekend.

Vertrouwelijk
Informatie die uitsluitend voor een beperkte groep medewerkers van de provincie toegankelijk is. Bij de informatie dient aangegeven te worden wie toegang heeft tot de informatie.

Persoonlijk
Informatie uitsluitend bestemd voor de geadresseerde.

Labelen en verwerken van informatie
- Voor alle informatiesystemen wordt de geldende classificatie van informatie vastgesteld.
- Informatie zonder label wordt als "Intern gebruik" behandeld.
- Documenten met vertrouwelijke en persoonlijke informatie dienen op de voorpagina en in de koptekst voorzien te zijn van het label.

Nog in te voeren maatregelen
- Voor alle informatiesystemen dient de classificatie van de informatie vastgesteld te worden door de eigenaar.
- Verstrekking van informatie omtrent labeling en classificatie aan medewerkers.

Documentverwijzing

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

6 Beveiligingseisen ten aanzien van personeel

NB: dit hoofdstuk doornemen met PO. Insteek: geen aparte zaken opnemen in arbeidscontracten etc.

6.1 Beveiligingseisen in functieomschrijving en aannemen van personeel

Hoofdstuk : Beveiligingseisen t.a.v. personeel Onderwerp : Beveiligingseisen in de functieomschrijving	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.1.1

Doelstelling

Het verminderen van de risico's van menselijke fouten, diefstal, fraude of misbruik van voorzieningen. Het opnemen van beveiligingseisen in de functieomschrijving zorgt ervoor dat de betreffende functionaris op de hoogte is van de beveiligingseisen en bij aanname van personeel de beveiligingseisen worden meegewogen.

Toelichting

Beveiligingstaken en verantwoordelijkheden zijn vastgelegd in de functieomschrijvingen. Op basis van het bestaande Informatieplan is gekozen de IT-functies te beschrijven middels de methodiek van het Nederlands Genootschap van Informatica (NGI). Het gaat qua uitvoering/toezicht om de volgende functies:

- Coördinator technische infrastructuur (Stafgroep Automatisering)
- Beheerder technische infrastructuur (Stafgroep Automatisering)
- Gegevens(bank)beheerder (Stafgroep Automatisering)
- Applicatiebeheerder (Stafgroep Automatisering)
- Functioneel beheerder (Lijn)

Nog in te voeren maatregelen

- Voor directie en lijnmanagers moet de in paragraaf 2.1.1 beschreven beleidsverantwoordelijkheid separaat worden omschreven.
- Functieomschrijving voor functioneel beheerder dient opgesteld te worden (project functioneel beheer) en voor applicatiebeheer aangepast.

Documentverwijzing

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beveiligingseisen t.a.v. personeel Onderwerp **Screening en personeelsbeleid**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.1.2

Doelstelling
Het screenen van personeel voor functies waarbij specifieke eisen aan beveiliging worden gesteld. Te denken valt aan referenties, controle op de volledigheid, juistheid van het C.V. en bij bijzonder gevoelige functies een controle op de kredietwaardigheid van de sollicitant.

Toelichting
Tijdens de sollicitatieprocedure worden sollicitanten beoordeeld op integriteit. Nieuwe medewerkers leggen de ambtseed af.

Nog in te voeren maatregelen
-

Documentverwijzing

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beveiligingseisen t.a.v. personeel Onderwerp **Geheimhoudingsverklaring**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.1.3

Doelstelling
De geheimhoudingsverklaring heeft tot doel medewerkers bewust te maken van de regels en plichten van de medewerker.

Toelichting
De plicht tot geheimhouding is geregeld in het ambtenarenreglement. In het arbeidscontract van de medewerkers is een verwijzing naar dit reglement opgenomen.

Nog in te voeren maatregelen
-

Documentverwijzing

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beveiligingseisen t.a.v. Personeel Onderwerp **Arbeidscontract**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.1.4

Doelstelling
Door ondertekening van het arbeidscontract wordt de medewerker gewezen op werkwijzen en regels ten aanzien van beveiliging.

Toelichting
De volgende maatregelen zijn getroffen:
- De functieomschrijving, inclusief verantwoordelijkheden ten aanzien van beveiliging maken deel uit van het arbeidscontract.
- Het ambtenarenreglement, wat integraal onderdeel uitmaakt van het arbeidscontract, bevat geheimhoudingsverklaring.
- In het arbeidscontract van de medewerkers van de stafgroep automatisering wordt verwezen naar het handboek informatiebeveiliging, waar de medewerker kennis van moet nemen. Het handboek bevat onder meer:
    - De wettelijke rechten en plichten van de werknemer, bijvoorbeeld ten aanzien van de wetgeving op het gebied van auteursrecht en gegevensbescherming zijn opgenomen in het handboek informatiebeveiliging.
    - De verantwoordelijkheid voor de classificatie en het beheer van de gegevens van de werkgever te worden opgenomen.
    - Waar van toepassing dient het arbeidscontract te vermelden dat deze verantwoordelijkheden zich uitstrekken tot buiten het bedrijfsterrein van de organisatie en ook buiten de normale werktijden gelden, bijvoorbeeld in het geval van thuiswerken.
- Bij de introductie van nieuw personeel wijst de direct leidinggevende de nieuwe medewerker op de geheimhoudingsplicht conform het geldende ambtenarenrecht. Ook wijst de direct leidinggevende op de plicht tot het juist gebruik van de middelen die ter beschikking worden gesteld voor het uitoefenen van de opgedragen taken.

Nog in te voeren maatregelen
- Controle en eventueel aanpassing arbeidscontracten.

Documentverwijzing

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

6.2 *Training voor gebruikers*

Hoofdstuk : Beveiligingseisen t.a.v. Personeel Onderwerp **Opleiding en training voor informatiebeveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.2.1

Doelstelling
Waarborgen dat gebruikers zich bewust zijn van de bedreigingen voor en de belangen van informatiebeveiliging en hen te voorzien van de juiste middelen om het beveiligingsbeleid te ondersteunen tijdens het uitvoeren van hun normale werkzaamheden.

Gebruikers dienen te worden getraind in het omgaan met de beveiligingsprocedures en het correcte gebruik van IT-voorzieningen, om eventuele beveiligingsrisico's te minimaliseren.

Toelichting
Opleiding en training vindt als volgt plaats:
- In de standaard introductiecursus voor medewerkers worden het beveiligingsbeleid en de bijbehorende procedures opgenomen. Wijzigingen worden via mededeling op het netwerk (prikbord) kenbaar gemaakt. Uiteraard valt hier ook onder dat een juist gebruik van de ICT voorzieningen onderwezen wordt.
- Voor medewerkers die geen introductiecursus volgen wordt het cursusmateriaal beschikbaar gesteld en volgt instructie door IT personeel.
- Specifieke beveiligingstraining voor het gebruik van applicaties valt onder de verantwoordelijkheid van de functioneel beheerder. Uiteraard valt hier ook onder dat een juist gebruik van de applicaties onderwezen wordt.
- Op het Huisnet is informatie opgenomen ten aanzien van procedures en richtlijnen voor gebruikers van informatiesystemen. Wijzigingen worden via het Huisnet gecommuniceerd.
- Medewerkers van de stafgroep automatisering dienen het handboek informatiebeveiliging te lezen en kennis te nemen van de maatregelen.
- bij de introductie wijst de leidinggevende de nieuwe medewerker op de plichten inzake geheimhouding en omgaan met apparatuur.
- De stafgroep Automatisering informeert de medewerkers via publicaties, folders en Huisnetberichten over het onderwerp beveiliging.

Nog in te voeren maatregelen
- Informatieverstrekking aan alle medewerkers van de provincie
- Informatiebeveiliging opnemen op het Huisnet.
- Introductiecursus

Documentverwijzing

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

6.3 *Reageren op beveiligingsincidenten en storingen*

Hoofdstuk : Beveiligingseisen t.a.v. personeel Onderwerp **Rapporten van beveiligingsincidenten**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer :3.1

Doelstelling
Incidenten die de beveiliging aantasten, dienen zo snel mogelijk via de geëigende managementkanalen te worden gerapporteerd.

Toelichting
Incidenten moeten door medewerkers formeel worden gerapporteerd aan de verantwoordelijke lijnmanager en aan het hoofd van de Stafgroep Automatisering Het hoofd van de Stafgroep Automatisering rapporteert bij ernstige incidenten aan de directie.

In praktische zin moeten medewerkers en tijdelijk personeel echter een beperkt aantal "aanspreekpunten" hebben om dergelijke meldingen kwijt te kunnen. De praktische procedure is:

- Medewerker rapporteert incident aan de Helpdesk (tel 57 89).
- Helpdesk registreert incident in Assyst en rapporteert incident afhankelijk van het type aan:
    - coördinator technische infrastructuur
    - Eigenaar/ functioneel beheerder
    - gegevens(bank) beheerder
    - medewerker belast met beveiligingsvraagstukken. Deze medewerker besluit hoe het incident verder zal worden verwerkt.

- De helpdesk bewaakt de afhandeling van het incident.
- Rapportage vindt plaats in de lijn:
    - Automatiseringsmedewerkers rapporteren aan Hoofd Stafgroep Automatisering en eventueel aan betrokken lijnmanagers;
    - Hoofd Stafgroep Automatisering rapporteert eventueel aan concernstaf
    - Functioneel beheerder onderneemt actie en rapporteert incident aan hiërarchisch lijnmanager en i.a.a. hoofd Stafgroep Automatisering *(secr. STINFO)*

Nog in te voeren maatregelen

Documentverwijzing

- Handboek ICT beheer

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beveiligingseisen t.a.v. personeel Onderwerp **Het rapporteren van zwakke plekken in beveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.3.2

Doelstelling
Medewerkers (gebruikers) zijn verplicht alle zwakke plekken in (of bedreigingen van) de beveiliging van systemen of diensten die zij opmerken dan wel vermoeden, te rapporteren.

Toelichting
De procedure voor rapportage is identiek aan de rapportage inzake beveiligingsincidenten, paragraaf 6.3.1 Ten aanzien van zwakke plekken gelden de volgende maatregelen:

- Gebruikers mogen onder geen enkele voorwaarde de mogelijke aanwezigheid van een zwakke plek proberen te bewijzen. Ter eigen bescherming. Omdat pogingen om een zwakke plek te testen gezien kunnen worden als misbruik van IT-voorzieningen.
- Alleen bevoegd personeel (Stafgroep Automatisering eventueel i.o.m. de functioneel en applicatiebeheerder) mag een dergelijke test uitvoeren.

Nog in te voeren maatregelen
-

Documentverwijzing

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beveiligingseisen t.a.v. personeel Onderwerp **Het rapporteren van onvolkomenheden in software**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.3.3

Doelstelling
Ook onvolkomenheden in applicatieprogrammatuur en/of kantoorautomatiseringpakketten dienen door gebruikers te worden gerapporteerd. Een onvolkomenheid betreft het niet correct werken (d.w.z. niet volgens de specificaties).

Toelichting

De procedure is identiek aan de rapportage inzake beveiligingsincidenten, zie paragraaf 4.3.1.

Bij een storing die te wijten valt aan slecht functionerende programmatuur dient de gebruiker:
- Alle symptomen en berichten die op het scherm verschijnen te noteren.
- De computer niet meer te gebruiken (zo mogelijk afzonderen)
- Eventuele diskettes niet te verwijderen
- Melden aan de Helpdesk (26 57 89) en eventueel applicatiebeheerder

Gebruikers mogen onder geen enkele voorwaarde de verdachte programmatuur testen dan wel verwijderen. De programmatuur dient te worden hersteld door personeel van de Stafgroep Automatisering of van de betreffende leverancier dat daarvoor is opgeleid.

Nog in te voeren maatregelen
Informeren van gebruikers

Documentverwijzing
-

Auteur [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beveiligingseisen t.a.v. personeel Onderwerp **Lering trekken uit incidenten**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.3.4

Doelstelling
Lering trekken uit incidenten heeft tot doel:
- Terugkerende beveiligingsproblemen te detecteren en maatregelen treffen ter voorkoming van deze maatregelen.
- Veranderingen in bedreigingen tijdig te detecteren en hier passende maatregelen tegen te treffen.

Toelichting
- Momenteel is dit proces niet ingericht.

Nog in te voeren maatregelen
Onderdeel van het ITIL problem management proces is detectie van beveiligingsproblemen. Dit betekent:
- Het regelmatig analyseren van gemelde beveiligingsincidenten. Dit betreft meldingen in Assyst alsmede analyse van meldingen en logfiles van systemen en applicaties.
- Bij de analyse de beveiligingsincidenten classificeren en trends bijhouden. Bij veranderingen dienen maatregelen onderzocht te worden.
- Bij detectie van nieuwe of toegenomen bedreigingen dient het risicoprofiel aangepast te worden en eventuele aanvullende maatregelen getroffen te worden.
- Bij veranderingen in bedreigingen en het risicoprofiel dient eventuele aanpassing van het beveiligingsbeleid overwogen te worden.

Documentverwijzing
- Handboek ICT Beheer – probleemmanagement

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beveiligingseisen t.a.v. personeel Onderwerp **Disciplinaire maatregelen**	Verwijzing naar Code IB Hoofdstuknummer : 6 paragraafnummer : 6.3.5

Doelstelling
Er dient een formele procedure met disciplinaire maatregelen te zijn. Dit voor medewerkers die opzettelijk het beveiligingsbeleid of de bijbehorende procedures doorbreken. Enerzijds werkt dit als afschrikmiddel, anderzijds schept het duidelijkheid en zorgt ervoor dat betrokken medewerkers gelijk, correct en eerlijk worden behandeld.

Toelichting
Het ambtenarenreglement voorziet in deze procedure.

Nog in te voeren maatregelen
-

Documentverwijzing
-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

7 Fysieke beveiliging en beveiliging van de omgeving

7.1 *Beveiligde ruimten*

Hoofdstuk : Fysieke beveiliging Onderwerp **Fysieke beveiliging van de omgeving**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.1.1

Doelstelling

Het voorkomen van ongeautoriseerde toegang tot, schade aan of verstoring van de gebouwen en informatie van de organisatie.

Toelichting

De ruimtes die fysiek moet worden beveiligd zijn:

- de centrale computerruimte (kamer 2.26). De computerruimte is voorzien van slagvast glas en fysieke toegangsbeveiliging.
- de clusterruimtes (kamers 2.34, 2.61, 1.21 , 1.13). Twee clusterruimtes (1.13 en 2.61) zijn als zodanig niet fysiek beveiligd, maar de netwerkapparatuur in deze ruimtes bevindt zich in afgesloten kasten.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Fysieke toegangsbeveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer :7.1.2

Doelstelling
Het voorkomen van ongeautoriseerde toegang tot, schade aan of verstoring van de gebouwen en informatie van de organisatie.

Toelichting
De centrale computerruimte is beveiligd met een elektronische toegangsbeveiliging met cijfercode. De toegangscode van de centrale computerruimte is slechts bekend bij geautoriseerd personeel. Overig personeel of onderhoudspersoneel kan slechts met toestemming en onder verantwoording van geautoriseerd personeel toegang verkrijgen. Het openen gebeurt door geautoriseerd personeel op zodanige wijze dat de code niet wordt vrijgegeven. Derden mogen uitsluitend onder begeleiding of na toestemming van een geautoriseerde medewerker van de stafgroep automatisering in de computerruimten werken.

De clusterkasten zijn bereikbaar met een sleutel. Slechts geautoriseerd personeel mag een kast openen. Indien geautoriseerd personeel de betreffende ruimtes verlaat worden deze gesloten of onder direct toezicht op de toegang van geautoriseerd personeel geplaatst. Ook hier geldt dat slechts geautoriseerd personeel van de Stafgroep Automatisering en Facilitaire Groep in bezit kan komen van de sleutel.

Bij vertrek/ontslag van geautoriseerd personeel wordt de toegangscode van de centrale computerruimte onmiddellijk aangepast. Bij verlies van een of meerdere sleutels van de clusterkasten worden de sloten vervangen. Het beheer van code en sleutels is in handen van een ICT systeemspecialist.

Nog in te voeren maatregelen

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Beveiliging van kantoren, ruimten en voorzieningen**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.1.3

Doelstelling

Het voorkomen van ongeautoriseerde toegang tot, schade aan of verstoring van de gebouwen en informatie van de organisatie.

Toelichting

De beveiligde ruimten zijn beschreven in paragraaf 7.1.1. De volgende beveiligingsmaatregelen gelden voor computerruimten:

- De centrale computerruimte is voorzien van:
    a. Slagvast glas;
    b. Rookmelder;
    c. Koelinstallatie;
    d. Noodstroomvoorziening.
- Apparaten zoals kopieermachines en faxapparatuur, papieropslag worden niet in het beveiligde gebied geplaatst, zodat ongeautoriseerd personeel zo weinig mogelijk in het beveiligde gebied komt en gevoelige informatie zo beperkt mogelijk in gevaar wordt gebracht.
- Gevaarlijke en brandbare materialen worden opgeslagen op een veilige afstand van computervoorzieningen. Computertoebehoren zoals papier mogen pas op het moment dat ze nodig zijn in de computerruimte worden geplaatst. In de computerruimte is branddetectie aanwezig en in de onmiddellijke omgeving is brandblusapparatuur aanwezig.

Voor kantoren geldt:

- Er worden geen bedrijfsgegevens opgeslagen op systemen die zijn opgesteld in niet beveiligde ruimten (Personal Computers), standaard worden gegevens opgeslagen op de centrale servers. Vooralsnog wordt een uitzondering gemaakt voor specifieke gegevensbestanden die nog niet op een server opgeslagen kunnen worden!

Nog in te voeren maatregelen

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Werken in beveiligde ruimten**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.1.4

Doelstelling

Het waarborgen van de beveiliging van beveiligde ruimten.

Toelichting

De volgende maatregelen gelden:

a) Het personeel dient alleen indien noodzakelijk op de hoogte te zijn van het bestaan van of de activiteiten binnen een beveiligde ruimte.
b) Derden, ook inhuur, moet onder toezicht werken in beveiligde ruimten zowel om veiligheidsredenen als om de kans op kwaadwillige handelingen te voorkomen.
c) Leegstaande beveiligde ruimten dienen fysiek te zijn afgesloten en periodiek te worden gecontroleerd.
d) Aan personeel van externe ondersteunende diensten dient alleen wanneer dit noodzakelijk is beperkte toegang te worden verleend tot beveiligde ruimten of voorzieningen waar gevoelige informatie wordt verwerkt. Deze toegang dient goedgekeurd en bewaakt te worden.
e) Fotografische, video-, audio- of andere opnameapparatuur is niet toegestaan, tenzij hier autorisatie voor is verleend door de coördinator informatiebeveiliging.
f) Roken en eten in ruimten met centrale computerapparatuur is verboden.

Nog in te voeren maatregelen

- Bovenstaande regels bekend maken en toezien op naleving.

Documentverwijzing

-

Auteur [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Afgeschermde ruimten voor laden en lossen**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer :7.1.5

Doelstelling
Voorkomen van diefstal van apparatuur en zoekraken van bestellingen.

Toelichting
De aflevering van goederen geschiedt na tussenkomst van de Facilitaire Groep via afsluitbare ruimten en wel in de kamers 2.34 of 0.0.16.

Nog in te voeren maatregelen
- Invoering van procedures door de sectie Inkoop die toezien op levering en ophalen van goederen.

Documentverwijzing

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

7.2 Beveiliging van apparatuur

Hoofdstuk : Fysieke beveiliging Onderwerp **Het plaatsen en beveiligen van apparatuur**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.2

Doelstelling

Het voorkomen van verlies, schade of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsvoering door de juiste plaatsing van apparatuur.

Toelichting

Alle servers en centrale computersystemen worden in de centrale computerruimte geplaatst. De centrale computerruimte is voorzien van de volgende beveiligingen:

- Noodstroomvoorziening met een waarschuwingssysteem bij uitval van netstroom.
- Rookmelders.
- Eten en drinken in de computerruimten is niet toegestaan.
- Fysieke beveiliging.
- Opslag van brandgevoelige en chemische middelen in de nabijheid van de computerruimte is niet toegestaan.

De computerruimte is zodanig geplaatst en ingericht dat er geen problemen zijn te verwachten zijn met stof; wateroverlast; trillingen; chemische reacties; interferentie via de elektriciteitsvoorziening en elektromagnetische straling.

Op de werkplekken worden **uitsluitend** PC's, laptops en randapparatuur gebruikt. Waar noodzakelijk worden PC's en laptops voorzien van een anti diefstal kabel (Kensington kabel) en niet verwijderbare eigendomssticker. Overige apparatuur wordt niet in kantoorruimtes geplaatst.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Stroomvoorziening**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.2.2

Doelstelling

Het voorkomen van verlies, schade of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsvoering door problemen in de stroomvoorziening.

Toelichting

Een UPS (Uninterruptable Power Supply) en een noodstroomvoorziening zijn aanwezig ten behoeve van de centrale computerapparatuur en de clusterruimtes waarin rangeerappartuur is opgesteld t.b.v. het netwerk.

De UPS- en noodstroomapparatuur wordt in samenwerking met de Facilitaire Groep regelmatig getest volgens de voorschriften van de fabrikant. Bij uitval van een UPS wordt na stroomuitval op reguliere wijze opgestart waarbij verlies van data niet uit te sluiten valt. Dit risico wordt aanvaardbaar geacht.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Beveiliging van kabels**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.2.3

Doelstelling

Het voorkomen van interceptie en beschadiging aan het bekabelingsysteem.

Toelichting

Bekabeling voor dataverkeer ligt in kabelgoten. Deze maatregelen zijn tijdens de aanleg en uitbouw van het netwerk volgens het bestek voor de aanleg van het datanetwerk uitgevoerd. Dit bestek is onderdeel van het contract met de leverancier van het netwerk en blijft geldig. De Facilitaire Groep bewaakt na acceptatie de kwaliteit van de kabel(goten)structuur.

Nog in te voeren maatregelen

-

Documentverwijzing

- Programma van eisen bekabelingsysteem (bestek bekabeling 1991)

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Onderhoud van apparatuur**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.2.4

Doelstelling

Het voorkomen van verlies, schade of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsvoering als gevolg van slecht onderhoud aan apparatuur.

Toelichting

Apparatuur dient op de juiste wijze te worden onderhouden met in achtneming van het volgende:

- Apparatuur wordt onderhouden volgens de voorschriften van de leverancier en op geregelde tijden zoals door de leverancier wordt aanbevolen. Hiertoe wordt voor alle systemen een onderhoudscontract afgesloten.
- Reparatie en onderhoud van apparatuur mogen alleen worden uitgevoerd door geautoriseerd onderhoudspersoneel.
- Er wordt een overzicht bijgehouden van alle storingen of mogelijke storingen. Alle incidenten worden geregistreerd in Assyst. Handleidingen van systemen dienen informatie te verschaffen over mogelijke storingen en wijze van handelen bij het optreden van de storing. Dit wordt bij de verwerving van systemen opgenomen.

Nog in te voeren maatregelen

- Handboek Operationeel Beheer

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Beveiliging van apparatuur buiten de locatie**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.2.5

Doelstelling

Het voorkomen van verlies, schade of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsvoering aan extern opgestelde apparatuur.

Toelichting

Beveiligingsprocedures en beveiligingsmaatregelen dienen ook te gelden voor apparatuur die buiten het bedrijf wordt gebruikt. Hiervoor gelden de volgende richtlijnen:

- Personal computers mogen thuis niet worden gebruikt voor bedrijfsactiviteiten als er geen viruscontrole (zie 6.3.1) wordt toegepast. Medewerkers worden hierover geïnformeerd.
- Tijdens het vervoer mogen apparatuur (en media) niet onbeheerd worden achtergelaten in publieke ruimten. Draagbare computers dienen tijdens het reizen als handbagage te worden vervoerd.
- Draagbare computers met relevante informatie op de harde schijf dienen te worden beveiligd met sloten, wachtwoorden of andere maatregelen.

Nog in te voeren maatregelen

- Optie om voor Windows XP het gebruik van EFS (encrypted file system) in te voeren.
- Optie om bij inloggen bij telewerken te controleren op viruscontrole programma (afh. van inlogproces bij VPN).
- Optie om een anti-spyware programma te installeren.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Veilig afvoeren en hergebruik van apparatuur**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.2.6

Doelstelling

Het voorkomen van uitlekken van informatie bij afvoeren en hergebruik van apparatuur.

Toelichting

Bedrijfsgegevens kunnen worden gecompromitteerd wanneer apparatuur onzorgvuldig wordt afgevoerd. Bij afvoer van apparatuur en media gelden de volgende maatregelen:

- Alle onderdelen van de apparatuur waarop gegevens kunnen worden opgeslagen (bijvoorbeeld vaste schijven) dienen te worden gecontroleerd en er dient voor te worden gezorgd dat alle gevoelige gegevens en gelicentieerde programmatuur worden verwijderd of overschreven voordat de apparatuur wordt afgevoerd. Als apparatuur hergebruikt wordt voor derden dan moet dit op zodanige wijze gebeuren dat software gemaakt om bestanden te reproduceren (als 'Undelete' functionaliteit) niet meer bruikbaar is. Dit kan via een gecertificeerd bedrijf, een speciaal daarvoor ontwikkeld programma of door de media minimaal 7 keer **volledig** te formatteren.
- Media, zoals CD-ROM's; magneetbanden; harde schijven en diskettes worden vernietigd.

Het kan nodig zijn om voor beschadigde opslagmedia die bijzonder gevoelige gegevens bevatten een risico-analyse uit te voeren om te bepalen of deze dienen te worden vernietigd of gerepareerd.

Verantwoordelijk voor de uitvoering is de sr. ICT systeemspecialist.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

7.3 *Algemene beveiligingsmaatregelen*

Hoofdstuk : Fysieke beveiliging Onderwerp **Clear desk en clear screen policy**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.3.1

Doelstelling:
Informatie en IT-voorzieningen dienen te worden beveiligd tegen bekendmaking aan, wijziging of diefstal door ongeautoriseerde personen. Er dienen maatregelen te worden genomen om het verlies en de schade te minimaliseren.

Toelichting
Voor de kamers van personeel van de Stafgroep Automatisering geldt:
- Diskettes/tapes/CDROM, met name als sprake is van geregistreerde en/of gelicenceerde software dienen te worden opgeborgen in een kast wanneer zij niet worden gebruikt en zeker buiten werktijd.
- Gevoelige of kritieke gegevens dienen achter slot en grendel te worden opgeborgen. (Bij voorkeur in een brandvrije kluis, zeker wanneer het kantoor verlaten is.)
- In principe worden er geen gegevens op de lokale schijf van PC's opgeslagen. Als dit toch noodzakelijk is wordt de lokale harde schijf beveiligd door middel van sloten, moet de PC zijn voorzien van wachtwoorden en de data op de schijf gecodeerd worden.

Voor alle PC's geldt:
- Er is een gebruiksvriendelijke functie om schermbeveiliging te activeren.

Nog in te voeren maatregelen
- Alle medewerkers krijgen informatie omtrent informatiebeveiliging via folders, introductiecursussen en het huisnet.
- Er geldt (nog) geen clear desk policy voor alle werkplekken. Uiteraard kan het betrokken lijnmanagement ook besluiten een dergelijke clear-desk policy in te voeren in de eigen werkruimtes. Met name als het gaat om gevoelige informatie op gemakkelijk te kopiëren media als diskettes. Alle medewerkers van de provincie krijgen aanvullende informatie ten aanzien van de informatiebeveiliging.
- Lokale schijven beveiligen met sloten en encryptie

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Fysieke beveiliging Onderwerp **Het verwijderen van bedrijfseigendommen**	Verwijzing naar Code IB Hoofdstuknummer : 7 paragraafnummer : 7.3.2

Doelstelling
Voorkomen dat bedrijfseigendommen worden meegenomen.

Toelichting
Bedrijfseigendommen mogen alleen worden verwijderd wanneer daarvoor toestemming is verleend. Apparatuur, gegevens en programmatuur van het bedrijf mogen niet door medewerkers uit het gebouw worden verwijderd zonder formele toestemming van de *sr. ICT systeemspecialist* of bij zijn afwezigheid *het hoofd van de Stafgroep Automatisering*. Het uitlenen van draagbare computerapparatuur is gedelegeerd aan de helpdesk medewerkers.

Van alle uitgeleende apparatuur wordt een registratie bijgehouden door de helpdesk. Bij uitleen van apparatuur dienen medewerkers een bruikleen overeenkomst te ondertekenen. Onderdeel van deze overeenkomst is instructie ten aanzien van gebruik en beveiliging van het systeem.

Nog in te voeren maatregelen
- Uitleen instructie verifiëren cq. uitbreiden met onderdeel beveiliging.

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

8 Beheer van communicatie- en bedieningsprocessen

8.1 Bedieningsprocedures en verantwoordelijkheden

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Gedocumenteerde bedieningsprocedure**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.1.1

Doelstelling
Het garanderen van een correcte en veilige bediening van IT-voorzieningen.

Toelichting
Er zijn schriftelijke procedures opgesteld voor de bediening van alle computersystemen, waarin instructies zijn opgenomen voor de uitvoering van alle taken, waaronder:

- De juiste behandeling van gegevensbestanden.
- Instructies voor de afhandeling van fouten en andere uitzonderlijke gebeurtenissen die tijdens de uitvoering van de taak kunnen optreden, inclusief beperkingen in het gebruik van systeemhulpmiddelen.
- Contactpersonen in geval van onverwachte bedieningsmoeilijkheden of technische storingen.
- Procedures voor het stoppen, opnieuw opstarten en herstellen van het systeem in geval van systeemstoringen.
- Procedures voor het maken en herstellen van back-ups.
- Procedures bij uitwijk.

Bedieningsprocedures worden als formele documenten behandeld en wijzigingen mogen alleen worden aangebracht na goedkeuring het hoofd Stafgroep Automatisering na overleg met de sr. ICT systeemspecialist en de gegevens(bank)beheerder.

Nog in te voeren maatregelen
- Handleidingen en procedures verifiëren, aanvullen en bundelen.

Documentverwijzing

- Handleidingen en procedures, deze zijn opgenomen in DocSite.
- Handboek ICT beheer – wijzigingsprocedure

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Het beheer van wijzigingen**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.1.2

Doelstelling

Beheersing van wijzigingen om storingen in systemen te voorkomen.

Toelichting

Voor het aanbrengen van wijzigingen geldt de standaard wijzigingsprocedure volgens ITIL. Deze omvat:

- Het vaststellen en noteren van wijzigingsvoorstellen (RFC: request for change)
- Het bepalen van de mogelijke gevolgen van dergelijke wijzigingen (impact-analyse). Onderdeel van deze impactanalyse zijn de beveiligingsaspecten!
- Een goedkeuringsprocedure voor voorgestelde wijzigingen.
- Een gedetailleerde mededeling van de wijzigingen aan alle betrokken personen.
- Procedures en verantwoordelijkheden voor het afbreken en herstellen van niet geslaagde wijzigingen (back-out scenario).

De wijzigingsprocedure is opgenomen in het handboek operationeel beheer. Change management behoort tot het takenpakket van de sr. ICT systeemspecialist.

Nog in te voeren maatregelen

- Handboek operationeel beheer
- Opstellen Change Mangement procedure voor applicaties

Documentverwijzing

- Handboek ICT beheer - wijzigingsprocedure

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Procedures voor het behandelen van incidenten**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.1.3

Doelstelling

Het garanderen van een correcte afhandeling van beveiligingsincidenten. Zie ook paragraaf 6.3.

Toelichting

Beveiligingsincidenten worden via de helpdesk en de standaard incidentbeheer procedure afgehandeld. De volgende specifieke aandachtspunten gelden ten aanzien van beveiliging:

- In de procedures dienen voorziene beveiligingsincidenten te worden opgenomen, zoals:
    - systeemstoringen en niet beschikbaar zijn van diensten
    - fouten die het resultaat zijn van incomplete of onnauwkeurige bedrijfsgegevens
    - inbreuk op de vertrouwelijkheid van gegevens.
    - Virusmeldingen
- Naast de normale noodprocedures (die zijn ontworpen om systemen en diensten zo snel mogelijk te herstellen) dienen deze procedures ook maatregelen te beschrijven met betrekking tot:
    - analyse en identificatie van de oorzaak van het probleem
    - planning en implementatie van maatregelen om herhaling te voorkomen
    - verzamelen van audit trails en gelijksoortig bewijsmateriaal
    - communicatie met zakelijke gebruikers en anderen die getroffen zijn door (of betrokken zijn bij) het incident.
- Audit trails en soortgelijk bewijsmateriaal dienen te worden verzameld en veilig opgeslagen in verband met:
    - interne probleemanalyse
    - gebruik als bewijsmateriaal in geval van mogelijke contractbreuk of bij het overtreden van wettelijke voorschriften
    - onderhandelingen over compensatie van leveranciers van programmatuur en diensten
    - bewijsmateriaal in geval van computermisbruik of overtreding van de Wet Persoonsregistratie.
- De actie die dient te worden ondernomen om beveiligings incidenten en systeem-storingen te corrigeren en te herstellen, dient zorgvuldig en formeel te worden bestuurd.

Nog in te voeren maatregelen

- Aanpassing operationele procedures.

Documentverwijzing

- Handboek ICT beheer (DocSite)

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Functiescheiding**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.1.4

Doelstelling

Functiescheiding vermindert het risico van nalatigheid en opzettelijk misbruik van systemen.

Toelichting

De volgende maatregelen gelden ten aanzien van functiescheiding:

- Wijzigingen dienen via de wijzigingsprocedures te worden afgehandeld. Wijzigingen, zijnde geen standaard RCF's, worden altijd vastgelegd en goedgekeurd door de change manager.
- Nieuw ontwikkelde systemen worden via een formele testprocedure geverifieerd. De test wordt altijd door een derde, zijnde niet de ontwikkelaar, uitgevoerd.
- Systemen moeten zodanig zijn ingericht dat kritische acties worden geregistreerd en controleerbaar zijn door de beveiligingscoördinator.
- Administratieve controle op beveiliging worden uitgevoerd door de beveiligingscoördinator.

De sr. ICT systeemspecialist is verantwoordelijk voor beveiliging op tactisch niveau - beveiligingscoördinator) . De ICT systeemspecialist (3e lijn) is verantwoordelijk voor de uitvoerende taken.

Nog in te voeren maatregelen

- Rol beveiligingscoördinator organisatorisch beleggen.

Documentverwijzing

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Scheiding van voorzieningen voor ontwikkeling en productie**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.1.5

Doelstelling

Het voorkomen van uitval van systemen door ongecontroleerde wijzigingen in productiesystemen en verstoring door fouten in nieuwe systemen.

Toelichting

De volgende maatregelen gelden:

- De programmatuur voor ontwikkeling en de programmatuur voor productie dienen, voor zover mogelijk, door verschillende processors en in verschillende domeinen of directories te worden uitgevoerd.
- De werkzaamheden voor ontwikkelen en voor testen dienen zoveel mogelijk te worden gescheiden.
- Compilers, editors en andere systeemhulpmiddelen dienen, als het niet echt nodig is, niet te worden opgeslagen bij operationele systemen.
- Alvorens nieuwe versies van systemen in productie worden genomen dient een test te worden uitgevoerd in de test/ ontwikkelomgeving.

Op dit moment bezit de provincie een drietal testsystemen (2 HP Unix, 1 Novell server). De gegevens(bank)beheerder ziet er op toe dat er op de productiesystemen in de HP Unix lijn niet wordt getest/ontwikkeld. Slechts na toestemming van de gegevens(bank) beheerder kan een ontwikkeld systeem op de productiesystemen worden overgezet. De sr. ICT systeemspecialist regelt het gebruik van de Novell testserver.

Nog in te voeren maatregelen

- Ontbrekende test en ontwikkelomgeving inrichten inclusief procedures.

Documentverwijzing

- Handboek ICT Beheer

Auteur [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Extern beheer van voorzieningen**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.1.6

Doelstelling
Maatregelen voor beveiliging treffen bij extern beheer van voorzieningen.

Toelichting
Extern beheer van voorzieningen betreft:
- Transfer BV, voor het remote beheer van de Oracle databases.
- Internet aansluiting via GemNet;
- Hosting van website (www.drenthe.nl) bij IAF;
- Helpdesk en beheer van SIS bij Getronics.
- Onderhoudscontracten met leveranciers van hardware en software.

De beveiligingsaspecten die in de contracten opgenomen moeten worden zijn:
- Het leveren van software vrij van virussen en trojan horses;
- De leverancier dient beveiligingsproblemen in de software, systemen of diensten direct bij de provincie te melden inclusief de mogelijk te treffen maatregelen.
- Vertrouwelijk behandelen van informatie omtrent werkwijze en procedures van de Provincie en de informatie op de systemen van de provincie;
- Uitsluitende geautoriseerde en gescreende medewerkers mogen namens de leverancier werkzaamheden verrichten. Een medewerker moet zich kunnen identificeren, anders is de provincie gerechtigd de toegang te ontzeggen.

Verantwoordelijkheid voor de contracten en het opnemen van beveiligingseisen berust bij het hoofd van de Stafgroep Automatisering.

Nog in te voeren maatregelen
- Controle en evt. aanvullen van contracten.

Documentverwijzing
- Contracten met service providers

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

8.2 Systeemplanning en acceptatie

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Capaciteitsplanning**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.2.1

Doelstelling
Het risico van systeemstoringen tot een minimum beperken.
Een goede planning en voorbereiding zijn noodzakelijk om te kunnen garanderen dat de juiste capaciteit en de juiste hulpbronnen beschikbaar zijn.

Toelichting
De capaciteitseisen dienen voortdurend in de gaten te worden gehouden, zodat storingen die een gevolg zijn van een gebrek aan capaciteit kunnen worden voorkomen. Voor informatiesystemen en communicatiesystemen wordt gebruik gemaakt van CiscoWorks en BMC Patrol.

De *gegevens(bank)beheerder* en de *ICT systeemspecialist* gebruiken Monitoringsystemen om potentiële knelpunten te signaleren en te voorkomen, zodat deze geen gevaar opleveren voor de continuïteit en beveiliging van het systeem of voor diensten aan gebruikers. Ook gebruiken zij de systemen om de juiste tegenmaatregelen voor te bereiden en te rapporteren aan de *sr. ICT systeemspecialist*. Voor het preventief beheer van Oracle databases is BMC Patrol als monitoringsysteem aanwezig.

Nog in te voeren maatregelen
De beheerders van systemen en database stellen maandelijks trendrapportages op, waarin het volgende is opgenomen:
- Belasting/ performance van de systemen over de afgelopen 12 maanden;
- Maximaal realiseerbare belasting van de systemen;
- Gesignaleerde knelpunten en mogelijk toekomstige knelpunten op basis van de trends.
- Indien noodzakelijk voorstel voor maatregelen ter voorkoming van knelpunten (RfC).

De rapportages zijn bestemd voor hoofd Stafgroep Automatisering en coördinator wijzigingsbeheer (sr. ICT systeemspecialist).

- BMC Patrol gebruiken voor systeem en netwerkbeheer.

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Acceptatie van systemen**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.2.2

Doelstelling

Het vaststellen van duidelijke acceptatiecriteria voor nieuwe systemen; upgrade en nieuwe versies. De acceptatiecriteria bieden een garantie voor de correcte werking van de systemen; afdoende beveiligingsmaatregelen en aansluiting op de infrastructuur van de provincie.

Toelichting

Voordat nieuwe informatiesystemen kunnen worden geaccepteerd, dienen de acceptatiecriteria te worden vastgesteld en de benodigde tests te worden uitgevoerd. Dit omvat:

- Functionele eisen voor het systeem;
- Beschikbaarheid van procedures voor foutherstel; herstart en continuïteitsplannen;
- Gedocumenteerde bedieningsprocedures;
- Aansluiting op de architectuur en infrastructuur van de provincie;
- Verificatie van standaard beveiligingseisen;
- Beschikbaarheid van documentatie en cursussen voor bediening en gebruik;
- Voor belangrijke nieuwe ontwikkelingen is het van belang dat de operationele functie betrokken wordt bij alle fasen van het ontwikkelingsproces, zodat de operationele efficiëntie van het voorgestelde systeemontwerp gegarandeerd blijft.

Er dienen tests te worden uitgevoerd om te bevestigen dat volledig aan alle acceptatiecriteria is voldaan.

De provincie hanteert een standaard contract voor de levering en onderhoud van informatiesystemen. In dit standaardcontract staan artikelen over oplevering en acceptatie. Via deze weg is gegarandeerd dat dit onderwerp aan de orde komt bij aanschaf en installaties. Het beheer van het standaardcontract ligt bij het hoofd Stafgroep Automatisering.

Nog in te voeren maatregelen

- Vastleggen van acceptatiecriteria van systemen. (voor bestaande is dit zinvol als er nieuwe versies getest moeten worden).
- Vaststellen van algemene beveiligingseisen voor systemen.
- Standaard indeling voor bedieningsprocedures

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord:	Geldig tot: 1 januari 2006

8.3 Bescherming tegen kwaadaardige software

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Maatregelen tegen kwaadaardige software**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.3.1

Doelstelling

Het beschermen van de integriteit van software en informatie door maatregelen te treffen ter voorkoming van de introductie van kwaadaardige software.

Toelichting

Er zijn maatregelen ingevoerd voor preventie en detectie van virussen en adequate procedures om het bewustzijn van de gebruikers te vergroten. Hierbij is het volgende van belang:

- De Provincie Drenthe maakt uitsluitend gebruik van officiële programmatuurlicenties. Het gebruik van niet-geautoriseerde programmatuur is verboden.
- Op de centrale Novell servers wordt gebruik gemaakt van een virusscanner die éénmaal per dag wordt uitgevoerd (Norman Virus Control). Updates worden door systeembeheerders bijgehouden en geïnstalleerd.
- Op de PC's zijn continue virusscanners (NVC) actief. Updates op de virusscanner worden automatisch geïnstalleerd.
- Op de mailservers zijn continue virusscanners en spywarescanners (GWAVA) actief. Updates worden automatisch geïnstalleerd.
- Alle diskettes, m.n. die uit onzekere of ongeautoriseerde bron dienen door bedienend personeel op virussen te worden gecontroleerd voordat zij worden gebruikt. Op de PC's is een virusscanner (NVC) aanwezig die gebruik maakt van de actuele informatie van de centrale virusscanner.
- Alle diskettes die de provincie verstrekt aan derden moeten worden gecontroleerd met de virusscanner.
- Er zijn procedures en verantwoordelijkheden voor het management vastgelegd ten aanzien van het rapporteren en herstellen van virusaanvallen.
- Inkomende en uitgaande E-mail wordt automatisch gecontroleerd op virussen en spyware. Dit gebeurd zowel op de mailserver van GemNet (inkomende mail – alleen virussen) als op de mail server van de provincie (inkomend en uitgaande mail – virussen en spyware).

Nog in te voeren maatregelen

- Gezien het toenemende aantal incidenten m.b.t. tot spyware op de PC's zullen hier maatregelen tegen moeten worden genomen.

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord:	Geldig tot: 1 januari 2006

8.4 Huisregels

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Reservekopieën maken (back-ups)**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.4.1

Doelstelling

Het handhaven van de integriteit en beschikbaarheid van informatieverwerkende en communicatiediensten door middel van back-ups.

Toelichting

De procedures voor het maken van reservekopieën voor de afzonderlijke systemen zijn:

- Dagelijks wordt van alle in gebruik zijnde bestanden en programmatuur een reservekopie gemaakt. Deze worden opgeslagen in een brandvrije kluis.
- De cyclus van de backup-tapes is volgens het GFS-principe.
- Voor de Novell systemen wordt wekelijkse een volledige en dagelijks een differential back-up gemaakt. Deze worden opgeslagen in een brandvrije kluis.
- Wekelijks wordt op maandag de "week-end backup" (full-backup) op een externe lokatie (safe-loket) opgeslagen. Dit wordt door de bode van de provincie uitgevoerd.
- Van bestanden en programmatuur (o.a. bronmateriaal) die gearchiveerd moeten worden, worden twee archieftapes aangemaakt. Eén archieftape wordt extern opgeslagen, de andere wordt bewaard in de datasafe op het Provinciehuis.
- Reservekopieën worden een maal per jaar getest zodat het zeker is dat zij betrouwbaar zijn en in geval van nood kunnen worden gebruikt.
- Eénmaal per jaar worden gedefinieerde databestanden ouder dan 4 jaar verwijderd van de Novell servers. Deze worden tot twee keer toe gearchiveerd op CD-ROM of DVD-ROM. 1 exemplaar (set) wordt extern opgeslagen, de andere wordt bewaard in de datasafe op het Provinciehuis.

Nog in te voeren maatregelen

- Testen van back-up opnemen in het operationeel systeembeheer.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Bijhouden van een logboek**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.4.2

Doelstelling

Werkzaamheden en incidenten dienen in een logboek bijgehouden te worden. Op basis hiervan kunnen controles worden uitgevoerd en correcte werking van procedures geverifieerd worden.

Toelichting

De *ICT systeemspecialisten* dienen een logboek bij te houden van alle werkzaamheden die zij verrichten aan alle centrale systemen en het reageren op incidenten. Hierin dienen de volgende punten te worden opgenomen:

- de tijdstippen waarop het systeem wordt opgestart en afgesloten
- systeemfouten en de maatregelen die daartegen zijn genomen
- een bevestiging dat gegevensbestanden en computer uitvoer op de juiste wijze zijn verwerkt.
- De naam van de persoon die de logboekaantekening heeft gemaakt.

Regelmatig dient door de *sr. ICT systeemspecialist* te worden gecontroleerd of het logboek van een operator wordt bijgehouden volgens de geldende procedures. De logboeken zijn fysiek naast de computers geplaatst en/of opgenomen in Assyst.

Nog in te voeren maatregelen

- Logboeken bijhouden middels Assyst!
- Bijhouden logboeken voor databases bijhouden en opnemen in Assyst

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Storingen opnemen in een logboek**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.4.3

Doelstelling

Het registreren van storingen met als doel de afhandeling te kunnen bewaken en probleemanalyses uit te kunnen voeren.

Toelichting

Alle storingen die door gebruikers worden gemeld, worden bijgehouden in het Helpdesksysteem (Assyst) en in overeenstemming met het Handboek ICT beheer afgehandeld.

Nog in te voeren maatregelen

-

Documentverwijzing

- Handboek ICT Beheer

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

8.5 Netwerkbeheer

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Maatregelen voor netwerken**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.5.1

Doelstelling

Het handhaven van de beveiliging van informatie in netwerken en de bescherming van de ondersteunende infrastructuur.

Toelichting

De volgende maatregelen zijn getroffen voor beveiliging van netwerken en infrastructuur:

- Het lokale netwerk is via een beveiliging (firewall) afgeschermd van externe netwerken. Dit zijn het Internet (via GemNet) en het netwerk van het provinciaal museum.
- Voor Telewerken en remote toegang tot het SIS wordt een VPN gebruikt. Toegang vanuit het VPN tot het interne netwerk is alleen mogelijk via de firewall.
- Beheer op afstand (via modem) is alleen mogelijk na afstemming met de beheerders van de provincie. Na afronding van de werkzaamheden wordt de modemverbinding verbroken (fysiek).
- Het is, voor gebruikers, niet toegestaan programmatuur via Internet; e-mail of andre externe bronnen te downloaden en te installeren op de systemen van de provincie. Systeembeheerders zullen uitsluitend programmatuur downloaden van betrouwbare bronnen en deze testen alvorens te installeren in de productie omgeving.

Nog in te voeren maatregelen

- Het interne netwerk splistsen in een deel voor beheerders en gebruikers. Hiermee kan toegang tot systemen beperkt worden en interne bedreigingen gereduceerd worden.
- Firewall voor Wireless LAN of evenwaardig.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

8.6 *Behandeling en beveiliging van media*

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Management van verwijderbare computermedia**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.6.1

Doelstelling
Het voorkomen van uitlekken van informatie via diverse media.

Toelichting
Er dient toezicht te worden gehouden op verwijderbare computermedia. Hiertoe dienen de volgende maatregelen te worden genomen:

- Indien de inhoud van een medium dat opnieuw gebruikt kan worden niet meer nodig is, dient deze te worden gewist of overschreven voordat het medium het bedrijf verlaat.
- Alle media wordt in een veilige en beveiligde omgeving bewaard die voldoet aan de eisen die door de fabrikant worden gesteld. Hiervoor is een beveiligde kluis beschikbaar.
- Medewerkers dienen media te behandelen conform de classificatie van de informatie op de media. Hierbij geldt dat de classificatie van het medium minimaal gelijk is aan de hoogst geclassificeerde informatie.

Nog in te voeren maatregelen
- Informeren medewerkers.

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Afvoer van media**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.6.2

Doelstelling
Het voorkomen van uitlekken van informatie via afgevoerde media.

Toelichting
Computermedia dienen op een veilige manier te worden afgevoerd wanneer zij niet langer nodig zijn. Hiervoor gelden dezelfde regels als voor de afvoer van apparatuur.

Papieren uitvoer dient volgens de normale weg te worden afgevoerd middels de procedures van de *Facilitaire Groep*. Hierdoor is versnippering gewaarborgd.

Nog in te voeren maatregelen
- Communicatie aan gebruikers

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Procedures voor behandeling van informatie**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.6.3

Doelstelling

Het zorgdragen voor de juiste behandeling van informatie rekening houdend met vertrouwelijkheid.

Toelichting

Er dienen indien het betrokken management dat nodig acht procedures te worden opgesteld voor de behandeling van gevoelige gegevens. In overleg met de *gegevens(bank)beheerder* en de *applicatiebeheerder(s)* kan per informatiesysteem of per register/databestand een 'protocol' worden opgesteld.

Hierbij dient rekening te worden gehouden met de volgende aspecten:

- Voldoen aan uitgangspunten van het informatiebeleid (in principe is informatie openbaar)
- Procedures voor de behandeling van in- en uitvoermedia en het aanbrengen van labels op dit soort media.
- Het bijhouden van een formeel overzicht van personen die geautoriseerd zijn voor de ontvangst van bepaalde gegevens.
- Procedures om te controleren of de in te voeren gegevens compleet zijn.
- Procedures voor de ontvangstbevestiging van verzonden gegevens.
- Het beperken van de verspreiding van gegevens.
- Het aanbrengen van een duidelijke markering op alle kopieën van de gegevens waarmee wordt aangegeven wie toestemming heeft de gegevens te ontvangen.
- Verzendlijsten en lijsten van geautoriseerde ontvangers dienen regelmatig te worden herzien.

(Zie ook de paragrafen 3.2 en 6.7.2.)

Nog in te voeren maatregelen

- Protocol opstellen voor behandeling gevoelige gegevens. Vertrouwenspersoon aanwijzen.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Beveiliging van systeemdocumentatie**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.6.4

Doelstelling

Het voorkomen van illegale toegang tot systeemdocumentatie en daarmee een beveiligingsrisico.

Toelichting

Systeemdocumentatie dient te worden beveiligd tegen ongeautoriseerde toegang. De volgende maatregelen dienen dan te worden getroffen:

- Systeemdocumentatie dient (bij de *applicatiebeheerder* en bij de *Stafgroep Automatisering*) te worden opgeborgen in goed afgesloten kasten. De systeemdocumentatie omvat de werkwijzen en procedures voor bediening van de systemen, zoals beschreven in hoofdstuk 8.
- Op het huisnet en centrale systemen is systeemdocumentatie uitsluitend toegankelijk voor daartoe geautoriseerde medewerkers. Het functioneel beheer hiervoor is belegd bij het hoofd stafgroep automatisering.
- De verzendlijst voor systeemdocumentatie dient zo kort mogelijk te zijn en worden geautoriseerd door de eigenaar van de applicatie of de applicatiebeheerder, in ieder geval ontvangt de sr. ICT systeemspecialist een kopie van de actuele systeemdocumentatie.

Documentatie die door de computer is gegenereerd, mag niet op dezelfde plaats worden opgeborgen als andere toepassingsbestanden en de toegang tot de documentatie dient beveiligd te worden.

Nog in te voeren maatregelen

- Invoeren/ handhaven maatregelen

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

8.7 *Uitwisseling van informatie en software*

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Overeenkomsten over het uitwisselen van informatie en software.**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.7.1

Doelstelling

Voorkomen dat informatie die wordt uitgewisseld tussen organisaties verloren gaat, gewijzigd of misbruikt wordt.

Toelichting

Momenteel gelden de volgende maatregelen:

- E-mail wordt uitsluitend gebruikt voor informele communicatie. Dit dient ook in de e-mail vermeld te worden.
- Overige elektronische gegevensuitwisseling met andere organisaties is momenteel niet aan de orde.

Nog in te voeren maatregelen

- Standaardtekst (disclaimer) informele communicatie opnemen in voettekst bij elke uitgaande e-mail.
- Maatregelen opstellen voor risicokaart zodra derden informatie kunnen aanleveren. Specifieke aandachtspunten betreffen bronvermelding, uitsluiting van (gevolg)schade etc. Per geval zal een specifieke overeenkomst nodig zijn gebaseerd op de uitgangspunten als geformuleerd in het Informatieplan.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Beveiliging van media tijdens transport**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.7.2

Doelstelling

Voorkomen dat informatie die wordt uitgewisseld tussen organisaties verloren gaat, gewijzigd of misbruikt wordt.

Toelichting

Computermedia dienen tijdens transport te worden beveiligd tegen verlies en misbruik. De volgende maatregelen dienen te worden getroffen:

- Maak gebruik van betrouwbare transport- of koeriersdiensten.
- De verpakking dient in overeenstemming te zijn met de specificaties van de fabrikant van de media en dient afdoende bescherming te bieden tegen fysieke schade die tijdens het transport kan optreden.
- Het kan nodig zijn speciale maatregelen te nemen zodat gevoelige informatie niet openbaar kan worden gemaakt of kan worden gewijzigd.

Nog in te voeren maatregelen

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Beveiliging van elektronische handel (e-commerce)**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.7.3

Doelstelling

Voorkomen dat informatie die wordt uitgewisseld tussen organisaties verloren gaat, gewijzigd of misbruikt wordt.

Toelichting

Dit is momenteel niet aan de orde.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

8.8 *Titel voor paragraaf invoeren*

NB: paragraafnummers komen niet overeen met bloknummering, maar omdat het een verwijzing is naar de Code IB, weet ik niet of ik dit zomaar mag veranderen

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Beveiliging van elektronische post (e-mail)**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.7.4.1

Doelstelling

Voorkomen dat informatie die via e-mail wordt uitgewisseld tussen organisaties verloren gaat, gewijzigd of misbruikt wordt.

Toelichting

Maatregelen dienen mogelijk te worden genomen om de zakelijke en beveiligings-risico's, verbonden aan het gebruik van elektronische post, te beperken. Hierbij dient aandacht te worden besteed aan de volgende punten:

- Standaard E-mail verkeer is kwetsbaar voor onbevoegde onderschepping of wijziging. Daarom kan het uitsluitend gebruikt worden voor informele communicatie.
- De gevoeligheid voor fouten (bijvoorbeeld foutieve adressering of verzending) en de algemene betrouwbaarheid en beschikbaarheid van het systeem. Hierdoor kunnen berichten bij verkeerde personen terecht komen of niet aankomen.
- De gevolgen die een andere communicatiemethode kan hebben voor het bedrijf (wat is bijvoorbeeld het effect van een snellere verwerking of van de wijziging van de benadering van bedrijf-naar-bedrijf in een benadering van persoon-naar-persoon).
- Wettelijke voorschriften, zoals de behoefte aan een bewijs van het oorspronkelijke bericht, een verzendbewijs, een bevestiging van aflevering en een ontvangstbewijs.
- De gevolgen voor de beveiliging als directory-gegevens bekend worden gemaakt.
- De behoefte aan beveiligingsmaatregelen in verband met de toegangcontrole voor gebruikers op afstand.

In de handleiding voor gebruikers van e-post (GroupWise en Internet) heeft de provincie een aantal 'good practice' spelregels opgenomen.

Nog in te voeren maatregelen

- 'Good practice' regels verwerken in nieuw op te stellen e-mail reglement.

Documentverwijzing

- Gebruikershandleiding Groupwise en Internet

Auteur [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Beleid ten aanzien van e-mail**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.7.4.2

Doelstelling

Voorkomen dat informatie die wordt uitgewisseld tussen organisaties verloren gaat, gewijzigd of misbruikt wordt.

Toelichting

Ten aanzien van e-mail gelden de volgende maatregelen:

- De provincie gebruikt e-mail uitsluitend voor informele communicatie.
- Het is niet toegestaan vertrouwelijke informatie via e-mail te verzenden.
- Alle e-mail wordt gecontroleerd op virussen en spam. Verdachte e-mail of verdachte bijlagen worden verwijderd.
- De provincie heeft het recht om e-mail te archiveren en in te zien. Dit zal uitsluitend na goedkeuring van de directie plaatsvinden en na mededeling aan betrokkene.
- Medewerkers mogen geen via e-mail verzonden programmatuur op de PC installeren.
- Verdachte e-mails dienen als beveiligingsincident gemeld te worden.

Nog In te voeren maatregelen

- In de toekomst het gebruik van PKI voor encryptie; digitale handtekening.
- Vastleggen in e-mail reglement.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Beveiliging van elektronische kantoorsystemen**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : **8.7.5**

Doelstelling

Voorkomen dat informatie die wordt uitgewisseld tussen organisaties verloren gaat, gewijzigd of misbruikt wordt. Het kan noodzakelijk zijn speciale maatregelen te treffen ter beveiliging van de elektronische uitwisseling van gegevens. Hierbij valt te denken aan een bevestiging (en bewijs) van verzending of aflevering van EDI-gegevens. Daarnaast dienen de aangesloten computersystemen te worden beveiligd tegen alle risico's die een elektronische verbinding met zich mee kan brengen.

Toelichting

Op dit moment is de provincie als beheerder niet ingeschakeld bij het gebruik van EDI, hoewel de salarisadministratie vormen van EDI gebruiken. Hier is het beheer bij een externe organisatie ondergebracht.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Publiek toegankelijke systemen**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : 8.7.6

Doelstelling

Er dient aandacht te worden besteed aan het beschermen van de integriteit van elektronisch gepubliceerde informatie, om ongeoorloofde wijzigingen te voorkomen die de reputatie van de uitgevende organisatie zouden kunnen schaden.
Informatie op een publiek beschikbaar systeem, bijvoorbeeld informatie op een webserver die toegankelijk is via het Internet, moet mogelijk voldoen aan de wetgeving, regels en voorschriften in het betreffende rechtsgebied waar het systeem zich bevindt of waar de handel plaatsvindt. Er dient een formeel autorisatieproces plaats te vinden, voor de informatie publiek beschikbaar wordt. Software, data en andere informatie die een hoog niveau van integriteit vergen en die beschikbaar worden gesteld via een publiek toegankelijk systeem, dienen door middel van geschikte mechanismen, bijvoorbeeld een digitale handtekening (zie **10.3.3**) te worden beschermd.

Toelichting

Publiekelijk toegankelijk systemen zijn www.drenthe.nl en www.drenthe.info. Deze systemen verstrekken data maar bieden geen invoermogelijkheden voor gebruikers. Beveiliging van de sites bestaat uit:

- De webserver van www.drenthe.nl is niet gekoppeld met het netwerk van de provincie.
- De webserver van www.drenthe.info is beveiligd via diverse interne en externe (Gemnet) firewalls en reverse proxy.
- Wijzigingen in de inhoud van de webservers is uitsluitend voor geautoriseerde medewerkers mogelijk.

Nog in te voeren maatregelen

- Striktere beveiliging van www.drenthe.nl c.q. vervangen. Dit betreft het gebruik van Frontpage updates met onbeveiligde wachtwoorden.
- Plaatsing van de systemen in zogenaamde demilitarized zone (DMZ).
-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Beheer van communicatie- en bedieningsprocessen Onderwerp **Andere vormen van informatieuitwisseling**	Verwijzing naar Code IB Hoofdstuknummer : 8 paragraafnummer : **8.7.7**

Doelstelling

Voorkomen dat informatie die wordt uitgewisseld, via onder meer fax, telefoon en videocommunicatie, tussen organisaties verloren gaat, gewijzigd of misbruikt wordt.

Toelichting

Gebruikers krijgen informatie omtrent informatiebeveiliging en gevaren van fax en telefoon. Hiervoor is:

- een folder ontwikkeld;
- wordt in de introductiecursus voor nieuwe medewerkers aandacht besteed aan informatiebeveiliging;
- informatie op het huisnet geplaatst.

Nog in te voeren maatregelen

Informatie aan gebruikers via:

- Folder verspreiden
- Informatie op Huisnet
- Introductiecursus

I.s.m. Facilitaire Groep, zijnde eigenaar van fax- en telefoondiensten.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

9 Toegangsbeveiliging

9.1 Zakelijke eisen ten aanzien van toegangsbeveiliging

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beleid ten aanzien van toegangsbeveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.1.1.1

Doelstelling
Het beheersen van de toegang tot informatie, deze dient te worden beheerst op grond van zakelijke behoeften en beveiligingseisen. Hierbij dient rekening te worden gehouden met het geldende beleid ten aanzien van informatieverspreiding en autorisatie.

Toelichting
De eigenaar van een IT-voorziening (infrastructuur, applicaties) is verantwoordelijk voor de vastlegging van de toegangsprocedures en autorisaties.

Nog in te voeren maatregelen
- Vaststellen van autorisatieschema's door functioneel beheerders. Voor Kantoorautomatisering is dit de afdeling automatisering. Kleinere applicaties waarvoor geen functioneel beheerder is zullen ook door de stafafdeling automatisering worden beheerd.

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Regels voor toegangsbeveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.1.1.2

Doelstelling

Het beheersen van de toegang tot informatie.

Toelichting

Voor het toekennen van toegang tot systemen/applicaties gelden de volgende regels:

- Rechten worden toegekend op basis van rol/functie van een medewerker.
- Functionele beheerders geven aan welke toegangrechten voor specifieke rollen/functionarissen gelden.
- Nieuwe medewerkers krijgen toegangsrechten op basis van een aanvraagformulier ondertekend door de afdelingsmanager.
- Systeembeheerders en helpdesk medewerkers kennen de rechten toe op basis van een ondertekend aanvraagformulier.
- Indien rechten (tijdelijk) gewijzigd moeten worden zal dit ook via een ondertekend aanvraagformulier moeten plaats vinden. Goedkeuring vindt plaats door de eigenaar van het systeem. Het aanbrengen van de autorisaties wordt door de helpdesk uitgevoerd op basis van het ondertekende formulier.
- Veranderingen in functie en bij vertrek van medewerkers geeft de stafafdeling P&O dit door aan de automatiseringsafdeling.

Nog in te voeren maatregelen

- Procedure bekend maken en doorvoeren
- Eigenaren/ functioneel beheerders benoemen

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

9.2 *Management van toegangsrechten*

Hoofdstuk : Toegangsbeveiliging Onderwerp **Registratie van gebruikers**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.2.1

Doelstelling

Het voorkomen van ongeautoriseerde toegang tot informatiesystemen.
Er dienen formele procedures te bestaan voor het beheer van autorisaties voor informatiesystemen en diensten.

Toelichting

Er bestaat een formele procedure (in de vorm van een standaard-formulier dat volledig ingevuld moet worden) voor het registreren en afmelden van gebruikers van de technische infrastructuur en de IT-diensten met meerdere gebruikers.
Dit wordt beheerd aan de hand van de volgende procedures:

- Controleer bij de eigenaar of de gebruiker een machtiging heeft voor de desbetreffende service.
- Verstrek aan de nieuwe gebruiker het document "informatie voor de medewerker", zie bijlage 1.
- Zorg ervoor dat dienstverlenende bedrijven geen toegang verlenen totdat de machtigingsprocedures zijn voltooid.
- Houd een overzicht bij van alle personen die geregistreerd zijn voor het gebruik van de dienst (in Assyst).
- Verwijder onmiddellijk de machtigingen van personen die van functie zijn veranderd of het bedrijf hebben verlaten.
- Check en verwijder periodiek overtollige gebruikers-ID's en machtigingen die niet langer nodig zijn.
- Zorg ervoor dat overtollige gebruikers-ID's niet opnieuw worden toegewezen aan andere gebruikers.

De procedure wordt uitgevoerd door de Frontoffice medewerkers.

Nog in te voeren maatregelen

- Koppeling met personeelsadministratie en T&A-systeem, inclusief tijdelijke medewerkers en inhuur.
- Voor het tijdig en correct muteren van gebruikersgegevens is het nodig dat er een goede (organisatorische) koppeling komt met deze systemen.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beheer van speciale bevoegdheden**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.2.2

Doelstelling
Het voorkomen van ongeautoriseerde toegang tot informatiesystemen en het voorkomen van onnodige uitgifte van speciale bevoegdheden.

Toelichting
Het gebruik van speciale bevoegdheden dient te worden beperkt en beheerd. Het onnodig verlenen en gebruiken van systeembevoegdheden blijkt vaak een belangrijke oorzaak te zijn van de kwetsbaarheid van een systeem.
De toewijzing van bevoegdheden voor systemen voor meerdere gebruikers, die beveiliging vereisen tegen ongeautoriseerde toegang, dient te worden beheerd aan de hand van een formele machtigingsprocedure, bestaande uit de volgende stappen:

- Bepaal de bevoegdheden behorend bij elk systeem (bijvoorbeeld een besturingssysteem of databasesysteem) en de categorieën werknemers aan wie deze bevoegdheden dienen te worden toegewezen.
- Wijs pas bevoegdheden toe aan personen wanneer dit echt nodig is "(need to use") en bekijk de toewijzing van geval tot geval ("event by event") (d.w.z. de minimum behoefte noodzakelijk voor hun functie).
- Hanteer een machtigingsprocedure en houd een overzicht bij van alle toegewezen bevoegdheden. Bevoegdheden dienen niet te worden verleend voordat de machtigingsprocedure is voltooid.
- Bevorder de ontwikkeling en het gebruik van systeem-routines om het verlenen van bevoegdheden aan gebruikers te vermijden.

Applicatiebeheerders en de gegevens(bank)beheerder regelen de autorisatie van gevoelige informatiesystemen. Deze wordt opgenomen in de systeemdocumentatie.

Nog in te voeren maatregelen
- Vaststellen van medewerkers die over speciale bevoegdheden moeten beschikken.

Documentverwijzing
-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beheer van gebruikerswachtwoorden**	Verwijzing naar Code IB Hoofdstuknummer : 9 Paragraafnummer : 9.2.3

Doelstelling

Het voorkomen van ongeautoriseerde toegang tot informatiesystemen.

Toelichting

- Gebruikers zijn verplicht hun persoonlijke wachtwoorden geheim te houden.
- Gebruikers dienen hun eigen wachtwoord te onderhouden. Een nieuwe gebruiker en een gebruiker die zijn wachtwoord is vergeten of waarvan het wachtwoord is verlopen, krijgt een tijdelijk wachtwoord, dat onmiddellijk dient te worden gewijzigd.
- Tijdelijke wachtwoorden worden persoonlijk (dus niet via een derde) en mondeling medegedeeld. Bij het telefonisch uitgeven van een tijdelijk wachtwoord moet de identiteit van de medewerker worden vastgesteld.

Nog in te voeren maatregelen

- Informatie aan gebruikers
- Wijze vaststellen identiteit

Documentverwijzing

-

Auteur [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Verificatie van toegangsrechten**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.2.4

Doelstelling

Het voorkomen van ongeautoriseerde toegang tot informatiesystemen.

Toelichting

Toegangsmachtigingen dienen regelmatig te worden gecontroleerd. Om de toegang tot gegevens en IT-diensten effectief te beheren is de volgende procedure van toepassing:

- Regelmatige controle van gebruikersmachtigingen.
- Frequentere controle van machtigingen met speciale bevoegdheden.
- Regelmatige controle van toegewezen bevoegdheden om het gebruik van niet-geautoriseerde bevoegdheden te voorkomen.

Applicatiebeheerders en de gegevens(bank)beheerder controleren regelmatig de autorisatie van gevoelige informatiesystemen. Mutaties worden gelogd en opgenomen in de systeemdocumentatie. Toegang tot het netwerk wordt regelmatig gecontroleerd door de ICT systeemspecialist.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

9.3 *Verantwoordelijkheid van gebruikers*

Hoofdstuk : Toegangsbeveiliging Onderwerp **Gebruik van wachtwoorden**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.3.1

Doelstelling

Het voorkomen van ongeautoriseerde toegang.
Effectieve beveiliging vereist de medewerking van geautoriseerde gebruikers.
Gebruikers dienen te worden gewezen op hun verantwoordelijkheid voor het handhaven van effectieve toegangsbeveiliging, met name met betrekking tot het gebruik van wachtwoorden en beveiliging van gebruikersapparatuur.

Toelichting

Gebruikers dienen de beveiligingsregels in acht te nemen bij het kiezen en gebruiken van wachtwoorden, overigens worden deze deels afgedwongen door de besturingsystemen.

- Gebruikers kiezen zelf hun wachtwoord, waarvoor ze persoonlijk verantwoordelijk zijn.
- Gebruikers dienen hun wachtwoord geheim te houden.
- Schrijf wachtwoorden niet op papier, tenzij dit veilig kan worden opgeborgen.
- Wijzig een wachtwoord wanneer er aanwijzingen zijn dat het wachtwoord bekend is bij anderen.
- Kies wachtwoorden met een minimale lengte van zes tekens.
- Baseer wachtwoorden niet op:
- maanden van het jaar, dagen van de week of andere verwijzingen naar de datum
- familienamen, huisdiernamen, initialen, automerken of autokentekens
- namen van bedrijven, ID's of verwijzingen
- telefoonnummers (of andere cijfercombinaties)
- gebruikers-ID's, groeps-ID's of andere systeem-ID's
- meer dan twee achtereenvolgende identieke tekens
- reeksen die uitsluitend bestaan uit cijfers of alfabetische tekens
- Lijsten uit puzzelwoordenboeken, indexen van atlassen etc.
- Wachtwoorden dienen om de 60 dagen te worden gewijzigd en het opnieuw gebruiken van oude wachtwoorden is niet toegestaan.
- Wachtwoorden voor machtigingen met speciale bevoegdheden dienen om de 30 dagen te worden gewijzigd en het opnieuw gebruiken van oude wachtwoorden is niet toegestaan.
- Wijzig tijdelijke wachtwoorden meteen na aanmelding.
- Gebruik geen wachtwoorden in automatische aanlogprocedures (bijvoorbeeld opgeslagen in een macro of onder een functietoets).

Indien gebruikers toegang dienen te hebben tot meerdere diensten of platforms en meerdere wachtwoorden dienen te onderhouden, mogen zij één geldig wachtwoord gebruiken voor alle diensten waarvoor de opslag van wachtwoorden niet aan strenge regels is gebonden.
Voor de toegang tot bepaalde informatiesystemen is een separate toegang soms nodig. Dit wordt geregeld door de applicatiebeheerder.

Nog in te voeren maatregelen

- Informatie aan gebruikers

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Onbeheerde gebruikersapparatuur**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.3.2

Doelstelling

Het voorkomen van ongeautoriseerde toegang via onbeheerde systemen zoals PC's in kantoorruimten.

Toelichting

Gebruikers dienen ervoor te zorgen dat onbeheerde apparatuur voldoende is beveiligd en dienen de volgende regels te hanteren:

- Beëindig actieve sessies wanneer u klaar bent (tenzij deze sessies kunnen worden beveiligd met een passende programmatuurvergrendeling).
- Meldt u af bij de mini cq. server wanneer de sessie is beëindigd - schakel de PC of het werkstation niet gewoon uit.
- Indien aanwezig, personal computers met gevoelige (persoonlijke en/of niet openbare informatie, bijvoorbeeld bij personeelszaken, Kabinet der CdK ,,,,) op de lokale harde schijf dienen te worden beveiligd door middel van sloten, wachtwoorden of andere maatregelen wanneer zij niet worden gebruikt.
- Als een PC langer dan 20 minuten niet actief is zal het systeem automatisch vergrendeld worden.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord:	Geldig tot: 1 januari 2006

9.4 Toegangsbeveiliging voor netwerken

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beleid ten aanzien van het gebruik netwerkdiensten**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.1

Doelstelling

De toegang tot interne en externe netwerkdiensten dient te worden beheerst Dit is nodig om ervoor te zorgen dat gebruikers die toegang hebben tot netwerken of netwerkdiensten de veiligheid hiervan niet in gevaar brengen. Deze maatregelen dienen onder andere te bestaan uit:

a) de juiste interfaces tussen het netwerk van de organisatie en netwerken van andere organisaties, of openbare netwerken;
b) de juiste authenticatiemechamismen voor gebruikers en apparatuur;
c) toegangsbeveiliging tot informatiediensten.

Toelichting

De volgende maatregelen zijn getroffen:

- Toegang tot Internet en netwerkdiensten wordt toegekend aan medewerkers op basis van hun functie/ rol. Standaard is uitsluitend toegang mogelijk tot het www en ontvangen en verzenden van e-mail.
- Bijzondere rechten worden toegekend via de daarvoor geldende procedure.
- Het gebruik van speciale netwerkdiensten zoals Telnet, ftp, SNMP en NFS is uitsluitend voor systeembeheerders toegestaan, tenzij er dit via de procedure voor bijzondere rechten anders is geregeld.

Nog in te voeren maatregelen

- LAN beveiliging (splitsing in subnetwerken).

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Verplichte route**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.2

Doelstelling

Bescherming van netwerkdiensten.

Indien nodig dient de route van het werkstation naar de computerservice te worden beheerd. Het doel van een verplichte route is het voorkomen dat gebruikers afwijken van de route tussen het werkstation en de computer-services waarvoor zij zijn gemachtigd. Dit vereist doorgaans de implementatie van een aantal beveiligingsmaatregelen op verschillende punten in de route. Het doel hiervan is het beperken van de routing-opties op elk punt in het netwerk door middel van de volgende keuzen:

- Het toewijzen van vaste lijnen of telefoonnummers.
- Het automatisch verbinden van poorten aan bepaalde toepassingssystemen of beveiligings-gateways.
- Het beperken van het aantal menu- en submenu-opties voor individuele gebruikers.
- Het voorkomen van onbeperkt "ronddwalen" in het netwerk.

De vereisten voor een dergelijk verplicht pad dienen te zijn gebaseerd op het toegangsbeleid van het bedrijf (zie 7.1.1).

Toelichting

Het lokale netwerk kent voorzieningen op verzoek een dergelijke verplichte route te maken. Echter gelet op de wens een zo flexibel mogelijk netwerk aan te bieden wordt een frequente toepassing hiervan ontraden.

Nog in te voeren maatregelen

- Scheiding LAN

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Authenticatie van gebruikers bij externe verbindingen**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.3

Doelstelling

Bescherming van netwerkdiensten bij gebruik van externe verbindingen – dit zijn verbindingen die op afstand tot stand worden gebracht via openbare netwerken.

Toelichting

Externe verbindingen worden gebruikt voor statenleden (SIS) en telewerkers. Toegang wordt verkregen via een VPN verbinding. Hiervoor geldende de volgende richtlijnen:

- Authorisatie wordt verleend via de afdelingsmanager/ functioneel beheerder;
- Het VPN biedt een gecodeerde verbinding tussen de PC op afstand en het netwerk;
- Gebruikers moeten zich identificeren middels een gebruikersnaam en wachtwoord. Hiervoor geldende de standaard regels voor wachtwoorden.
- De remote PC mag niet gelijktijdig verbonden zijn met het VPN en andere externe netwerken.
- Indien de remote PC het VPN opzet via het Internet dan dient gebruik gemaakt te worden van PKI beveiliging.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Node authenticatie**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.4

Doelstelling
Bescherming van netwerkdiensten voor computersystemen op afstand waarvoor de verbinding automatisch tot stand wordt gebracht.

Toelichting
Automatische verbinding tussen externe en interne systemen wordt uitsluitend gebruikt voor de verbinding tussen de "WebCache" server van www.drenthe.info en de achterliggende Oracle database.

Nog in te voeren maatregelen

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beveiliging van diagnosepoorten op afstand**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.5

Doelstelling

Beveiliging tegen ongeautoriseerde toegang via diagnosepoorten.

Toelichting

De procedure voor het gebruik van diagnosepoorten is als volgt:

- Standaard zijn alle poorten uitgeschakeld. Dit betekent dat de verbinding tussen de diagnosepoort en de telefoonlijn is losgekoppeld.
- Uitsluitend op aanvraag wordt een diagnosepoort met de telefoonlijn verbonden. Dit kan alleen na overleg met de sr. ICT systeemspecialist.
- De externe partij dient zich te identificeren op een vooraf afgesproken wijze.
- Na afronding van de werkzaamheden wordt de verbinding weer verbroken.
- Het gebruik van de poort wordt geregistreerd.

Nog in te voeren maatregelen

- Wijze van identificatie van externe partij.

Documentverwijzing

-

Auteur [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Scheiding in netwerken**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.6

Doelstelling

Bescherming van netwerkdiensten door splitsing van het netwerk in logische domeinen.

Toelichting

Het netwerk wordt onderverdeeld in de volgende domeinen:

- Gebruikers LAN, waarin alle gebruikers van systemen zijn opgenomen.
- Beheerders LAN, waarin uitsluitend systeem en applicatiebeheerders zijn opgenomen. Deze beheerders krijgen bijzondere rechten tot de centrale systemen en kunnen onder meer gebruik maken van TelNet; FTP en SNMP.
- Een DMZ voor het draadloze netwerk en telewerken.
- Een scheiding met het netwerk van het Drents Museum.

Nog in te voeren maatregelen

- Aanbrengen van de scheiding in LAN
- Aanbrengen van de scheiding met het LAN van het Drents Museum.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beheer van netwerkverbindingen**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.7

Doelstelling

Bescherming van netwerkdiensten. Mogelijk dienen de verbindingsmogelijkheden voor gebruikers te worden beheerd om de toegangsvereisten voor bepaalde bedrijfstoepassingen te ondersteunen. Dergelijke verbindingsmogelijkheden kunnen worden geïmplementeerd via netwerk-gateways die het netwerkverkeer filteren op basis van vooraf gedefinieerde tabellen of regels.

Toelichting

Toegang tot Internet en van en naar het provinciaal museum worden via een firewall gecontroleerd. Hiervoor gelden de volgende regels:

- www toegang tot Internet is mogelijk voor alle medewerkers;
- Alle medewerkers kunnen e-mail via Internet zenden en ontvangen;
- Toegang van en naar het netwerk van het Drents museum is uitsluitend voor systeem- en applicatiebeheerders van de stafafdeling automatisering mogelijk.

Nog in te voeren maatregelen

- Drents museum via firewall

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beheer van netwerkroutering**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.8

Doelstelling

Bescherming van het netwerk voor gemeenschappelijk gebruik.

Toelichting

Deze maatregel wordt (nog) niet relevant geacht voor de provincie Drenthe.

Nog in te voeren maatregelen

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beveiliging van netwerkdiensten**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.4.9

Doelstelling

Bescherming van netwerkdiensten.

Toelichting

Momenteel worden er geen specifieke netwerkdiensten gebruikt. Er dient per geval een impact-analyse te worden gemaakt van het gebruik van nieuwe netwerk-services. Dit wordt beschouwd als een wijziging in de technische infrastructuur en terzake gelden de normale regels van Change-management. (ITIL)

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

9.5 *Toegangsbeveiliging voor besturingssystemen*

Hoofdstuk : Toegangsbeveiliging Onderwerp **Automatische identificatie van werkstations**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.5.1

Doelstelling

Additionele beveiliging door middel van identificatie van werkstations zodat specifieke activiteiten uitsluitend vanuit daarvoor geautoriseerde systemen kunnen worden uitgevoerd.

Toelichting

Toegangsbeveiliging geschiedt door middel van wachtwoorden er zijn geen beveiligingen op basis van werkstation identificatie.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Aanlogprocedure voor werkstations**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.5.2

Doelstelling

Het voorkomen van ongeautoriseerde toegang tot computers door een beveiligde aanlogprocedure.

Toelichting

Aanloggen op Windows werkstations vindt plaats via de Novell Netware client.In deze aanlog procedure wordt:

- geen toepassingsidentificatie te worden afgebeeld totdat het aanlogproces met succes is voltooid.
- tijdens het aanloggen geen hulpboodschappen gegeven die kunnen worden benut door onbevoegden.
- na drie mislukte aanlogpoging de verbinding verbroken en geen hulp geboden.
- de aanloginformatie pas geverifieerd als alle gegevens zijn ingevuld.
- het aantal mislukte aanlogpogingen voordat actie wordt ondernomen, beperkt tot drie. De te nemen actie bestaat uit:
- het vastleggen van de mislukte poging
- het invoeren van een vertraging voordat nieuwe aanlogpogingen worden toegestaan
- het verbreken van de verbinding.
- de toegestane maximum- en minimumtijd voor het aanloggen beperkt. Indien deze tijd wordt overschreden, wordt het aanlog-proces beëindigd.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Gebruikersidentificatie en authenticatie**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.5.3

Doelstelling
Unieke identificatie van gebruikers en veilige manier van authenticatie van gebruikers. Hiermee zijn activiteiten terug te voeren tot individuele personen.

Toelichting
Gebruikersnamen zijn als volgt opgebouwd: <voornaam><(1^{e}) letter(s) van achternaam>
E-mail adressen zijn als volgt opgebouwd: <voorletter>.<achternaam>

Het gebruik van gemeenschappelijke of groepsaccounts is in principe niet toegestaan. Ontheffing kan uitsluitend verkregen worden via het hoofd stafgroep automatisering / beveiligingscoördinator.

Authenticatie vindt plaats middels wachtwoorden.

Nog in te voeren maatregelen
- Authenticatie door middel van een smartcard (T&A).

Documentverwijzing
-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Wachtwoordmanagement systeem**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.5.4

Doelstelling

Eisen aan wachtwoordmanagement systemen.

Toelichting

Wachtwoordmanagement voor alle Windows werkplekken wordt uitgevoerd door Novell. Voor de UNIX systemen wordt het door het UNIX systeem uitgevoerd. Een aantal applicaties beschikt over eigen wachtwoordbeveiliging. De systemen moeten aan de volgende eisen voldoen:

- Waar nodig dient het gebruik van individuele wachtwoorden te worden afgedwongen om aanspreekbaarheid te handhaven.
- De gebruikers hebben de mogelijkheid hun eigen wachtwoord te kiezen en te wijzigen. Er dient een bevestigingsprocedure te zijn die rekening houdt met typefouten.
- Het systeem dient een minimumlengte van 6 tekens voor wachtwoorden af te dwingen.
- Wachtwoorden dienen om de 60 dagen te worden gewijzigd en het opnieuw gebruiken van oude wachtwoorden is niet toegestaan.
- Tijdelijke wachtwoorden dienen bij de eerste aanlogpoging te worden gewijzigd.
- Het systeem dient zo mogelijk een overzicht bij te houden van eerder gebruikte wachtwoorden.
- Hergebruik dient te worden voorkomen.
- Het systeem dient wachtwoorden niet te tonen op het scherm wanneer deze worden ingevoerd.
- Het systeem dient de wachtwoordbestanden gescheiden te houden van de gegevens in de belangrijkste toepassingen.
- Het systeem dient wachtwoorden in vercijferde vorm op te slaan, waarbij zo mogelijk gebruik dient te worden gemaakt van een onomkeerbaar versleutelings-algoritme.

(Zie 7.3.1 voor informatie over het gebruik van wachtwoorden).

Nog in te voeren maatregelen

- Controleren of alle systemen hieraan voldoen.
- Invoeren van SSO.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Gebruik van systeemhulpmiddelen**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.5.5

Doelstelling

Toegang tot en gebruik van systeemhulpmiddelen dient te worden beperkt tot geautoriseerd personeel. Het is van wezenlijk belang dat het gebruik van dergelijke systeemhulpmiddelen nauwlettend wordt beheerd.

Toelichting

De Windows en UNIX systemen worden zodanig ingericht dat systeemhulpmiddelen niet toegankelijk zijn tenzij hiervoor expliciet autorisatie is verleend. De systeemhulpmiddelen zijn in principe uitsluitend voor systeem- en applicatiebeheerders toegankelijk op basis van gebruikersnaam en wachtwoord beveiliging.

Waar mogelijk dienen de volgende beveiligingsmaatregelen te worden toegepast:

- Wachtwoordbeveiliging voor systeemhulpmiddelen.
- Het scheiden van systeemhulpmiddelen en toepassingsprogrammatuur.
- Het verlenen van ad hoc machtigingen voor systeemhulpmiddelen.
- De beschikbaarheid van systeemhulpmiddelen beperken (bij voorbeeld voor de duur van een geautoriseerde wijziging).

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Stil alarm ter bescherming van gebruikers**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.5.6

Doelstelling

Het stil alarm (om onder dwang verkregen toegang te signaleren) dient te worden overwogen voor gebruikers die het risico lopen het doelwit te worden van dwang.

Toelichting

Is bij de provincie niet in voorzien voor IT-voorzieningen.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp · **Time-out voor werkstations**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.5.7

Doelstelling

Voor inactieve werkstations op locaties met verhoogd risico dient een time-out te worden ingesteld om toegang door onbevoegden te voorkomen.

Toelichting

Wordt toegepast op alle werkstations, met een standaard tijd van 20 minuten.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beperking van de verbindingstijd**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.5.8

Doelstelling

Een beperking van de verbindingstijd biedt aanvullende beveiliging..

Toelichting

In zijn algemeenheid is de verbindingstijd tussen 7.00 uur tot 0.00 uur op werkdagen. Maatwerk is mogelijk via de ICT systeemspecialisten. Dit wordt geregistreerd in Assyst. Overwerk buiten de standaard verbindingstijd dient aangevraagd te worden

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

9.6 *Toegangsbeveiliging voor toepassingen*

Hoofdstuk : Toegangsbeveiliging Onderwerp **Beperking van toegang tot informatie**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.6.1

Doelstelling
Gebruikers van toepassingssystemen, inclusief het onderhoudspersoneel, dienen toegang te krijgen tot informatie en functies overeenkomstig een vastgesteld toegangsbeleid, gebaseerd op de beveiligingseisen voor de afzonderlijke bedrijfstoepassingen en overeenkomstige het toegangsbeleid van de organisatie.

Toelichting
In het algemeen is het kennisnemen van gegevens altijd toegestaan echter dat wil niet zeggen dat ook fysieke toegang tot gegevens altijd mogelijk moet zijn. De volgende beveiligingsmaatregelen moeten worden toegepast ter ondersteuning van het toegangsbeleid:

- Het aanbieden van menu's om de toegang tot functies van het toepassingssysteem te beheren.
- Informatie over gegevens of functies waarvoor gebruikers geen toegangsmachtiging hebben, beperken. (De gebruikersdocumentatie dient op overeenkomstige wijze te worden aangepast.)
- De toegangsmogelijkheden van gebruikers controleren (bijvoorbeeld lezen, schrijven, wissen, ten uitvoerbrengen).
- Zeker stellen dat de uitvoer van toepassingssystemen waarin vertrouwelijke gegevens worden verwerkt, alleen gegevens bevatten die relevant zijn voor het doel van de uitvoer. (Deze uitvoer dient regelmatig te worden gecontroleerd om ervoor te zorgen dat overtollige gegevens worden verwijderd.)

Het is de verantwoordelijkheid van de functioneel beheerder om voor de toepassingen het toegangsbeleid te formuleren alsmede eventuele specifieke eisen waaraan de applicatie moet voldoen. Realisatie van deze eisen is een verantwoordelijkheid voor de applicatiebeheerders c.q. technisch beheerders van de stafafdeling automatisering.

Nog in te voeren maatregelen
- Per toepassing autorisatieregels vaststellen door functioneel beheerder

Documentverwijzing

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Isolatie van gevoelige systemen**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.6.2

Doelstelling

Mogelijk vereisen gevoelige systemen een vast toegewezen (geïsoleerde) computeromgeving.

Toelichting

Voor isolatie van systemen gelden de volgende richtlijnen:

- De gevoeligheid van een toepassingssysteem dient uitdrukkelijk te worden bepaald en gedocumenteerd door de "eigenaar" van de toepassing (zie paragraaf 2.1.3).
- Wanneer een gevoelige toepassing wordt gedraaid in een gemeenschappelijke omgeving, dienen de toepassingssystemen waarmee faciliteiten worden gedeeld, te worden geïdentificeerd en goedgekeurd door de "eigenaar" van de gevoelige toepassing.
- Indien afweging van de eigenaar leidt tot een separaat systeem, niet opgenomen in de gemeenschappelijke infrastructuur, dient daar uitdrukkelijk toestemming voor worden gegeven door de directie.

Er zijn momenteel geen systemen geïdentificeerd als “gevoelig systeem”.

Nog in te voeren maatregelen

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005
Akkoord: Geldig tot: 1 januari 2006

9.7 *Monitoring van toegang tot en gebruik van systemen*

Hoofdstuk : Toegangsbeveiliging Onderwerp **Vastleggen van beveiligingsrelevante activiteiten**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.7.1

Doelstelling

Het ontdekken van ongeautoriseerde activiteiten. Systemen dienen te worden gemonitored om afwijkingen van het toegangsbeleid te detecteren en de te controleren gebeurtenissen te registreren, als bewijs bij beveiligingsincidenten.

Toelichting

Beveiligingsrelevante activiteiten worden door systemen en applicaties vastgelegd in logfiles. Systemen en applicaties dienen de volgende gegevens te registreren:

- Gebruikers-ID;
- Data en tijdstip van de gebeurtenis;
- Identiteit van het werkstation;
- Ondernomen geslaagde acties en geweigerde acties, waaronder pogingen om toegang te krijgen tot het systeem.

De logifles worden gedurende 6 maanden bewaard ter ondersteuning van toekomstige onderzoeken.

Nog in te voeren maatregelen

- Bewaren van logfiles zetten op min. 6 maanden.
- Definieren welke logfiles van alle systemen bewaard moeten worden.

Documentverwijzing

-

Auteur [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Monitoring van systeemgebruik**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.7.2

Doelstelling
Het ontdekken van ongeautoriseerde activiteiten door controle van event logs.

Toelichting
De log files van systemen en applicaties dienen onderzocht te worden op potentiële beveiligingsproblemen. Dit kan uitgevoerd worden door tweede lijn beheerders (Frontoffice en applicatiebeheerders). De volgende rapportages worden opgesteld:
- Trends van de hieronder gedefinieerde risicogebieden;
- Acute beveiligingsproblemen.

Deze worden gerapporteerd aan de beveiligingscoördinator.

De servers aangesloten op Internet worden dagelijks onderzocht. Dit betreft:
- Webcache server;
- Het SIS systeem;
- De telewerkomgeving (Citrix server).

De centrale systemen worden twee maal per week onderzocht. De logfiles van PC's worden uitsluitend onderzocht als er beveiligingsproblemen zijn geïdentificeerd die verder onderzoek op specifieke PC vereisen.

De volgende punten worden onderzocht in de logfiles:
- Mislukte aanlogpogingen.
- Analyseren van aanlogpatronen op aanwijzingen van abnormaal gebruik of hergebruik van oude gebruikers-ID's
- Nadrukkelijk worden geen individuele metingen naar systeemgebruik uitgevoerd die kunnen leiden tot conclusies over persoonlijke efficiency (als toetsaanslagen per minuut).
- Virusmeldingen;
- Starten en stoppen van event log services;

Alle activiteiten verband houdend met deze bewaking zijn opgenomen in de functies *ICT systeemspecialist* en *gegevens(bank)beheerder*.

Nog in te voeren maatregelen
- Uitvoering geven aan de procedure

Documentverwijzing
-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Synchronisatie van systeemklokken**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.7.3

Doelstelling

Een juiste instelling van systeemklokken is van wezenlijk belang om de nauwkeurigheid van logfiles te waarborgen.

Toelichting

Systeemklokken van de servers moeten onderling worden gesynchroniseerd. Hierdoor zijn de gegevens nauwkeurig vast te leggen. Alle servers en overige netwerkcomponenten worden regelmatig handmatig door de *ICT systeemspecialist* gesynchroniseerd met atoomtijd

Nog in te voeren maatregelen

- Invoeren van NTP voor tijd synchronisatie.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Mobiele computers**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.8.1

Doelstelling

Het waarborgen van informatiebeveiliging bij het gebruik van mobiele computers en voorzieningen voor telewerken.

Toelichting

- Mobiele computers zijn voorzien van een stand-alone partitie en een netwerkpartitie voor het gebruik in het netwerk van de provincie.
- Alle mobiele computers worden voorzien van een gebruikersnaam en wachtwoord. Guest accounts en algemene accounts zijn niet toegestaan
- Alle mobiele computers zijn voorzien van een virusbeveiliging.

Nog in te voeren maatregelen

- Mobiele computers, uitgerust met Windows XP of 2000 worden voorzien van disc encryptie op basis van EFS.
- Mobiele computers die toegang hebben tot Internet via dial-up worden voorzien van een persoonlijke firewall en anti-spyware.
- Medewerkers die gebruik maken van mobiele computers ontvangen specifieke instructies omtrent:
    - Het bijwerken van de virusscanner en anti-spyware;
    - Het bijhouden van Windows updates;
    - De personal firewall.

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Toegangsbeveiliging Onderwerp **Telewerken**	Verwijzing naar Code IB Hoofdstuknummer : 9 paragraafnummer : 9.8.2

Doelstelling

Het waarborgen van informatiebeveiliging bij het gebruik van mobiele computers en voorzieningen voor telewerken.

Toelichting

Telewerken wordt door statenleden gebruikt voor toegang tot het SIS en door een aantal medewerkers van de Provincie. Toegang tot het netwerk wordt verkregen via een VPN verbinding. Via deze VPN verbinding wordt een connectie opgebouwd naar een centrale Citrix Server. Op deze server zijn autorisaties voor toepassingen gerealiseerd. Aan telewerken worden de volgende eisen gesteld:

- Gebruikers krijgen een persoonlijke gebruikers ID en wachtwoord. Ten aanzien van wachtwoorden gelden dezelfde procedures als voor interne systemen.
- Remote PC's mogen niet gelijktijdig een verbinding met Internet en het VPN onderhouden.
- Indien de remote PC het VPN opzet via het Internet dan dient gebruik gemaakt te worden van PKI beveiliging.
- Gebruikers van telewerk voorzieningen krijgen instructies omtrent beveiligingsmaatregelen.

Nog in te voeren maatregelen

- Remote PC's mogen niet gelijktijdig een verbinding met Internet en het VPN onderhouden.
- Gebruikers van telewerk voorzieningen krijgen instructies omtrent beveiligingsmaatregelen.

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord:	Geldig tot: 1 januari 2006

10 Ontwikkeling en onderhoud van systemen

10.1 Beveiligingseisen voor systemen

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Analyse en specificatie van beveiligingseisen**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.1.1

Doelstelling

Een analyse van beveiligingseisen dient te worden uitgevoerd tijdens het specificeren van de systeemeisen voor elk informatiesysteem. Dit geldt voor zowel nieuw te ontwikkelen systemen als voor de aanschaf van standaardsystemen. Bij nieuw te ontwikkelen systemen moeten geautomatiseerde beveiliging en handmatige/organisatorische maatregelen worden ontworpen, gedocumenteerd en geïmplementeerd. Dezelfde overwegingen gelden voor het beoordelen van de systeemspecificaties van een standaard-pakket bij pakketselectie. De analyse richt zich op twee richtlijnen:

- Het bepalen van de mate waarin vertrouwelijkheid, integriteit en beschikbaarheid van informatie(-voorzieningen) gewaarborgd dient te worden.
- Het bepalen van de beveiligingsmaatregelen die genomen moeten worden om storingen of incidenten te voorkomen, op te sporen en te herstellen.

Toelichting

Afhankelijk van het soort systeem dient aandacht te worden besteed aan:

a) Autorisatiebeheer, dat wil zeggen het beheren van de toegang tot informatie en diensten, inclusief eventuele vereisten voor scheiding van functies of taken (zie 6.1.3., 6.1.4. en Hfd 7).
b) Audit trails, dat wil zeggen het loggen van belangrijke gebeurtenissen voor het uitvoeren van routinecontroles of specifieke onderzoeken, inclusief bewijsvoering in contractuele of andere onderhandelingen (zie ook 8.7.1).
c) Integriteit, dat wil zeggen het controleren en beschermen van de correctheid en volledigheid van vitale gegevens in alle (of bepaalde) stadia van verwerking (zie 10.2.2. en 10.2.4).
d) Vertrouwelijkheid, dat wil zeggen het beschermen van gegevens tegen ongeautoriseerde toegang, inclusief het mogelijke gebruik van gegevens-encryptie in speciale omstandigheden (zie 10.2.3).
e) Voldoen aan regulerende, wettelijke of contractuele vereisten, inclusief het produceren van speciale rapporten om tegemoet te komen aan bepaalde wettelijke eisen (zie 12.1.1).
f) Continuïteit door regelmatig reservekopieën te maken van belangrijke bedrijfsgegevens en deze te controleren op betrouwbaarheid (zie 8.4.1).
g) Continuïteit door het herstellen van storingen, met name voor systemen die altijd beschikbaar dienen te zijn. Uitwijkvoorzieningen worden gedefinieerd tijdens het specificeren van de systeemeisen. (zie 11).
h) Integriteit door het systeem te beveiligen tegen ongeautoriseerde wijzigingen (zie 6.3.1, 10.4.1 en Hoofdstuk 7).
i) Gebruikersvriendelijkheid door het systeem geschikt te maken voor gebruik door niet-gespecialiseerde (maar wel daarvoor opgeleide) gebruikers (zie 4.2).
j) Controleerbaarheid door (waar passend) ervoor te zorgen dat het systeem voldoet aan de eisen van externe auditors (bijvoorbeeld door het gebruik van voorzieningen zoals ingebouwde programmaroutines voor steekproeven en onafhankelijke programmatuur voor het controleren

van kritieke berekeningen).
k) Continuïteit door het uitvoeren van versiebeheer.
l) Continuïteit door het bijhouden van documentatie van systeemwijzigingen.

In het Handboek Systeemontwikkeling van de provincie Drenthe staan aanbevelingen hoe om te gaan met alle aspecten van informatiesystemen, echter op het terrein van de informatiebeveiliging is dit vrij beperkt uitgewerkt. Bovenstaande is dan ook een aanvulling op het handboek die bij vaststelling van dit Plan in werking treedt.

Bij het ontwikkelen van nieuwe systemen of wijzigingen van bestaande systemen wordt de integriteit van gegevens zoveel mogelijk door het database (RDBMS-)pakket ondervangen. Basis is en blijft een kwalitatief goed functioneel model.

In dat model worden zaken als autorisatie, geldigheid van gegevens en relaties tussen gegevens geregeld. Deze worden via een technisch ontwerp vertaald in:
- een datamodel (de modelmatige opzet van de database),
- database roles (toegekende rechten aan groepen gebruikers),
- constraints (vooraf gedefinieerde beperkingen op waarden),
- procedures (volgtijdelijk afgewerkte regels) en
- triggers (gebeurtenissen die een controlemechanisme in werking zetten) .

Bij de selectieprocedure voor de aanschaf van standaard systemen gelden, voor zover van toepassing en beschikbaar, dezelfde overwegingen.

Nog in te voeren maatregelen

- Opstellen checklist met aandachtspunten bij het ontwikkelen of aanschaffen van een nieuwe informatiesysteem.

Documentverwijzing

- Handboek Systeemontwikkeling

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

10.2 Beveiliging in toepassingssystemen

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Validatie van invoergegevens**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.2.1

Doelstelling

Bij het invoeren van gegevens in informatiesystemen dienen deze gegevens te worden gevalideerd op juistheid en volledigheid.

Toelichting

Validatie van invoergegevens dient door de applicaties uitgevoerd te worden. Er dienen controles te worden uitgevoerd op de invoer van zakelijke transacties, vaste gegevens (namen en adressen, referentienummers van klanten) en parametertabellen (valutawisselkoers, belastingtarieven). Bij ontwerp en selectie van systemen worden deze eisen opgenomen. Hiervoor gelden de volgende eisen:

a) Invoercontroles op:
- het bereik waarin waarden mogen liggen
- ongeldige tekens in invoervelden
- ontbreken of onvolledige gegevens
- over- of onderschrijding vande hoeveelheid gegevens
- controle op integriteit en geldigheid (foreign key relatie's)
- de inhoud van sleutelvelden
- ongeautoriseerde of inconsistente sturingsgegevens

b) Periodieke controle van de inhoud van sleutelvelden of gegevensbestanden op geldigheid en integriteit.
c) Controle van papieren invoerdocumenten op ongeautoriseerde wijzigingen in invoergegevens (voor alle wijzigingen in invoerdocumenten is toestemming vereist).
d) Procedures voor het corrigeren van fouten bij geldigheidscontrole.
e) Procedure voor het testen van de plausibiliteit van invoergegevens.
f) Het definiëren van de verantwoordelijkheden van alle medewerkers die betrokken zijn bij het invoeren van gegevens.

In het Handboek Administratieve Organisatie van de Provincie Drenthe staan procedures beschreven met betrekking tot autorisatie, controles en het corrigeren van fouten.

Nog in te voeren maatregelen

- Het gezamenlijk met de applicatiebeheerder opstellen van een checklist voor invoercontroles.

Documentverwijzing

- Handboek Administratieve Organisatie

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Validatie van interne gegevensverwerking**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.2.2.

Doelstelling

Toepassingen dienen interne gegevensverwerking te valideren en foutieve verwerkingen te voorkomen. Geïdentificeerde risicogebieden zijn:
- Wijzigen van gegevens via toevoegen en verwijderen.
- Programma's die in bepaalde volgorde gedraaid moeten worden.
- Toevoegen en verwijderen functies in programma's.

Toelichting

Voor applicaties zullen deze eisen expliciet worden opgenomen en in de systeemselectie of ontwerp worden opgenomen. Welke maatregelen nodig zijn, hangt af van de aard van de toepassing en de impact die verminking van gegevens heeft op de organisatie.
Afhankelijk van de applicaties zijn de volgende controles denkbaar:
- Sessie- of batchcontroles, om bestandstotalen na transactie-updates met elkaar te vergelijken.
- Balanscontroles (verbandscontroles).
- Geldigheidscontroles op door het systeem gegenereerde gegevens (zie 10.2.1).
- Integriteitscontroles (distributie gegevens tussen centrale en decentrale computers).
- Controletotalen van records en bestanden.
- Logging om juistheid en tijdstippen van draaien van toepassingsprogramma's te verifieren.
- Logging om volgordelijkheid en afhandeling van fouten te controleren.

Nog in te voeren maatregelen

- Opstellen checklist voor invoercontroles bij aanschaf of ontwikkeling van nieuwe systemen.

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Authenticatie van berichten**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.2.3

Doelstelling

Authenticatie van berichten wordt gebruikt om niet geautoriseerde wijzigingen of verminking van inhoud van berichten te voorkomen en op te sporen.

Toelichting

Dit is momenteel niet van toepassing binnen de Provincie.

Nog in te voeren maatregelen

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Validatie van uitvoergegevens**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.2.4

Doelstelling

Validatie van uitvoergegevens van toepassingssystemen om zeker te stellen dat de verwerking van opgeslagen gegevens op de juiste manier plaats vindt.

Toelichting

De volgende maatregelen zijn van kracht:

- Aan de toepassingen worden functionele eisen gesteld ten aanzien van de gegevensverwerking en uitvoer (validatie en verificatie van gegevens).
- Bij test en acceptatie worden deze eisen gevalideerd.
- Functioneel applicatiebeheerders kunnen specifieke controles invoeren, waaronder:
    - Plausibiliteit controle om te testen of de uitvoergegevens aanvaardbaar zijn.
    - Controletellingen
    - Aanvullende informatie verstrekken om de juistheid van de uitvoer te bepalen.
    - Verantwoordelijkheden van medewerkers vaststellen die bij het proces zijn betrokken.

Nog in te voeren maatregelen

Functioneel applicatiebeheerders toewijzen (voorzover dit nog niet gerealiseerd is) en informeren.

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

10.3 Cryptografische beveiliging

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Beleid cryptografische beveiliging**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.3.1

Doelstelling

Cryptografische beveiliging biedt mogelijkheden om integriteit; authenticiteit en vertrouwelijkheid van gegevens te waarborgen.

Toelichting

Vooralsnog worden er binnen de provincie geen specifieke cryptografische beveiligingen toegepast met uitzondering van:

- Wachtwoorden in systemen en applicaties. Deze worden gecodeerd opgeslagen waarbij gebruik wordt gemaakt van de standaard systeemfuncties.
- Deels wordt voor telewerken al gebruik gemaakt van een VPN zodat alle netwerkverkeer gecodeerd is.

Nog in te voeren maatregelen

- Invoering van PKI voor de volgende toepassingen:
  - Authenticatie van medewerkers;
  - Beveiliging van e-mail (encryptie van berichten en digitale handtekening);
- Telewerken met gebruikmaking van VPN voor alle medewerkers die voor telewerken in aanmerking komen.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Versleuteling (Encryptie)**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.3.2

Doelstelling

Versleuteling van berichten om vertrouwelijkheid van berichten en gegevens te kunnen waarborgen.

Toelichting

Encryptie is van toepassing bij:

- Opslag van wachtwoorden, hiervoor worden de standaard systeemfuncties gebruikt. Toegangsbeveiliging met behulp van beheerde gebruikersrechten (bv beperkte leesrechten) wordt een afdoende en werkbaar alternatief geacht.
- Deels wordt voor telewerken al gebruik gemaakt van een VPN zodat alle netwerkverkeer gecodeerd is.

Nog in te voeren maatregelen

- EFS – Encrypted File System - voor bestanden op portable computers, voorzover ze zijn uitgerust met Windows 2000 en XP, waarbij de gebruiker toeziet op verantwoord gebruik.
- Telewerken met gebruikmaking van VPN voor alle medewerkers die voor telewerken in aanmerking komen.

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Digitale handtekening**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.3.3

Doelstelling

Het gebruik van digitale handtekening om authenticiteit en integriteit van digitale berichten en documenten te kunnen waarborgen.

Toelichting

Niet van toepassing.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Onweerlegbaarheid**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.3.4

Doelstelling

Het aantonen dat een activiteit door een gebruiker is uitgevoerd c.q. een specifiek bericht op document afkomstig is van een gebruiker.

Toelichting

Er zijn op dit moment geen activiteiten geïdentificeerd waarvoor specifieke eisen aan onweerlegbaarheid worden gesteld buiten de standaard voorziening, waarbij gebruikers met behulp van gebruikersnaam en wachtwoord worden geïdentificeerd.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Sleutelbeheer**	Verwijzing naar Code IB Hoofdstuknummer : 10 Paragraafnummer : 10.3.5

Doelstelling

Het beheer van sleutels ten behoeve van cryptografische beveiliging.

Toelichting

Dit is niet van toepassing

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

10.4 Beveiliging van systeembestanden

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Beheersing van operationele software**	Verwijzing naar Code IB Hoofdstuknummer : 10 Paragraafnummer : 10.4.1

Doelstelling

De Code vereist strenge controle op de implementatie van programmatuur op operationele systemen. Dit om de integriteit van de applicaties te waarborgen.

Toelichting

De ICT systeemspecialisten (voor de RDBMS applicaties de gegevens(bank)beheerders) zijn verantwoordelijk voor de beveiliging van systeembestanden. De taak vindt plaats in overleg met de betreffende applicatiebeheerder.

Programmatuur wordt gestructureerd opgeslagen in een afgesproken bestandsboom.

Voor de RDBMS applicaties geldt dat in deze boomstructuur maximaal vijf versies van de applicatie bewaard worden. Controle van aanpassingen (RFC's: request for change) op bestaande programmatuur vindt eerst plaats op een testomgeving. Als het testen succesvol is verlopen wordt de originele productie versie overschreven met de nieuwe versie. De nieuwe versie (bij ontwikkeling de broncode) wordt onder een aparte directory opgeslagen. De applicatiebeheerder is verantwoordelijk voor de acceptatie van het testresultaat en voor de opname van de RFC's in de systeemdocumentatie hetzij een daaraan toegevoegd logboek.

De structuur van opslag is voor de Oracle applicaties als volgt:
Runtime (binair):
F:\APPLIC\ORACLE\<applicatienaam>\Productie
Bron(source) of runtime(binair) bij standaard software:
F:\APPLIC\ORACLE\<applicatienaam>\VERSIEx.x

De opslagstructuur van de Oracle applicaties op de Unix systemen wijkt af van de bovenstaande opslagstructuur. Hierbij wordt uitgegaan van de zogenaamde OFA standaard (Optimal Flexible Architecture). Deze OFA standaard wordt wereldwijd gevoerd en is ingevoerd in de Oracle configuratie tools en documentatie.

Voor de overige applicaties geldt dat bij nieuwe installaties eerst de oude situatie veilig gesteld wordt en vervolgens de nieuwe installatie in de productieomgeving plaatsvindt. Als het testen succesvol is verlopen wordt de originele versie van het systeem verwijderd (het betreft hier veelal standaard software, waarvan de verschillende versies probleemloos over elkaar heen geïnstalleerd kunnen worden).

De structuur van opslag is voor de overige applicaties als volgt:
Software:
F:\APPLIC\ <applicatienaam>
Bijbehorende data
F:\DATA\ <applicatienaam>

Voor applicaties die door de gehele organisatie gebruikt worden (groepsoverschrijdend) geldt de volgende opslagstructuur:
Software:
S:\APPLIC\ <applicatienaam>

Bijbehorende data
S:\DATA\ <applicatienaam>

Nog in te voeren maatregelen

- Informeren gegevens(bank)beheerders en doorvoeren opslagstructuur Oracle applicaties.
- Documenteren standaard opslagstructuur Oracle applicaties op de Unix systemen.
- Informeren ICT-specialisten en doorvoeren van de opslagstructuur overige applicaties.
- Informeren applicatiebeheerders (systeemdocumentatie en logboek).

Documentverwijzing

- Handboek voor systeemontwikkeling
- The OFA Standard

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Beveiliging van testgegevens**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.4.2

Doelstelling

Testgegevens bevatten om een reële test te kunnen uitvoeren doorgaans grote hoeveelheden uit productiebestanden overgenomen data. Daarom moeten ook testgegevens worden beveiligd en beheerd.

Toelichting

In principe moeten testgevens worden beveiligd en beheerd als ware het productiegegevens (wat veelal ook het geval is). De volgende maatregelen dienen te worden genomen ter beveiliging van productiegegevens wanneer deze worden gebruikt bij het testen:

- De procedures voor toegangsbeveiliging die worden gebruikt voor operationele toepassingssystemen dienen ook te worden gebruikt bij het testen (autorisatiebeheer).
- Telkens wanneer operationele gegevens worden gekopieerd naar een testsysteem dient dit te worden vastgelegd in de bijbehorende RFC (request for change) en opgenomen in Assyst en/of het applicatielogboek.

Nog in te voeren maatregelen

- Informeren gegevens(bank)beheerders

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Toegangsbeveiliging voor softwarebibliotheken**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.4.3

Doelstelling

Om het risico van verminking van computerprogramma's te minimaliseren is strikt toezicht op toegang tot softwarebibliotheken vereist (zie ook 8.3).

Toelichting

Software bibliotheken zijn uitsluitend toegankelijk voor ontwikkelaars en applicatiebeheerders. Hiervoor wordt het standaard autorisatiemechanisme van de systemen gebruikt.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

10.5 Beveiliging bij ontwikkel – en ondersteuningsactiviteiten

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Procedures voor het beheer van wijzigingen**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.5.1

Doelstelling

Formele beheersing van wijzigingen zijn noodzakelijk om de kans van verminking van informatiesystemen te minimaliseren.

Toelichting

Nadat een applicatie is opgeleverd is de applicatiebeheerder de verantwoordelijke voor het goed functioneren van het systeem. Vanuit de gebruikersorganisatie kan een functioneel beheerder (vaak tevens de applicatiebeheerder) wijzigingsvoorstellen formuleren (RFC: Request for Change) op operationele applicaties. De applicatiebeheerder of diens manager kan een RFC indienen bij het hoofd Stafgroep Automatisering.

Op basis van een impactanalyse wordt een RFC (in overleg met de betrokken deskundigen) ofwel direct doorgevoerd ofwel een offerte opgesteld. Rekening wordt gehouden met een eventueel bestaande onderhoudsovereenkomst.

Documentatie van wijzigingen worden in de vorm van supplementen toegevoegd aan de bestaande systeemdocumentatie en als RFC opgeslagen in Assyst.

De procedures met betrekking tot het Change Management zijn uitputtend beschreven op de DOC-site. Dit is een webapplicatie waarin alle procedures opgenomen zijn die betrekking hebben op beheer (Indicent Management, Problem Management en Change Management).

Nog in te voeren maatregelen

- Professionalisering werkwijze Change Management.

Documentverwijzing

- DOC-site

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Technische controle op wijzigingen in het besturingssysteem**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.5.2

Doelstelling

Bij wijzigingen (nieuwe versies en patches) in het besturingssysteem dient opnieuw te worden beoordeeld of het systeem inclusief de toepassingen voldoet aan de functionele en beveiligingseisen.

Toelichting

De Change Manager bepaalt op welk moment nieuwe versies van besturingssystemen dan wel kleine aanpassingen beschikbaar worden gesteld. In dit kader is het van belang te weten op welke wijze de wijzigingen impact hebben op de beveiliging- en autorisatieprocedures in de verschillende applicaties.

Wijzigingen dienen door de Change Manager tijdig te worden aangekondigd en worden besproken met alle betrokkenen als de applicatiebeheerders, de gegevens(bank)beheerders, ontwikkelaars en eventueel leveranciers van standaardapplicaties.

De procedures met betrekking tot het Change Management zijn uitputtend beschreven op de DOC-site. Dit is een webapplicatie waarin alle procedures opgenomen zijn die betrekking hebben op beheer (Indicent Management, Problem Management en Change Management).

Nog in te voeren maatregelen

- Patch beleid, met name voor extern toegankelijke systemen.
- Beveiligingsupdates, die betrekking hebben op gebruikte faciliteiten van het systeem, dienen zo snel mogelijk te worden uitgevoerd.

Documentverwijzing

- DOC-site

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Restricties op wijzigingen in softwarepakketten**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.5.3

Doelstelling

Het voorkomen van beveiligingsrisico's en beheerproblemen bij aanbrengen van wijzigingen in standaard software pakketten.

Toelichting

Wijzigingen op programmatuur van derden vinden per definitie niet plaats. De organisatie heeft geen beschikking over de broncode van aangekochte programmatuur. Indien op basis van een escrow overeenkomst (zie paragraaf 3.1.1) dit wel het geval blijkt dan gelden dezelfde procedures als bij paragraaf 8.4.1.

Uitzondering op bovenstaande regel vindt plaats indien maatwerk noodzakelijk geacht wordt voor de functionaliteit van de applicatie. Indien mogelijk wordt de leverancier van de software gevraagd de gewenste aanpassingen uit te voeren en op te nemen in de standaard software. Wanneer dit niet mogelijk is wordt het maatwerk uitgevoerd volgens dezelfde procedure als beschreven onder 10.5.1 voor het beheer van wijzigingen. Daarnaast zijn afspraken vastgelegd met betrekking tot:

- De opslagstructuur van het maatwerk.
- Procedures voor het maatwerk bij de uitvoering van updates (veiligstellen, eventueel aanpassen en testen van het maatwerk).
- Documentatie en het bijhouden van het applicatielogboek

Nog in te voeren maatregelen

- Informeren ICT-specialisten en gegeven(bank)beheerders
- Invoeren applicatielogboek

Documentverwijzing

- Handboek Systeemontwikkeling
- DOC-site

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Geheime communicatiekanalen en Trojaanse paarden**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.5.4

Doelstelling

Het voorkomen dat via geheime communicatiekanalen informatie wordt verspreid en/ of illegaal toegang tot systemen en data wordt verkregen.

Toelichting

De volgende voorzieningen zijn getroffen:

- Op alle PC's zijn viruscontroles actief die ook Trojaanse paarden kunnen detecteren;
- Verbindingen van interne PC's naar externe systemen worden beperkt tot e-mail en www verkeer zodat geheime communicatiekanalen geblokkeerd worden, tenzij ze gebaseerd zijn op de www poorten.
- Bij ontwikkeling van software (zie paragraaf 10.5.5)
- Van leveranciers wordt geëist dat maatwerk software en standaard software vrij van virussen en Trojaanse paarden worden geleverd.
- Communicatiekanalen voor onderhoud op afstand van systemen moeten bekend zijn bij de Provincie en door de Provincie geactiveerd en gedeactiveerd kunnen worden.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Ontwikkeling en onderhoud van systemen Onderwerp **Uitbestede ontwikkeling van software**	Verwijzing naar Code IB Hoofdstuknummer : 10 paragraafnummer : 10.5.5

Doelstelling

Waarborgen dat maatwerksystemen voldoen aan de kwaliteitseisen en de beveiligingseisen van de Provincie.

Toelichting

Ten aanzien van de kwaliteitseisen gelden bij uitbesteding van software ontwikkeling de volgende maatregelen:

- In de specificatie worden expliciet eisen ten aanzien van kwaliteit en functionaliteit opgenomen.
- De ontwikkelaar dient garanties af te geven ten aanzien:
    - De kwaliteit en nauwkeurigheid van het uitgevoerde werk.
    - De uitvoering van de afgesproken functionaliteit.
    - Zorgen voor zekerheidstelling in geval de externe partij in gebreke blijft (escrow).

Ten aanzien van de beveiligingseisen gelden bij uitbesteding van software ontwikkeling de volgende maatregelen:

- In de specificatie worden expliciet eisen ten aanzien van beveiliging opgenomen.
- De ontwikkelaar dient garanties af te geven ten aanzien:
    - Juiste omgang met intellectuele eigendom.
    - Licenties van gebruikte standaard componenten.
    - Niet voorkomen van virussen en Trojaanse paarden.
- De ontwikkelaar moet het gebruik van toegangspoorten voor onderhoud op afstand aangeven en functionaliteit bieden om deze door de provincie aan- of uit te schakelen.

Nog in te voeren maatregelen

- Opstellen checklist kwaliteitseisen.
- Opstellen checklist beveiligingseisen.

Documentverwijzing

- Handboek Systeemontwikkeling

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

11 Continuïteitsmanagement

Hoofdstuk : Continuïteitsmanagement Onderwerp **Uitbestede ontwikkeling van software**	Verwijzing naar Code IB Hoofdstuknummer : 11 paragraafnummer :

Doelstelling

Dit hoofdstuk bevat maatregelen voor uitwijk

Toelichting

Momenteel wordt een definitiestudie opgesteld met de titel 'Calamiteitenplan Provincie Drenthe'. Hierin wordt de huidige situatie beschreven en worden aanbevelingen gedaan om de maatregelen met betrekking tot uitwijk goed gestalte te geven. De volgende stap is de uitvoering van deze maatregelen.

Nog in te voeren maatregelen

- Uitvoeren van de punten genoemd in de definitiestudie Dit maakt deel uit van het project Informatie Beveiliging met als opdrachtgever de Stuurgroep Informatievoorziening.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

12 Naleving

12.1 Naleving van wettelijke voorschriften

Hoofdstuk : Naleving Onderwerp **Specificatie van de van toepassing zijnde wetgeving**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.1.1

Doelstelling

Het voorkomen van schending van strafrechtelijke of civielrechtelijke wetgeving, wettelijke, reglementaire of contractuele verplichtingen of beveiligingseisen.

Toelichting

Het ontwerp, de bediening en het gebruik van IT-voorzieningen dient te voldoen aan alle relevante beveiligingseisen die wettelijk of contractueel zijn vastgelegd. De wetgeving die van kracht is voor de informatiesystemen van de provincie zijn:

- Intellectueel eigendomsrecht
- Auteursrecht
- Bescherming van persoonsgegevens
- Archiefwet
- Wet computercriminaliteit (als verwerkt in de Wetboeken van Strafrecht en Strafvordering)
- Wet telecommunicatievoorzieningen
- Burgerlijk wetboek

Nog in te voeren maatregelen

- Inventariseren of er binnen de provincie systemen gebruikt worden waarvoor speciale wetgeving geldt en dit expliciet vast te leggen.

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Naleving Onderwerp **Intellectuele eigendomsrechten**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.1.2

Doelstelling

Het waarborgen van wettelijke beperkingen met betrekking tot het gebruik van materiaal waarop intellectuele eigendomsrechten rusten, zoals auteursrecht, octrooirechten of handelsmerken. De overheid heeft een voorbeeldfunctie bij het bestrijden van inbreuken op auteursrechten op software.

Toelichting

Software wordt doorgaans geleverd op basis van een licentieovereenkomst die het gebruik van de producten beperkt tot bepaalde systemen, het aantal gebruikers en meestal ook het kopiëren van de programmatuur beperkt tot het maken van reservekopieën voor gebruik bij calamiteiten. Ten aanzien van intellectuele eigendomsrechten gelden de volgende procedures:

- Software mag uitsluitende geïnstalleerd worden als daarvoor de benodigde licenties beschikbaar zijn.
- De stafafdeling automatisering houdt een administratie bij van de beschikbare en gebruikte software licenties.
- Waarborgen dat uitsluitend geautoriseerde software en producten met licenties zijn geïnstalleerd (regelmatig uitvoeren van audits op de programmatuur en het scannen naar auteursrechtelijke software binnen de persoonlijke directories van medewerkers is hierbij toegestaan).

Nog in te voeren maatregelen

- Procedure voor de uitvoering van audits.

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Naleving Onderwerp **Beveiliging van bedrijfsdocumenten**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.1.3

Doelstelling

Bescherming van bedrijfsdocumenten tegen verlies, diefstal, vernietiging en vervalsing.

Toelichting

Bedrijfsdocumenten worden beheerd volgens wettelijk voorschift (archiefwet). De documenten worden geclassificeerd en voorzien van een label zoals is omschreven in hoofdstuk 5. Daarnaast gelden de volgende maatregelen:

- Vertrouwelijke informatie dient in afgesloten kasten te worden bewaard na werktijd en bij het verlaten van de werkruimte
- Belangrijke systeeminformatie (systeemtoegang) dient centraal in een afgesloten ruimte bewaard te worden.
- Applicatiebeheerders beheren systeemdocumentatie van de diverse informatiesystemen. Deze documentatie bestaat uit:
  - Documentatie inzake de logische werking
  - Documentatie inzake de technische werking
  - Contracten e.d. met de leverancier(s) van de applicatie (archief)
  - Kwaliteitsgegevens over het systeem (meta-informatie)
- Bij het gebruik van elektronische opslagmedia worden maatregelen getroffen die ervoor zorgen dat de informatie leesbaar blijft (zowel de media zelf, als het gegevensformaat) gedurende de gehele bewaarperiode, teneinde te voorkomen dat de informatie verloren gaat ten gevolge van toekomstige technologische veranderingen. Deze maatregelen met betrekking tot de houdbaarheid van gegevens betreffen uitsluitend actuele systemen.

Nog in te voeren maatregelen

- Procedure waarborgen houdbaarheid van gegevens van actuele systemen.

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Naleving Onderwerp **Bescherming van persoonsgegevens**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.1.4

Doelstelling

Het voorkomen dat privacy gevoelige gegevens toegankelijk zijn voor niet geautoriseerde.

Toelichting

De Privacy gevoelige gegevens binnen de Provincie betreffen de personeelsgegevens. Hiervoor gelden de procedures voor classificatie van gegevens en toegangsbeveiliging zoals deze zijn opgenomen in hoofdstuk 5 en 9.

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Naleving Onderwerp **Voorkomen van misbruik van IT voorzieningen**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.1.5

Doelstelling

Er voor zorgdragen dat de IT voorzieningen uitsluitend worden gebruikt voor geautoriseerde bedrijfsdoeleinden. Uiteraard kan met toestemming van het verantwoordelijke management ook voor andere doelstellingen gebruik gemaakt worden van de voorzieningen, mits deze niet strijdig zijn met de bedrijfsdoelstellingen.

Toelichting

De geldende regels en procedures worden op de volgende wijze bekend gemaakt aan de gebruikers:

- Informatie op het huisnet

Het ambtenarenreglement voorziet in mogelijkheden voor disciplinaire maatregelen.

Nog in te voeren maatregelen

- Folder "informatie voor veilig computergebruik"
- Opnemen informatie veilig computergebruik in de introductiecursus voor nieuwe medewerkers.

Documentverwijzing

- Huisnet

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Naleving Onderwerp **Voorschriften voor het gebruik van cryptografische middelen**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.1.6

Doelstelling

Vaststellen van regels en toepasselijke wetten voor het gebruik van cryptografische middelen.

Toelichting

Niet van toepassing

Nog in te voeren maatregelen

-

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 Datum: 1 april 2005 Akkoord: Geldig tot: 1 januari 2006

Hoofdstuk : Naleving Onderwerp **Verzamelen van bewijsmateriaal**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.1.7

Doelstelling

Verzamelen van bewijsmateriaal om maatregelen te kunnen treffen tegen personen of organisaties.

Toelichting

Geen

Nog in te voeren maatregelen

Verzamelen van bewijsmateriaal:

- Medewerkers dienen op de hoogte te zijn van de gegevens die de Provincie vastlegt over het computergebruik. Dit zijn:
  - Gearchiveerde e-mail berichten
  - Foutieve inlogpogingen
  - Voorkomen van virussen
  - Ongewenst netwerkverkeer, zoals het scannen van netwerkpoorten
  - Van alle centraal opgeslagen bestanden worden back-ups gemaakt. Deze worden conform de back-up procedure bewaard.
- Bewijsmateriaal wordt verzameld in logbestanden van systemen en netwerkapparatuur. Deze worden op regelmatige basis geanalyseerd. Standaard worden deze logbestanden gedurende drie maanden bewaard.

Analyse van materiaal vindt plaats op regelmatige basis. Bij een potentiële bedreiging zal het materiaal nader onderzocht worden. Bij verdenking wordt de volgende procedure gehanteerd:

- De logbestanden ouder dan 3 maanden worden bij een potentiële dreiging niet meer verwijderd gedurende het onderzoek.
- Na afronding van het onderzoek worden de gegevens apart gearchiveerd.

Documentverwijzing

-

Auteur: [redacted] Versie: 0.1 0.1 Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

12.2 Beoordeling van de naleving van het beveiligingsbeleid en technische vereisten

Hoofdstuk : Naleving Onderwerp **Naleving van het beveiligingsbeleid**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.2.1

Doelstelling

Waarborgen dat systemen voldoen aan het beveiligingsbeleid en de geldende beveiligingsnormen van de organisatie.

Toelichting

De eigenaars (zie paragraaf 5.1) van informatiesystemen en voorzieningen zijn functioneel verantwoordelijk voor regelmatige controles daarvan op naleving van het beveiligingsbeleid en alle andere beveiligingseisen. De operationele bewaking van het systeemgebruik is behandeld in paragraaf 9.7.

Nog in te voeren maatregelen

- Analyse van beveiligingsincidenten wordt uitgevoerd door de beheerders van de automatiseringssystemen conform de procedures voor incidentbeheer en probleembeheer.
- Op jaarlijkse basis wordt een controle uitgevoerd door de accountants van de Provincie Drenthe. De bevindingen worden vastgelegd in een rapport, op basis waarvan aanvullende maatregelen worden gepland.
- Op jaarlijkse basis worden de volgende audits uitgevoerd (Zie ook paragraag 12.3 voor richtlijnen t.a.v. audits):
  - Audit op basis van het handboek beveiliging waarbij aandacht wordt besteed aan de naleving en status van het handboek.
  - Procedures en maatregelen ten aanzien van leveranciers.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

Hoofdstuk : Naleving Onderwerp **Controle op naleving van technische normen**	Verwijzing naar Code IB Hoofdstuknummer : 12 paragraafnummer : 12.2.2

Doelstelling

De technische beveiliging van systemen dient regelmatig gecontroleerd te worden. De audit op naleving van de technische normen omvat het onderzoeken van de operationele systemen om zeker te stellen dat de beveiligingsmaatregelen ten aanzien van de hardware en software op de juiste manier zijn geïmplementeerd.

Toelichting

De controles worden handmatig uitgevoerd door de ICT systeemspecialisten en gegevens(bank)beheerders, of automatisch met behulp van programmatuur waarmee een technisch rapport wordt gegenereerd dat vervolgens door dezelfde deskundige(n) wordt bekeken.

Nog in te voeren maatregelen

Door middel van een technische security scan (penetratietest) worden de volgende beveiligingsaspecten gemeten:

- De potentiële mogelijkheden om binnen te dringen op het netwerk van de Provincie vanuit het Internet en andere gekoppelde netwerken, waaronder:
  - Het draadloze netwerk
  - De telewerkvoorziening
  - Modems
  - Koppeling met het provinciaal museum
- De potentiële mogelijkheden om vanuit het interne netwerk in te breken op systemen van de provincie en andere wijzen om integriteit; vertrouwelijkheid en beschikbaarheid van systemen aan te tasten
  - De status van security patches in besturingssystemen en toepassingssoftware
  - De compleetheid van de log gegevens voor analyse van beveiliging

De technische scans worden 2 maal per jaar uitgevoerd. Bij geconstateerde problemen kunnen extra scans worden uitgevoerd na reparatie van de gevonden defecten.

Documentverwijzing

-

Auteur: [redacted]
Versie: 0.1
Datum: 1 april 2005

Akkoord: Geldig tot: 1 januari 2006

12.3 Audits

Hoofdstuk : Naleving Onderwerp **Overwegingen ten aanzien van audits**	Verwijzing naar Code IB Hoofdstuknummer : 12 Paragraafnummer : 12.3.

Doelstelling

Effectiviteit van systeemaudits te maximaliseren en interferentie tijdens systeemaudits te minimaliseren. Audits op operationele systemen dienen zorgvuldig te worden gepland en goedgekeurd om het risico op verstoringen van bedrijfsprocessen tot het minimum te beperken.

Toelichting

Geen

Nog in te voeren maatregelen

Voor het uitvoeren van audits, zoals beschreven in paragraaf 12.2 gelden de volgende randvoorwaarden:

- Voor audits dient toestemming te worden verkregen van de eigenaars van de desbetreffende toepassingen.
- Audits mogen niet destructief van karakter zijn.
- De uitvoerende van de audit dienen een overeenkomst te tekenen waarin verklaard wordt:
  - De resultaten geheim te houden
  - Geen gegevens te kopiëren of te wijzigen
  - Alle resultaten volledig beschikbaar te stellen aan de Provincie
  - De provincie inzage te geven in de gebruikte werkwijze en hulpmiddelen
- Audits die een nadelige invloed kunnen hebben op performance en/ of beschikbaarheid van systemen dienen buiten kantooruren uitgevoerd te worden en nadat een back-up van de betroffen systemen is gemaakt.

Hulpmiddelen die gebruikt worden voor audits, het monitoren van beveiliging en analyseren van logfiles mogen uitsluitende toegankelijk zijn voor automatiseringsmedewerkers die deze taken moeten uitvoeren. Hiervoor gelden verder de standaard methoden voor toegangsbeveiliging.

Documentverwijzing

-

Auteur: [redacted]	
Versie: 0.1	
Datum: 1 april 2005	
Akkoord:	Geldig tot: 1 januari 2006

KPMG Forensic
Postbus 74555
1070 DC Amsterdam

Burg. Rijnderslaan 10-20
1185 MC Amstelveen
Telefoon (020) 656 7788
Fax (020) 656 7790

Persoonlijk en Vertrouwelijk
Provincie Drenthe
Mevrouw I. Rozema
Statengriffier
Postbus 122
9400 AC ASSEN

Onze ref MN/wv/130109

Contact [redacted]
Tel.: [redacted]

Amstelveen, 13 januari 2009

Betreft: Onderzoek naar verspreiding rapport Eurochamp

Geachte mevrouw Rozema,

Door middel van deze brief informeren wij u over het doel en de aard van het onderzoek dat wij zijn gestart in opdracht van de directeur-secretaris, mevrouw J.M. Imhof namens het college van Gedeputeerde Staten van de Provincie Drenthe. Wij verrichten een onderzoek naar aanleiding van berichten in de regionale media en vragen vanuit leden van Provinciale Staten over vermoedens dat het definitieve onderzoeksrapport inzake Stichting EuroChamp Foundation is verspreid vóórdat het rapport openbaar is gemaakt. Het college van Gedeputeerde Staten heeft besloten om een onderzoek te laten uitvoeren door KPMG Forensic naar de wijze waarop, wanneer en door wie het definitieve rapport inzake Stichting EuroChamp Foundation mogelijk eerder is verspreid.

Het doel van het onderzoek is in onze opdrachtbevestiging als volgt verwoord:

"Is het definitieve rapport van Deloitte Forensic Services inzake de stichting EuroChamp Foundation voortijdig verspreid vanuit het Provinciehuis? Zo ja, op welke wijze, wanneer en door wie?"

Met betrekking tot het voorgaande zullen wij relevante feiten, die uit ons onderzoek blijken, aan de opdrachtgever rapporteren. Voor zover relevant, zullen wij uw opmerkingen in onze rapportage verwerken. Het doel is te komen tot een evenwichtige weergave van de feiten in een juiste context.

Voor het kunnen verrichten van het onderzoek en het rapporteren van onze bevindingen, achten wij uw medewerking van belang. Voor de goede orde merken wij op dat uw medewerking vrijwillig is. Wij zullen de door u verstrekte informatie vertrouwelijk behandelen. Wij zullen slechts de voor ons onderzoek relevante feiten en/of omstandigheden rapporteren aan onze opdrachtgever.

Indien er uwerzijds bezwaren bestaan tegen, of indien u anderszins opmerkingen heeft over, het door ons verrichten van voornoemde opdracht, verzoeken wij u die aan ons kenbaar te maken.

Wij verzoeken u het onderzoek vertrouwelijk te behandelen. Wij vertrouwen er op u zo voldoende geïnformeerd te hebben. Bij vragen kunt u contact met ons opnemen.

Hoogachtend,
KPMG Advisory N.V.

[redacted]
Manager

MEMO

Aan	: Tanja en Annette
Afschrift	: Maarten
Van	: Andries
Datum	: 6 maart 2009; 8 maart aangevuld met opmerkingen Tanja en Annette
Onderwerp	: Rapport KPMG en concept GS nota
Classificatie	**: Vertrouwelijk, persoonlijk**

Hierbij het rapport van KPMG zoals ze dat hebben aangepast na het samenzijn in Hof van Saksen. Ik heb het zelf al gelezen en ook al besproken met Maarten Nooitgedacht. Hij heeft daar kennis van genomen en wil alle opmerkingen van ons drieën in een keer verwerken.

Mijn opmerkingen gaan hierbij.

De afspraak is dat jullie het lezen en de opmerkingen aan mij doorgeven (zondagavond bv) . Dan kan ik dat bundelen en aan Maarten doorgeven. KPMG levert dan het eindrapport op maandag 9 maart om 13.00 uur in tienvoud en genummerd bij ons aan. Ter verspreiding naar GS leden, de gedelegeerd opdrachtgever en de directeur/plaatsvervangend directeur.

Ik heb ook een GS nota opgesteld. De nota geeft een samenvatting, een tweetal (uiterste) scenario's voor de opstelling van GS naar PS en een beschrijving van mogelijke risico's. Ook een concept geleidebrief ri. PS is opgenomen.