Provincie Noord-Holland

Datum vergadering
19-april-2017
Nummer
17-062

Uw contactpersoon
[redacted]
CZ/CIO

Doorkiesnummer [redacted]

Bijlage: 16-009 directienota governance informatiebeveiliging

Betreft: Governance informatiebeveiliging

Nota Directie

1. Ontwerpbesluit

De directie besluit:

1. De taken, verantwoordelijkheden en bevoegdheden op het gebied van informatiebeveiliging in deze Nota vast te stellen.
2. Deze verantwoordelijkheden te communiceren naar alle managers en medewerkers.

2. Financiële, personele, juridische en communicatieve consequenties van het voorstel

Financieel*: geen financiële consequenties*
Communicatief: *De -op grond van het besluit over de Governance van 2 feb 2016 aangestelde CISO- is sinds juni 2016 actief. Er is over zijn aanstelling of over de Governance niet apart gecommuniceerd. Die actie en die vanuit het memo van een jaar geleden zullen nu alsnog worden opgepakt in samenwerking met communicatie.*
Personeel: *geen personele consequenties.*

3. Toelichting

Op 4 februari 2016 heeft de toen [redacted] een voorstel voor governance van de informatiebeveiliging ingediend, dat is geaccepteerd door Directie met uitzondering van de toen bijgevoegde RACI[1]-tabel. .
Van de tabel werd een nieuwe, leesbaardere versie gevraagd.
De kern van informatiebeveiliging is “risicomanagement” waarbij de lijn verantwoordelijk is voor het maken van afwegingen en beslissingen over het nemen van mitigerende maatregelen.
In deze Nota wordt de gevraagde, eenvoudiger RACI-tabel voorgesteld ter definitieve vaststelling. De tabel is bedoeld als hulpmiddel voor communicatie zodat alle betrokkenen helder krijgen waar welke rollen en verantwoordelijkheden liggen.

De volgende overwegingen staan nog steeds centraal:

- De hele organisatie is verantwoordelijk voor uitvoering van het beleid.

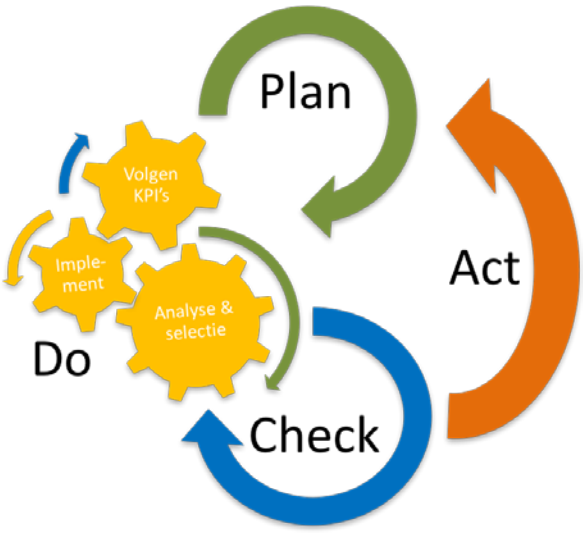
[1] RACI = Responsible - Accountable - Consulted - Informed

- Directies en sectoren zijn zelf verantwoordelijk voor de wijze waarop zij informatiebeveiliging in het dagelijks werk integreren. Vanuit het concern worden kaders gesteld om een minimaal niveau en de samenhang te bewaken.
- Een duidelijke scheiding tussen kaderstelling, uitvoering en toetsing, waarbij:
    - Kaderstelling door Concernzaken wordt voorbereid;
    - De lijnorganisatie de IB activiteiten uitvoert
    - Concerncontrol het systeem toetst op opzet, bestaan en werking;
- De taakgebieden uit het beleidsplan 2012 blijven van kracht en zijn geclusterd in drie verantwoordelijkheidsgebieden:
    - Activiteiten binnen het concern;
    - Activiteiten binnen de directies;
    - (systeem)toetsende activiteiten.

Informatiebeveiliging is en blijft een verantwoordelijkheid van directeuren, managers en medewerkers. Voor de uitvoerende activiteiten, zoals het uitvoeren van business impact analyses en risicoanalyses en het bepalen van maatregelen, staan de directies en sectoren aan de lat. Als het gaat om de generieke maatregelen en overkoepelend beleid (kaderstelling) is de directie Concernzaken verantwoordelijk. De controlfunctie is verantwoordelijk voor het toezicht op de naleving van de kaders en toetsing van de effectiviteit van de maatregelen en het beleid. Voor de noodzakelijke afstemming is binnen deze taakverdeling is een coördinerende en faciliterende rol weggelegd voor de centrale en decentrale informatiebeveiligingsfunctionarissen.

Hoofdpunten

- De lijnorganisatie behoudt haar eigen verantwoordelijkheid voor een goede informatieveiligheid
    - Concreet is dit vormgegeven door de formalisering van de rol van ‘systeem-eigenaar’ voor elk informatiesysteem.
- De coördinatie van de activiteiten om te komen tot en te verantwoorden over informatiebeveiliging worden belegd bij de CIO (CISO) en informatiemanagers.
- Concernzaken bereidt de goede kaderstelling voor en het directeuren, managers en medewerkers zijn verantwoordelijk voor de uitvoering.
- De toetsing op het systeem gebeurt door Concerncontrol.



Een en ander is in lijn met het principes van ‘Eigentijds sturen & verantwoorden’ en de visie op informatiebeleid zoals dat in het concept informatiebeleidsplan staat. De gedetailleerde uitwerking staat beschreven in de bijlage op deze nota uit 2016.

Aan de directie wordt gevraagd om, op basis van dit besluit, over hun de rollen taken en verantwoordelijkheden naar de betrokkenen te communiceren.
De CISO zal zelf een rondgang maken langs alle Sectormanagers om hun rol en taak te bespreken. Vooraf worden de directeuren gesproken. Van de directie wordt voorbeeldgedrag verwacht en ondersteuning van de activiteiten van de CISO in woord en daad.

De RACI-tabel hieronder geeft een overzicht van de taken voor informatiebeveiliging van alle betrokken partijen op hoofdlijnen weer.

	RACI informatiebeveiliging **R** = Responsible / uitvoeringsverantwoordelijke **A** = Accountable / eindverantwoordelijke **C** = Consulted / geraadpleegde **I** = Informed / geïnformeerde	Directie / AD	Stuurgroep I&I / CIO	CISO - Security Officer	FG/DPO - Privacy Officer	Directeur	Systeem-eigenaar	InformatieManager	Adviseur I&I	Beheerder (I&I, Cloud)	Concern-Control
Plan	**Strategisch en tactisch beleid**										
	Strategisch IB-Beleid opstellen (inclusief governance, RTV,)	**A**	**R**	C	C	I	I	I	I	I	I
	Tactisch IB-Beleid opstellen (IB-zakboekjes)	**A**	**R**	C	C	I	I	C	C	C	I
	Middelen beschikbaar stellen (BIA, RA & PIA, budgetten)	**A**	I	**R**	**R**	**R**	I	C	I	I	I
	Communiceren over rollen, taken, verantwoordelijkheden	**A**	I	**R**	**R**	**R**	I	C	I	I	I
Do	**Registratie, analyse & selectie per systeem & proces**										
	Informatiesystemen classificeren (BIA & PIA)	-	-	I	I	I	**A**	**R**	I	I	-
	Risico's beoordelen & maatregelen selecteren	-	-	C	C	I	**A**	C	**R**	I	-
	Documentatie en bewakingsagenda vastleggen	-	-	-	-	I	**A**	C	**R**	C	-
	Uitvoering & bewaking										
	IB-maatregelen implementeren (proces & techniek & contract)	-	-	C	C	**A**	**R**	I	C	**R**	-
	Over de werking van maatregelen rapporteren	-	-	I	I	**A**	**R**	I	I	**R**	-
Check	**Incidenten, audit & rapportage**										
	Registeren, beoordelen en opvolgen v incidenten	**A**	I	**R**	**R**	I	I	I	C	C	-
	De governance beoordelen en erover rapporteren - intern	**A**	I	**R**	**R**	C	C	C	C	C	-
	De governance beoordelen en erover rapporteren - intern	**A**	I	I	I	C	C	C	C	C	**R**
Act	**Jaarplan**										
	Bijsturen en plannen van verbeteringen	**A**	**R**	C	C	C	C	-	-	I	-
	AD = Algemeen Directeur										
	CIO = Chief Information Officer										
	CISO = Chief Information Security Officer										
	FG/DPO = Functionaris Gegevensbescherming / DataProtection Officer										
	IB = Informatiebeveiliging = **B**eschikbaarheid, **I**ntegriteit (betrouwbaarheid) en **V**ertrouwelijkheid van informatie										
	RTV = Rollen, Taken en Verantwoordelijkheden voor informatiebeveiliging										
	Informatiemiddel = dataverzamelingen, koppelingen, applicaties, apparatuur, diensten etc.										
	BIA = BusinessImpactAnalyse = hulpmiddel voor de classificatie van informatiemiddel										
	PIA = PrivacyImpactAnalyse = hulpmiddel voor analyse van 'verwerkingen' van persoonsgegevens										
	RA = RisicoAnalyse = anaalyse van kans op & impact van dreigingen										
	Baseline = Interprovinciale Baseline Informatiebeveiliging = afgeleide van de ISO27002										

4. Wijze van totstandkoming

Deze nota is opgesteld door de CISO van PNH (CIO Office).
Hij is afgestemd met de Informatiemanagers, directeur Concernzaken, het control-overleg en de CIO.

5. Verdere procedure

De tactische implementatie (‘precieze uitwerking’ van de governance) is gestart. Hierop zijn al besluiten genomen door Stuurgroep I&I & Directie. Deze handelden ook over de omzetting van het beleid naar IB-Zakboekjes. De rol van de Eigenaren wordt ook in een praktisch bruikbaar IB-Zakboekje uitgewerkt en toegelicht in de rondgang langs directeuren en sectormanagers.

Provincie Noord-Holland

IB-zakboekje 'Eigenaarschap informatiemiddelen en verwerkingen'

Tactisch beleid informatiebeveiliging & privacy Provincie Noord-Holland

Versie 1

Status: Definitief

Opgesteld door: [redacted]

Vastgesteld door: Directeur PNH

Datum: 29 november 2017

[1] CISO = Corporate Information Security Officer

Algemeen

De eindverantwoordelijkheid voor de informatiemiddelen (middelen voor informatieverwerking) & verwerkingen (hierna IM/V) berust bij de algemeen Directeur van PNH. Deze kan in de praktijk die verantwoordelijkheid niet uitoefenen en daarom wordt ze in de praktijk gedelegeerd naar anderen in de organisatie die op tactisch niveau beslissingen nemen en operationele taken aansturen. Het technisch en functioneel beheer en ook de beveiliging van een IM/V kan zowel binnen alsook buiten de provincie plaatsvinden, de verantwoordelijkheid blijft die van PNH.
Die door de directeur gedelegeerde verantwoordelijkheid noemen we 'eigendom'. Deze beslaat ook de Verantwoordelijkheid voor de Verwerkingen in de zin van de WBP[2] & AVG[3].

Doel van dit IB-Zakboekje

Dit zakboekje heeft -voor informatiebeveiliging & privacy- tot doel de eigendomsrol rondom IM/V te definiëren en uit te werken naar taken en verantwoordelijkheden voor de eigenaar. De uitwerking naar concrete handelingen volgt hierna en kan verschillen per eigenaar en verwerking.

Bereik van dit IB-Zakboekje

Alle eigendomstaken rondom IM/V vallen binnen het bereik van dit zakboekje. Het betreft de wijze waarop de eigendomsrol wordt toegekend alsmede de wijze waarop de verantwoordelijkheid wordt uitgeoefend. Soms wordt een onderwerp in een ander IB-Zakboekje verder uitgewerkt, zoals rondom rollen en rechten van toegang en privacy. Eigendom van individuele documenten (dus van de informatie in losse documenten, niet de dataverzamelingen in applicaties en databases) wordt behandeld in het IB-Zakboekje Classificatie.

Wíe zijn eigenaren

Eigendom namens de provincie berust in beginsel bij de *sectormanager* voor het IM/V waarvan hij hoofdgebruiker is en is gekoppeld aan *proceseigenaarschap*. Waar een middel meerdere processen bedient zijn er deel-eigenaren en overleggen deze over het geheel (bijvoorbeeld SAP als systeem/dienst voor HRM, Inkoop en Financiën). IM/V die niet aan een proces gekoppeld kunnen worden en als ondersteuning voor heel PNH gelden hebben (meestal) de sectormanager I&I als eigenaar. Denk hierbij aan het datanetwerk, email en de werkplekken. De mandateringsstructuur van PNH is leidend. Bij onduidelijkheid beslist in laatste instantie de algemeen directeur van PNH. In Bijlage 1en 2 zijn verschillende scenario's schematisch uitgewerkt, voor verwerkingen in eigen beheer, gehost, in de cloud en bij koppelingen/uitwisselingen met andere systemen en partijen.

Overige verantwoordelijken

Eigendom namens PNH is de centrale verantwoordelijkheid rondom alle IM/V. De advisering rond het IM/V berust bij specialisten in I&I en de uitvoering van de techniek bij de technisch beheerders (binnen en buiten PNH).

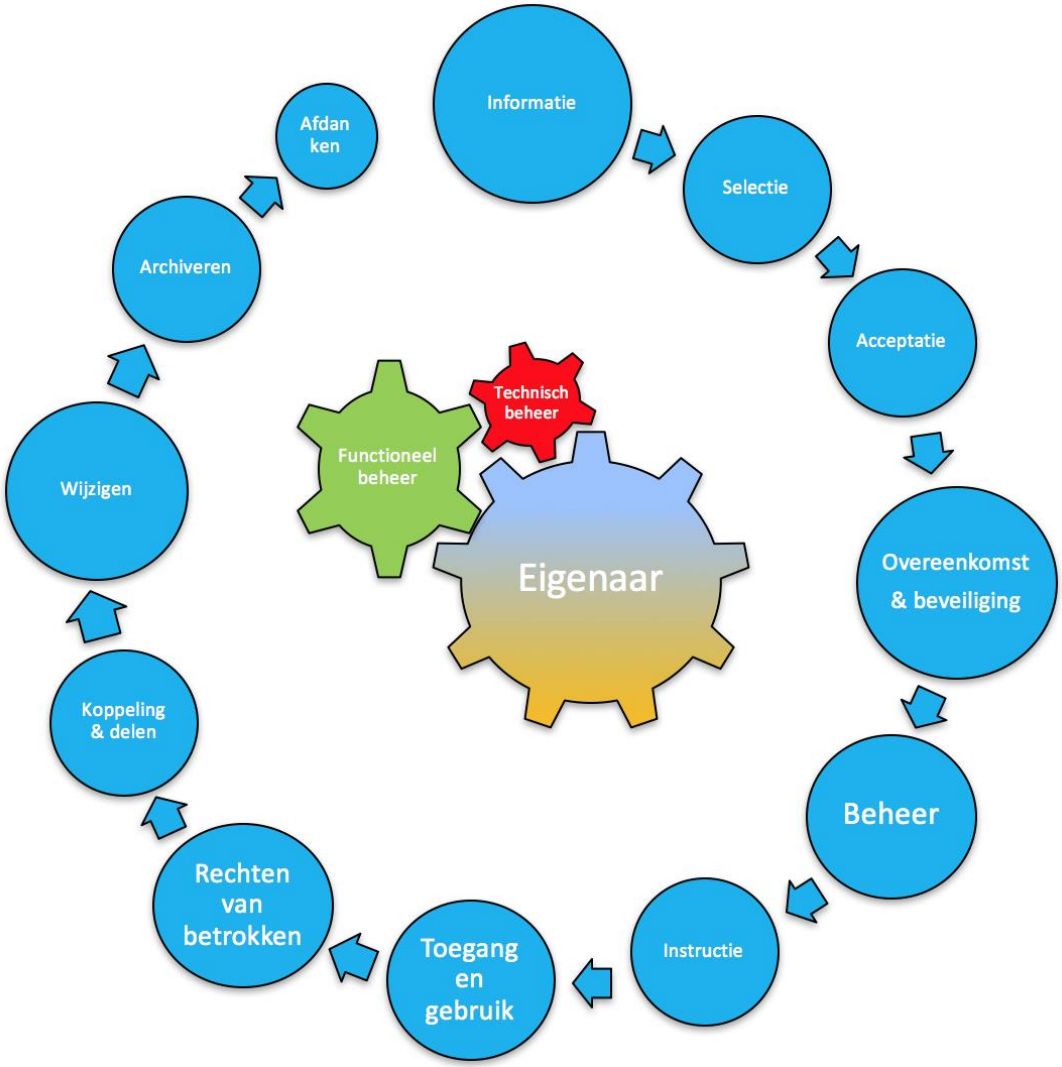
---

[2] WBP - Wet Bescherming Persoonsgegevens (van kracht sinds 2001)
[3] AVG - Algemene Verordening Gegevensbescherming (van kracht sinds mei 2016)

In Bijlage 2 staat de RACI-matrix voor informatiebeveiliging zoals die door de directie van PNH is vastgesteld.

Beleidsuitgangspunten voor eigendom

Ieder informatiemiddel van PNH heeft een eigenaar die namens de directie de verantwoordelijkheid uitoefent voor het informatiemiddel, zoals vastgesteld in de Directienota 'Governance informatiebeveiliging feb 2017', van 20 april 2017. De RACI[4]-tabel uit deze nota is hier als bijlage overgenomen.
De gedelegeerde verantwoordelijkheid omvat alle besluiten en activiteiten ten aanzien van het informatiemiddel gedurende de hele levenscyclus van het middel, dus van aanschaf tot en met afdanken De mandateringsstructuur van PNH voorziet in de noodzakelijke bevoegdheid.
De taken kunnen door de eigenaar voor uitvoering gedelegeerd worden naar andere medewerkers, maar houdt toezicht op de uitvoering. De eigenaar is primair aanspreekpunt voor adviseurs en toezichthouders en legt verantwoording af aan de directie.



Wat zijn 'Informatiemiddelen en -verwerkingen'

'Informatiemiddel' is elk systeem en elke dienst die een functie vervult in de informatievoorziening, zoals applicaties, uitbestede verwerkingen & diensten voor communicatie en archivering. Ook de gegevenskoppelingen met systemen of derden horen bij het systeem, of dat nu over een VPN of via de mail geschiedt.
Denk óók aan internetlijnen, cloud-services (zoals Box, Prezi), gehoste applicaties en zaken als eHerkenning & DigiD, authenticatiediensten en adviesdiensten.
Voor verwerkingen nemen we de definitie van de AVG[5], art.4: 'al dan niet geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens' *onder verantwoordelijkheid van PNH*.

[4] RACI = Responsible-Accountable-Consulted-Informed - 'wie_doet_wat'-tabel
[5] Algemene Verordening Gegevensbescherming

Wat zijn de taken van de eigenaar

Uitoefening van eigendom namens de Verantwoordelijke (algemeen directeur) behelst de volgende activiteiten die de hele levenscyclus van een informatiesysteem/verwerking beslaan:

- Informatie: tijdens het onderzoek naar nieuw aan te passen middel voor de informatievoorziening brengt hij/zij eisen die aan het informatiemiddel worden gesteld in beeld middels een BIA[6] (en soms een PIA[7]). Die eisen gaan over de Beschikbaarheid, Integriteit, Vertrouwelijkheid, Privacyklasse, Maximale uitvalduur, Maximaal gegevensverlies & de eisen uit de AVG (rechtmatigheid/doelbinding, proportionaliteit, subsidiariteit, dataminimalisatie)[8];
- Selectie: op basis van de gevonden waarden moeten passende criteria vastgesteld worden voor de beveiliging van het IM/V in de vorm van te treffen maatregelen en zekerheden dat die maatregelen ook effectief zijn, ook bij uitvoering door derden. Afwijking vergt expliciete acceptatie van het geassocieerde risico door de Eigenaar.
  Hierbij laat ze Eigenaar zich adviseren door Informatiemanagement en adviseurs I&I (ondersteund vanuit CIO-Office).
- Acceptatie: bij de start van het gebruik van het informatiemiddel wordt alle informatie rondom uitgevoerde BIA en PIA, vereiste maatregelen en zekerheden gedocumenteerd en vastgelegd in het Register van middelen & verwerkingen (hierna Register). De belangrijkste informatie is gestructureerd opgeslagen om snel toegankelijk te zijn en voor meldingen te kunnen zorgen naar actiehouders.
- Overeenkomst: alle afspraken (contract) rondom uitvoering van de beveiliging en privacy in de vorm van de Overeenkomst, SLA, OLA's en Verwerkersovereenkomst worden door de eigenaar ondertekend en opgenomen in het Register;
- Beheer: de eigenaar ziet actief toe op beheer van het IM/V conform afspraken en eisen. Terugkerende afspraken voor toezicht en rapportage worden waar mogelijk aan agenda's gekoppeld om de aandacht op komende acties te vestigen. Het toezicht op het IM/V krijgt hierbij de vereiste aandacht.
- Toegang en gebruik: de eigenaar zet een autorisatiematrix op die gegevens en functionaliteit koppelt aan rollen/functies in/voor het middel (meest gebruikelijk in applicaties). Hierbij neemt hij 'functiescheiding' mee in de beoordeling van de rollen. De eigenaar verleent toestemming voor de toegang en het gebruik en ook beëindiging van rechten (zie hiervoor verder het IB-Zakboekje IRR).
- Instructie: de eigenaar zorgt voor de nodige opleiding en training voor de gebruikers om het informatiemiddel te kunnen gebruiken zoals bedoeld en (vermoedens van) misbruik, kwetsbaarheden en datalekken direct te melden bij de eigenaar, beheerder, incidentloket of CISO/FG[9].
- Koppelingen en informatie uitwisselen: de eigendomstaak heeft ook betrekking op alle informatie-koppelingen en -verstrekkingen met andere middelen (systemen) of partijen, binnen en buiten PNH.
- Wijzigen: de eigenaar zorgt ervoor dat hij bij alle wijzigingen die invloed op de vereiste Beschikbaarheid, Integriteit of Vertrouwelijkheid of Privacy van zijn middel kunnen hebben betrokken is en waar mogelijk het laatste woord heeft. Bij grote wijzigingen in het IM/V zorgt hij voor een (geactualiseerde) BIA en/of PIA.
- Incidenten: de eigenaar zorgt ervoor dat hijzelf, de beheerder en de verwerker van het IM/V alle (vermoedens van) beveiligingsproblemen en datalekken zo spoedig mogelijk meldt en volledige medewerking verleent aan repressie van de gevolgen, onderzoek naar de oorzaken, ondersteuning bij de gevolgen (zoals melden bij de betrokkenen) en verhelpen het lek.

---

[6] BIA = Business Impact Analyse
[7] PIA = Privacy Impact Analyse: noodzakelijk bij zeer gevoelige, zeer veel persoonsgegevens of een risicovolle verwerking
[8] Uitwerking van de eisen uit de AVG in het Zakboekje Privacy
[9] FG = Functionaris Gegevensbescherming

- Rechten van betrokkenen: bij de verwerking van persoonsgegevens hoort ook dat er verantwoording wordt afgelegd aan de betrokkenen (natuurlijke personen waar het over gaat). De uitoefening van hun rechten –informatie, inzage, rectificatie, beperking van de verwerking, overdraagbaarheid, bezwaar en vergetelheid- verloopt via de eigenaar.
- Archiveren: toepassen van de archiveringsregels, zoals vastgesteld in 'Besluit informatiebeheer 2014-30-09-2014' en wettelijke bewaartermijnen.
- Afdanken: wanneer (een deel van) het informatiemiddel wordt afgedankt, zorgt de eigenaar dat alle informatie wordt gemigreerd of vernietigd.

Register van informatiemiddelen en verwerkingen

PNH onderhoudt een Register[10] waarin alle informatie rondom informatiemiddelen en verwerkingen hun eigenaren, de beveiligingseisen en -afspraken zijn vastgelegd, teneinde tijdens de levensloop van het IM/V de gewenste informatiebeveiliging & privacybescherming te kunnen waarborgen. Het Register is toegankelijk voor de eigenaren, betrokken beheerders en adviseurs CIO en I&I voor de uitoefening van hun respectievelijke sturende, operationele en toezichthoudende taken.
De eigenaar is verantwoordelijk voor de juistheid, actualiteit & volledigheid van de informatie voor *zijn* verwerking in het Register.

Hulpmiddelen voor de eigenaar

- De InformatieManagers zijn vanuit hun rol beschikbaar voor adviezen over beveiliging en begeleiden de tot stand komen van een goede BIA.
- BIA - Business Impact Analyse - belangrijk instrument om middel te classificeren in termen van vereiste Beschikbaarheid, Integriteit, Vertrouwelijkheid en privacy. Het is het sturende document bij alle vervolgstappen;
- PIA - Privacy Impact Analyse - analyse van grootschalige en/of risicovolle verwerkingen op rechtmatigheid, proportionaliteit etc.;
- Register - onlinevoorziening waar alle relevante informatie over het middel/de dienst, waaronder afspraken over beveiliging en privacy vastgelegd wordt, ter ondersteuning van beheer, gebruik & toezicht;
- Advies en ondersteuning - disciplines uit het CIO-office (CISO, PO[11] en FG), I&I en functioneel beheerders over informatiebeveiliging, privacy en architectuur ondersteunen de eigenaar bij de selectie van maatregelen en de uitvoering van zijn toezichthoudende taken.

Relatie met ander beleid

'Eigendom' heeft raakvlakken met bijna elk ander beleid rondom informatiebeveiliging & privacy. In het informatiebeveiligingsbeleid heeft de eigenaar de sturende en bewakende rollen voor de realisatie van de beveiliging, waarbij de algemeen directeur de eindverantwoordelijkheid behoudt. Eigenaarschap bestuurt veel activiteiten in aanpalende beleidsdomeinen in informatiebeveiliging en privacy (de andere IB-Zakboekjes).
Anderen (CISO, PO) adviseren over informatiebeveiliging & privacy en weer anderen (functioneel beheer) voeren veiligheidstaken uit, onder het gezag van de eigenaar.

[10] Register: hoe en waar wordt nog bepaald
[11] PO = Privacy Officer

Vaststelling, uitvoering en beheer

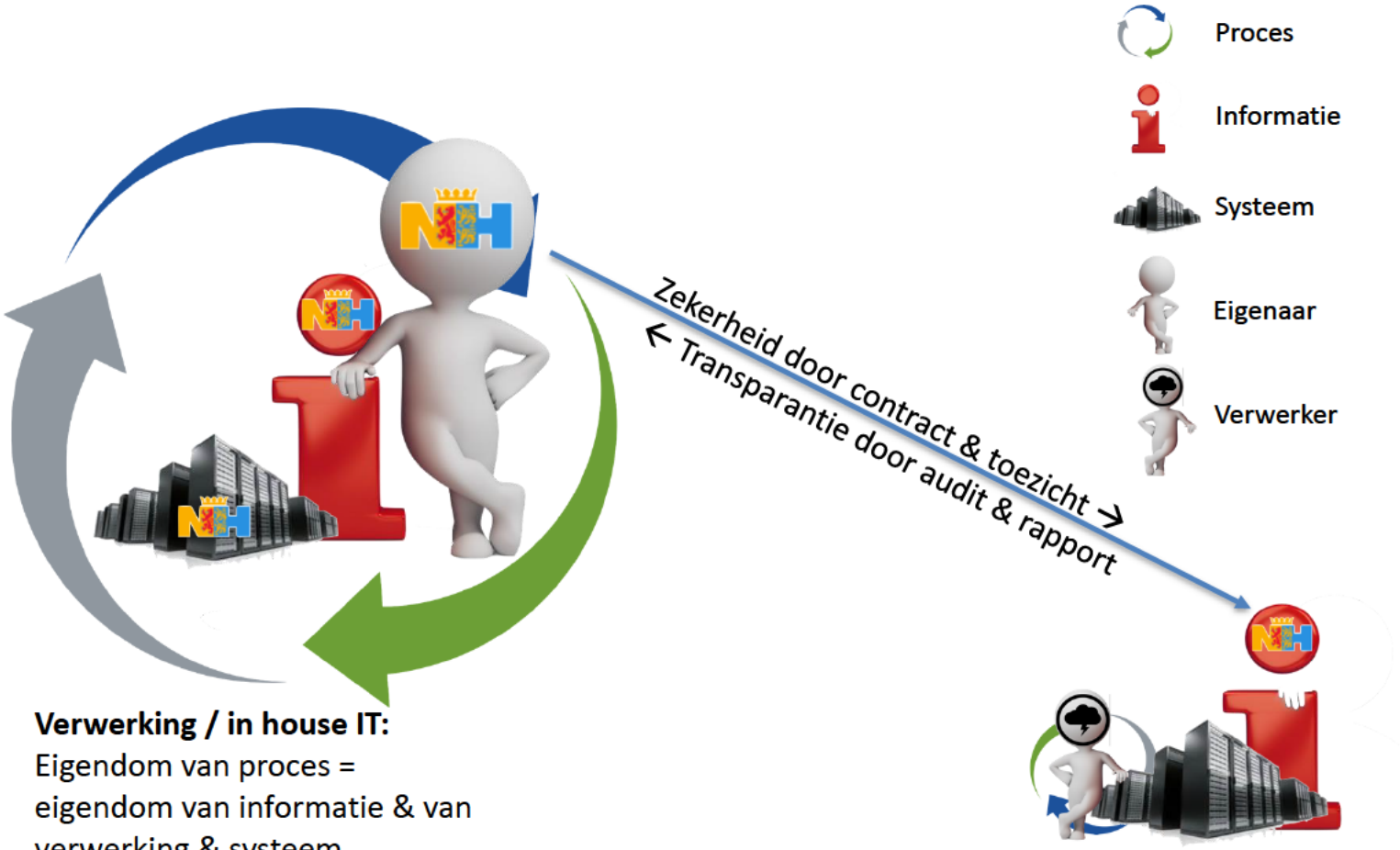
Dit document is vastgesteld door de Directie en wordt voor uitvoering bekend gemaakt aan alle betrokkenen. De CISO & FG zorgen voor bekendmaking bij alle Sectormanagers/beoogde eigenaren door het takenpakket toe te lichten. De InformatieManagers zijn mede-aangewezen om de invoering van dit beleid te begeleiden (zie RACI in Bijlage 2). De inrichting van het Register is de verantwoordelijkheid van de CISO & FG, de technische realisatie wordt belegd bij sector I&I. De CISO & FG houden toezicht op de toepassing en werking van dit beleid.
Revisie en aanvulling van dit beleid is een doorlopende verantwoordelijkheid van de CISO & FG, die ook zorgen voor afstemming met de eigenaren. Wijzigingen leiden tot opnieuw vaststellen van aangepast beleid door de directie.

Publicatie

Dit en alle andere Zakboekjes voor Informatiebeveiliging en Privacy worden gepubliceerd op het ‘Plein’, het intranet van PNH en zijn vindbaar met de zoekterm ‘IB-zakboekje’. Bij het opstellen zijn de informatiemanagers, adviseurs I&I, PNH IT-beheer en Fujitsu betrokken.

Datum inwerkingtreding	Namens de stuurgroep I&I	Namens de Directie
01 januari 2018	[redacted]	R. Bergkamp

Bijlage 1 - eigendom in verschillende verwerkingsscenario's

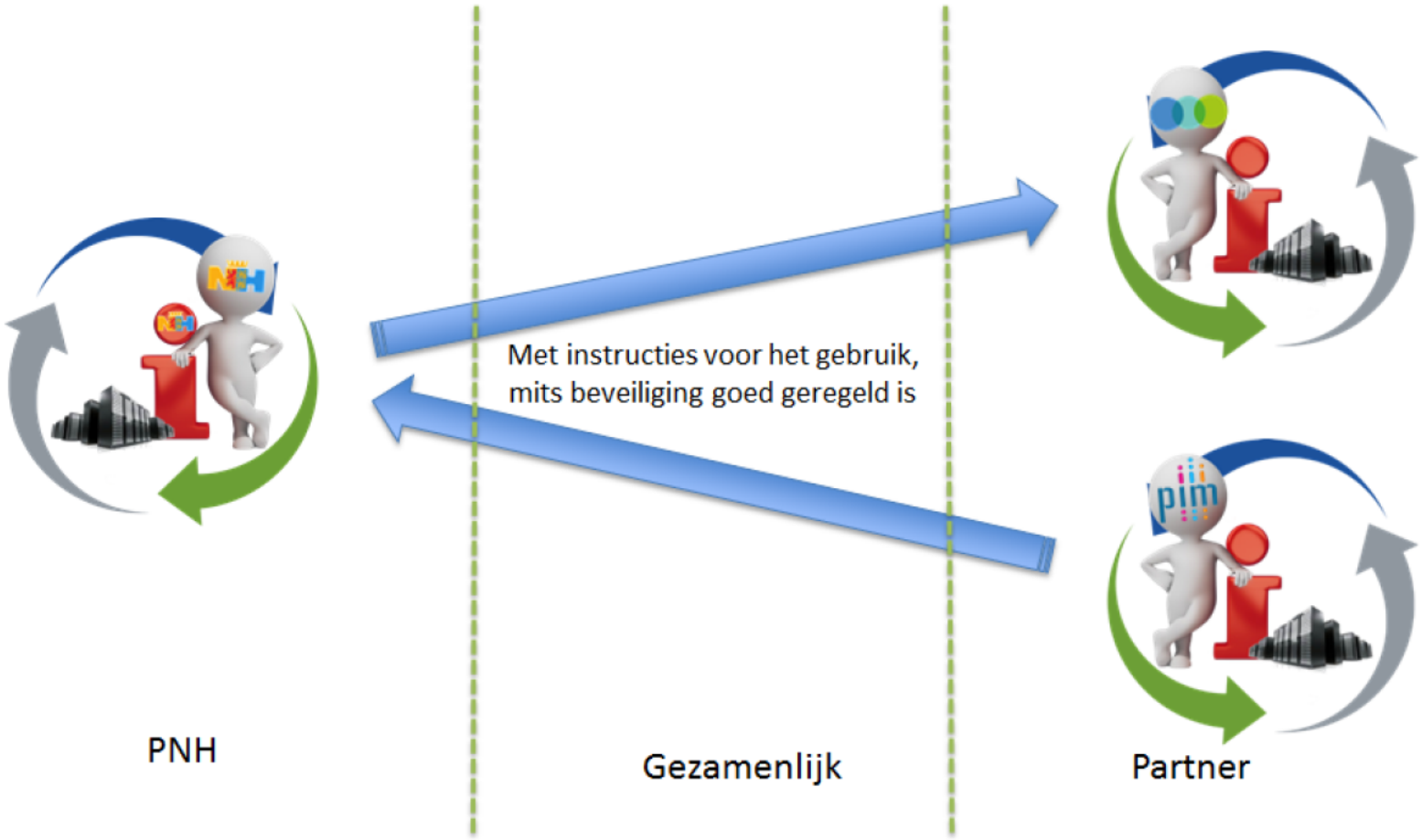


Verwerking / in house IT:
Eigendom van proces = eigendom van informatie & van verwerking & systeem.

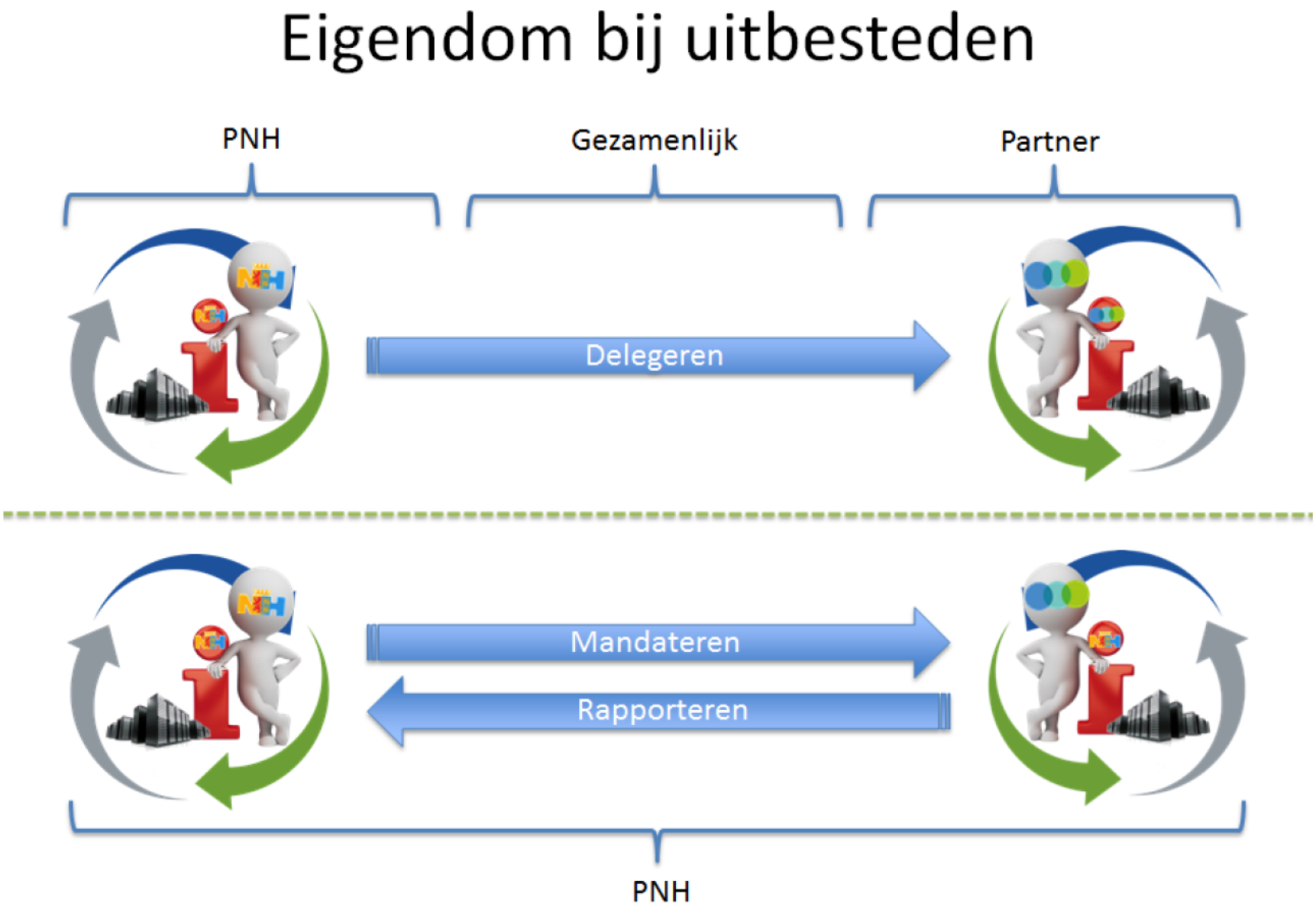
Uitbestede IT / SAAS:
Eigendom van proces = eigendom van informatie & verwerking door een 3e

Eigendom bij delen

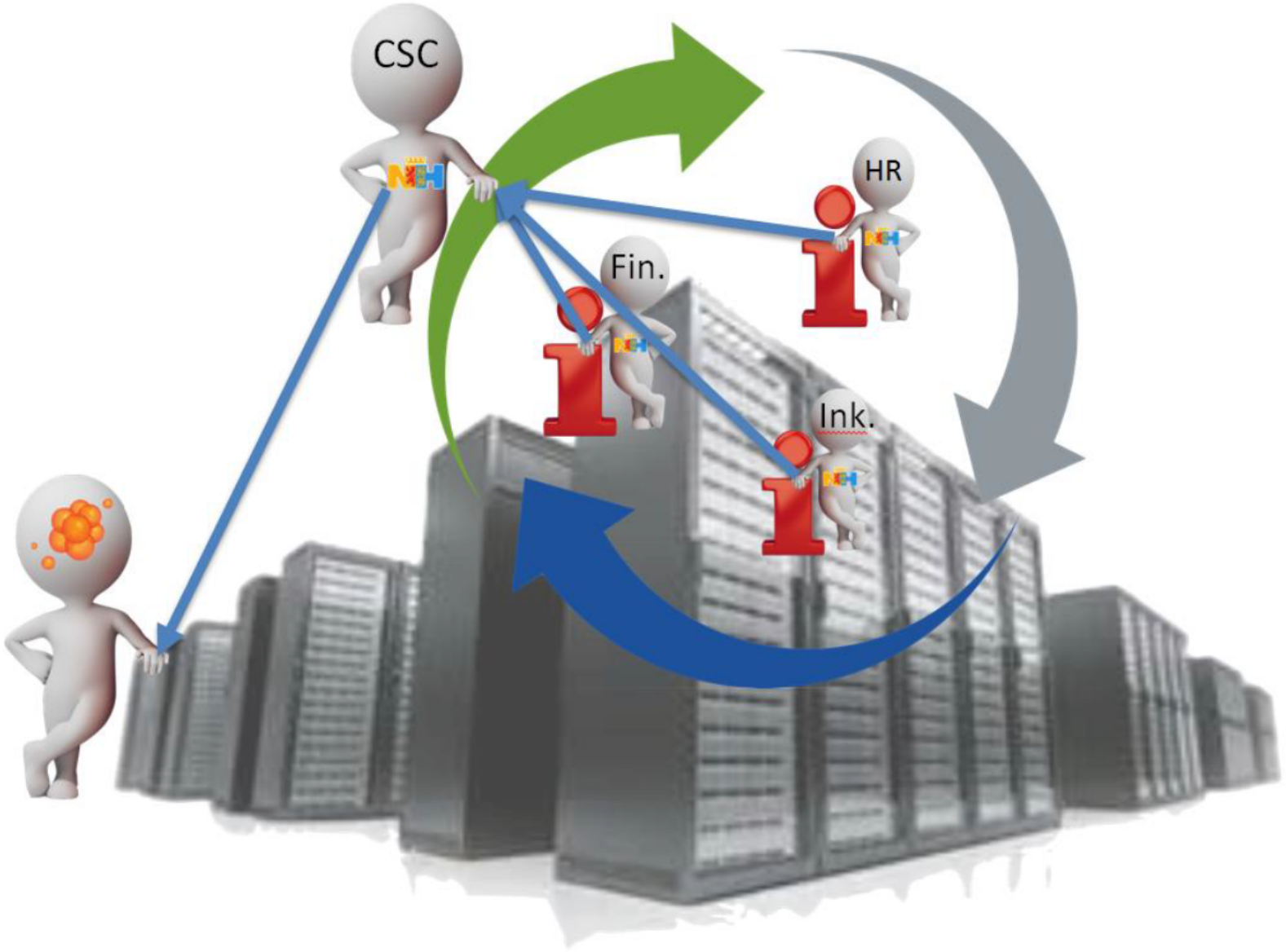
Verantwoordelijkheden bij delen



Eigendom bij delegeren & mandateren



Meerdere processen-verantwoordelijken, 1 gemandateerd (hoofd-)eigenaar



Bijlage 2 - informatiebeveiligings-governance RACI (Nota directie 20 april 2017)

RACI informatiebeveiliging

R = Responsible / uitvoeringsverantwoordelijke
A = Accountable / eindverantwoordelijke
C = Consulted / geraadpleegde
I = Informed / geïnformeerde

		Directie / AD	Stuurgroep I&I / CIO	CISO - Security Officer	FG/DPO - Privacy Officer	Directeur	Systeem-eigenaar	InformatieManager	Adviseur I&I	Beheerder (I&I, Cloud)	Concern-Control
Plan	**Strategisch en tactisch beleid**										
	Strategisch IB-Beleid opstellen (inclusief governance, RTV,)	**A**	**R**	C	C	I	I	I	I	I	I
	Tactisch IB-Beleid opstellen (IB-zakboekjes)	**A**	**R**	C	C	I	I	C	C	C	I
	Middelen beschikbaar stellen (BIA, RA & PIA, budgetten)	**A**	I	**R**	**R**	**R**	I	C	I	I	I
	Communiceren over rollen, taken, verantwoordelijkheden	**A**	I	**R**	**R**	**R**	I	C	I	I	I
Do	**Registratie, analyse & selectie per systeem & proces**										
	Informatiesystemen classificeren (BIA & PIA)	-	-	I	I	I	**A**	**R**	I	I	-
	Risico's beoordelen & maatregelen selecteren	-	-	C	C	I	**A**	**C**	**R**	I	-
	Documentatie en bewakingsagenda vastleggen	-	-	-	-	I	**A**	**C**	**R**	**C**	-
	Uitvoering & bewaking										
	IB-maatregelen implementeren (proces & techniek & contract)	-	-	C	C	**A**	**R**	I	C	**R**	-
	Over de werking van maatregelen rapporteren	-	-	I	I	**A**	**R**	I	I	**R**	-
Check	**Incidenten, audit & rapportage**										
	Registeren, beoordelen en opvolgen v incidenten	**A**	I	**R**	**R**	I	I	I	C	C	-
	De governance beoordelen en erover rapporteren - intern	**A**	I	**R**	**R**	C	C	C	C	C	-
	De governance beoordelen en erover rapporteren - intern	**A**	I	I	I	C	C	C	C	C	**R**
Act	**Jaarplan**										
	Bijsturen en plannen van verbeteringen	**A**	**R**	C	C	C	C	-	-	I	-

AD = Algemeen Directeur
CIO = Chief Information Officer
CISO = Chief Information Security Officer
FG/DPO = Functionaris Gegevensbescherming / DataProtection Officer
IB = Informatiebeveiliging = **B**eschikbaarheid, **I**ntegriteit (betrouwbaarheid) en **V**ertrouwelijkheid van informatie
RTV = Rollen, Taken en Verantwoordelijkheden voor informatiebeveiliging
Informatiemiddel = dataverzamelingen, koppelingen, applicaties, apparatuur, diensten etc.
BIA = BusinessImpactAnalyse = hulpmiddel voor de classificatie van informatiemiddel
PIA = PrivacyImpactAnalyse = hulpmiddel voor analyse van 'verwerkingen' van persoonsgegevens
RA = RisicoAnalyse = anaalyse van kans op & impact van dreigingen
Baseline = Interprovinciale Baseline Informatiebeveiliging = afgeleide van de ISO27002

Provincie Noord-Holland

Zakboekje ‘Classificatie van documenten’

Tactisch beleid Informatieveiligheid Provincie Noord-Holland

versie 1.2

Status: **Definitief**
Vastgesteld door: Directie van de provincie Noord-Holland
Datum: 13 juli 2017

1. Zakboekje ‘Classificatie van documenten’

1.1. Algemeen

De PNH-directie heeft het ‘open tenzij’ standpunt voor informatie van de provincie ingenomen. Dit betreft primair de vertrouwelijkheid van informatie. Dit standpunt behoeft interpretatie en toepassing. Zoals het ‘tenzij’ zegt: niet álle informatie kan met iedereen zomaar gedeeld worden om allerlei redenen. Bescherming van de vertrouwelijkheid vergt afspraken en middelen om die vertrouwelijkheid te effectueren. Daarover gaat dit Zakboekje.
Het effectueert mede het idee van ‘verantwoordelijkheid’, dat iedere medewerker heeft voor de **B**eschikbaarheid, **I**ntegriteit en **V**ertrouwelijkheid van informatie.

1.2. CRUD

De afkorting staat voor Create (Maken), Read (Lezen), Update (Aanpassen), Delete (Verwijderen). Dit zijn de rechten die een persoon kan hebben op een document. De klasse van een document stuurt de toekenning van deze rechten.

1.3. Definities

Eigendom = het recht om een document te maken, wijzigen, classificeren, bewerken, verspreiden en verwijderen én het recht dit aan anderen te toe te staan..
Gebruiker = persoon die het recht van een Eigenaar heeft gekregen om een document te lezen en delen of die er een eigen versie (kopie) van te maken;
Extern delen = een document beschikbaar maken voor niet-PNH-medewerkers.

1.4. Doel en doelgroep van dit beleid

Het doel van dit stuk is het formuleren en vastleggen van een classificatiemodel, dat geldt als basis onder nadere afspraken en besluiten over de gewenste omgang met documenten in de provincie Noord-Holland. *De doelgroep is het management*. Voor de grote groep medewerkers zal een eenvoudig lees- en hanteerbare ‘flyer’ worden opgesteld en gepubliceerd.

1.5. Bereik

Dit beleid heeft betrekking op alle informatie *in document-vorm* van de provincie en is bedoeld voor *intern* gebruik. Het betreft documenten (zoals .doc-, .xls-, .pdf –bestanden en vergelijkbare) die worden opgesteld, aangepast en gedeeld door medewerkers en applicaties *binnen en vanuit* het PNH-domein. Deze documenten vinden we in Verseon, RIS, personeelsdossiers in SAP en op de S-Schijf en andere PNH-shares[1]. Uitvoer uit applicaties vervat in documenten, vallen ook onder dit beleid.
Informatie in databases (SAP, GIS etc.) wordt als 'systeem'/ 'informatiemiddel' geclassificeerd met behulp van een BIA[2]. Dergelijke informatie noemen we geen documenten maar '*gestructureerde informatie*' die geen documentvorm heeft tot het als uitvoer een documentvorm aanneemt.

1.6. Klassen en kenmerken

De indeling in klassen volgt die van de landelijke overheid, Vertrouwelijk valt samen met 'Departementaal vertrouwelijk'.

- OPENBAAR – vrij in te zien en gebruiken door 'een ieder'; het toekenningsrecht berust bij PS, GS en CdK;
  - Informatie op de website https://www.noord-holland.nl;
  - Informatie die als gevolg van een WOB-verzoek is vrijgegeven;
  - 'Open Data' ingevolge een (gedelegeerd) Directiebesluit;
- INTERN – voor intern en selectief extern gebruik; standaardklasse voor informatie;
  - het document is in te zien voor iedereen met toegang tot de PNH-shares en Verseon;
  - het document kan gedeeld worden binnen en buiten PNH maar uitsluitend voor werk-gerelateerde doeleinden;
  - Is NIET 'openbaar voor een ieder', als bedoeld in de Wob);
  - Dit recht mag door iedere PNH-er worden toegekend aan een nieuw document;
- INTERN VERTROUWELIJK – voor beperkt intern gebruik; recht kan worden toegekend door iedere medewerker van PNH;
  - Het document is zichtbaar (het bestaan is dus algemeen bekend);
  - Beperkte verspreiding, alleen door de Eigenaar;
  - Het document is alleen te lezen, aan te passen of te Delen *met toestemming van de eigenaar*;
  - Verlagen van de klasse kan –in principe- alleen de eigenaar.
- GEHEIM – voor zeer beperkt Intern gebruik; Het toekenningsrecht berust bij PS, een statencommissie, GS en CdK;
  - onbekend, niet in te zien of verspreiden anders dan op last van de eigenaar;
  - De Provinciewet dicteert het gebruik van deze klasse;
  - Verlagen van de klasse (alleen door PS, statencommissie, GS en CdK, zij leggen & heffen de geheimhouding op)

[1] PNH-Share = netwerkschijven H:, S: en Y:, opslagplek voor documenten in het PNH-domein
[2] BIA = Business Impact Analyse = classificatie op Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatiesystemen en -middelen

2. Toepassing van de classificatie

2.1.1. Nieuw document

De classificatie wordt -door de opsteller- aan een document toegekend (dit is ook de persoon die een ‘uitdraai’ uit een applicatie maakt).. Maakt de opsteller van een document geen klasse-keuze, dan krijgt het document de classificatie ‘Intern’. Dit moet blijken uit duidelijk zichtbare markering.

2.1.2. Aanpassen document van anderen

Een bestaand ‘Intern’ document mag door iedereen worden aangepast (en verplicht onder een *nieuwe naam* worden opgeslagen) en dan ook gelijk opnieuw geclassificeerd door de *nieuwe eigenaar*. Een gekopieerd document krijgt zo, zonder noodzaak van toestemming, een eigen eigenaar en classificatie. Ook hier geldt dat niets doen tot de klasse ‘Intern’ leidt.

2.1.3. Aanpassen klasse

Aanpassen van de classificatie van andermans document is niet mogelijk. Een nieuwe klasse toekennen is alleen mogelijk door het onder een andere naam op te slaan. De aanpasser van de classificatie van het *nieuwe document* en wordt ook de *nieuwe eigenaar*.

2.1.4. Vertrouwelijk

Toekennen van de klasse ‘Vertrouwelijk’ betekent dat alleen (door de eigenaar) benoemde personen inzage krijgen en dat alleen de eigenaar het document mag aanpassen of vernietigen. Het document delen met personen/instanties binnen of buiten PNH mag alleen met toestemming van de eigenaar en op een veilige manier, zoals versleutelde e-mail.

2.1.5. WOB

Voor bijvoorbeeld privacygevoelige informatie is de classificatie Vertrouwelijk verplicht. De classificatie ‘vertrouwelijk’ heeft overigens geen betekenis in de zin van de WOB. Het is mogelijk dat een als vertrouwelijk geclassificeerd document alsnog openbaar gemaakt zal moeten worden als daar in het kader van de WOB om wordt gevraagd. Dit recht is voorbehouden aan GS, op basis van een Juridisch advies.

3. Randvoorwaarden & middelen

3.1. Interprovinciale Baseline Informatiemiddelen

De provinciale baseline waaraan wij ons hebben verbonden, alsmede alle achterliggen bronnen (wo ISO27002) en de Algemene Verordenign Gegevensbescherming dragen op tot het kennen en kenbaar maken van de informatieklasse van verwerkingen en documenten, opdat er verantwoordelijk mee kan worden omgegaan. De klasse moet worden vastgesteld door de Verantwoordelijke voor de verwerking.

3.2. Classificeren en autoriseren

Classificering en markering op het niveau van bestanden en PNH-Shares moet voor iedere medewerker mogelijk zijn middels *eenvoudig te bedienen hulpmiddelen*. De toegekende classificatie moet *gekoppeld zijn aan toegangsbeveiliging en autorisatiemechanismes*.
Delegeren van autorisatie moet eenvoudig zijn: specifiek waar nodig, generiek in andere gevallen (zoals bij ondersteuners of teamleden).

3.3. Markering

De toegekende classificatie zichtbaar zijn op de openingspagina van documenten én in de meta-informatie van het document, waar mogelijk. Op het niveau van mappen op ‘shares’ (S-schijf) is de markering liefst in de verkenner (Windows) zichtbaar.

3.4. Versleuteling

Versleuteling (cryptografische beveiliging) van documenten tijdens opslag (PNH-shares, Verseon) en transport (Delen) is een belangrijke gewenste faciliteit.
Voor persoonsgegevens is dit een wettelijke plicht, ‘waar mogelijk’. Optimaal is deze ingebouwd in de gebruikersinterface in de vorm van een ‘druk op de knop’ en van voldoende kwaliteit om eventuele aanvallen te weerstaan.

3.5. Vaststelling & Publicatie

De Directie van de provincie stelt dit beleid vast. Het toezicht op de uitvoering wordt uitgeoefend door de directeuren die hierover ook rapporteren. Op de werking zien toe de security officer (CISO) en de interne auditfunctie van de provincie. Voor de niet-ingewijde lezer zal een toelichting worden opgesteld met voorbeelden, te publiceren op Plein.
Dit en alle andere Zakboekjes worden gepubliceerd op het ‘Plein’, het intranet van PNH en zijn vindbaar met de zoekterm ‘Zakboekje’. Bij het opstellen zijn de informatiemanagers, adviseurs I&I, PNH IT-beheer en Fujitsu betrokken.

3.6. Bijlage 1 – voorbeelden[3] van vertrouwelijke/geheime informatie

Informatie over	**Voorbeelden**
Basis-persoonsinformatie	NAW, personeelsnummer, BSN, beoordelingen, klachten.. *Alles dat herleidbaar is naar een natuurlijke persoon.* *(informatie over vertegenwoordigers valt hier buiten)*
Bijzondere persoonsinformatie	politieke, sexuele, religieuze voorkeur, sociaal-economische informatie etc.
Financiën	Meerjarenraming, salarissen, bonussen.
Aanbestedingen	Beoordelingscriteria, contracten.
Bezwaarschriften	Tegen besluiten van de provincie.
ICT-systemen	Toegangsinformatie, nummerplannen, kwetsbaarheden.
Toekomstplannen, geheime onderhandelingen	Over aan- en verkopen, lopende onderhandelingen, aanbestedingen, conflicten etc.
Ondernemingsraad	Over organisatieveranderingen
Facilitair	Pacht- en huurcontracten

Bijlage 2 - voorbeelden van toepassingen en uitzonderingen

[3] Voorbeelden zijn precies dat: voorbeelden, indicaties. Ze gelden niet als regel of als wet.

Provincie Noord-Holland

IB-zakboekje[1] 'Werkplek'

Tactisch beleid informatiebeveiliging Provincie Noord-Holland

Versie 1.1

Status: **Definitief**
Opgesteld door: [redacted], dd 27 februari 2017
Vastgesteld door Stuurgroep I&I: positief, dd 23 maart 2017
Uitvoering: Directie CZ, Sector I&I

[1] IB = Informatiebeveiliging

IB-zakboekje 'Werkplek'

Algemeen

De moderne werkplek is al lang niet voor iedereen meer een plek aan een bureau bij de provincie. Thuis op de bank of in een coffeeshop kan even goed. Onderweg in de trein nog even een laatste mailtje bewerken, op zondagavond de agenda van maandag doornemen, vergaderingen 's ochtends thuis voorbereiden, het is voor velen al gewoon geworden.
'Werkplek' betekent nu nog meestal een volledig beheerd apparaat, maar wordt meer en meer beheerd *deel* van een apparaat en zelfs toegang vanuit een willekeurig, *niet beheerd apparaat* is gewoon geworden. Daarnaast verlenen we niet alleen vaste en tijdelijke medewerkers maar ook samenwerkingspartners en andere externen toegang.

De werkplek wordt dus meer en meer '*bewerk*plek': de manier om informatie van de provincie te *bewerken*: maken, inzien, aanpassen, verspreiden, verwijderen. Dat betekent:

- Het kan altijd en overal plaatsvinden;
- het gebruikte middel om te bewerken kan alle fysieke vormen aannemen: laptop, smartphone, tablet;
- het middel is niet altijd meer eigendom van de provincie;

De informatie en toepassingen van de provincie staan ondertussen ook niet allemaal meer op één plek, worden door meerdere partijen beheerd (denk SAAS) en zijn te benaderen vanuit heel Noord-Holland / Nederland.
Zoveel vrijheid vraagt om grenzen. De provincie moet haar verantwoordelijkheid over de informatie steeds kunnen blijven uitoefenen, dus ongewenste of onbedoelde interactie (toegang, besmetting, dataverlies) moet worden voorkomen.

Versiegeschiedenis

v1 - aangehouden stuurgroep I&I januari 2017 voor nadere toelichting door de CISO
v1.1 - vastgesteld door stuurgroep de stuurgroep I&I van 23 maart 2017

Doel van dit IB-Zakboekje

Met dit zakboekje stellen we kaders (tactisch beleid) die gebruikt kunnen (moeten) worden om de vele verschijningsvormen van werkplek te toetsen op veiligheid. Het laat veel vragen onbeantwoord, maar stelt de veiligheidskaders, waardoor ruimte blijft voor variatie, maar dan veilig.

Uitgangspunten voor de werkplek

Verantwoordelijke medewerkers

Wij beschouwen onze medewerkers als verantwoordelijke mensen die volwassen keuzes maken en dus goed zelf kunnen bepalen waar, waarmee en wanneer zij willen werken en ook met wie zij informatie delen. De werkplek moet die gedachte faciliteren.

'Binnen' versus 'buiten'

Door die mobiliteit, maar ook doordat we steeds vaker informatie opslaan en bewerken in de 'cloud', bij SAAS-diensten, is er geen vanzelfsprekend 'binnen' meer voor PNH. Dat vraagt om een nieuwe definitie.
Binnen vatten we daarom in dit document op als 'in een door PNH gecontroleerde omgeving'. Dat kan het PNH-netwerk zijn, of een Cloud-/SAAS-applicatie, of een beheerde werkplek die op een beheerde manier toegang zoekt.
Buiten is al het andere: onze burgers en partners, maar ook het internet met al zijn mogelijkheden, verlokkingen en bedreigingen.

Dreigingen

Het NCSC[2] stelt dat de werkplek, de persoonlijke apparaten van medewerkers het belangrijkste doelwit van aanvallen en misbruik worden. Het is de makkelijkste manier om spioneren, chanteren en zo geld te verdienen.

Verantwoordelijke Provincie

De provincie moet haar verantwoordelijkheid over haar informatie uitoefenen, dus ongewenste of onbedoelde interactie (toegang, besmetting, dataverlies) moet worden voorkomen. Zoiets gebeurt voor de gebruiker vaak ongemerkt.
Dat betekent dat de werkplek van de provincie niet geheel kan worden overgelaten aan de gebruikers. De medewerker moet gerust kunnen werken op de aangeboden werkplekken, zonder angst voor een besmetting of aanval die hem of de provincie kwaad kan berokkenen.

Uitwerking

De werknemer krijgt mogelijkheden om veilig tijd- en plaats- en apparaat-onafhankelijk te werken.

Hij/zij krijgt een set veilige mogelijkheden om *bewust en bedoeld* informatie uit te wisselen met 'buiten', terwijl onbewuste, onbedoelde uitwisseling van informatie tussen 'binnen' en 'buiten' onmogelijk is gemaakt'. Het middel om de veilige set te kiezen en werkend te leveren noemen we 'beheer'.

1. De beheerde werkplek kan zowel het hele apparaat (laptop, smartphone, tablet) als een deel ervan omvatten;
2. De beheerde opslag en de toegang tot applicaties en informatie is altijd beveiligd/versleuteld en voorzien van beveiliging naar de stand-van-de-techniek;

[2] NCSC – Nationaal CyberSecurity Center van het ministerie van Justitie

3. De toegang tot de werkplek is standaard mogelijk met behulp van een *sterk* wachtwoord
4. Alle toegang tot informatie en diensten is klasse- en risico-afhankelijk:
    a. Toegang tot vertrouwelijke informatie werkt alleen na aanvullende authenticatie;
    b. Sommige toepassingen zijn alleen te gebruiken van uit de beheerde omgeving.
5. Bij toegang vanuit een niet-beheerd apparaat zijn risicovolle handelingen of functies onmogelijk gemaakt, zoals bestanden up- of downloaden:
    a. is extra authenticatie noodzakelijk (2-factor);
    b. wordt een *afweging* gemaakt door de eigenaar welke views & functies benaderbaar zijn.
6. Verzenden, ontvangen, delen van informatie kan uitsluitend met behulp van beheerde PNH-voorzieningen, via de PNH-toegang tot 'buiten';
    a. Het gebruik van USB-sticks en andere opslag media is nog onderwerp van studie.

Toelichting

Tijd- en plaats-onafhankelijk

Of PNH-toepassingen en informatie ook van buiten Nederland benaderd moeten kunne worden is een zaak voor nadere risicoanalyse.
Buiten werktijden toegang bieden is eigenlijk al heel normaal geworden: in het weekeinde bereiden we ons al vaak voor op de maandag, 's avonds gaan we nog even door.

De geheel beheerde bewerkplek (ad 1)

De standaard PNH-werkplek is uitgerust met Windows10. Deze geeft volledige toegang tot alle applicaties en functies (ook de S-schijf) ongeachte je locatie of tijd van de dag. Ook applicaties die lokaal geïnstalleerde software vereisen werken hiermee. De verbinding met PNH applicaties en informatie (waar dan ook) is automatisch beveiligd en functioneel volledig toegankelijk.
We streven naar de mogelijkheid voor medewerkers om apps vanuit de Windows app-store te installeren[3].

Actieve beveiliging (ad 2)

Voor alle vormen van beheerde werkplekken geldt dat alleen actueel ondersteunde en gepatchte software wordt gebruikt en bescherming tegen virussen en andere kwaadaardige software actief is (volgens de 'stand_der_techniek'). Hiervoor worden de NCSC 'Beveiligingsrichtlijnen voor mobiele apparaten' toegepast.

[3] Hier gelden mogelijk beperkingen in verband met de veiligheid

Sterk wachtwoord / authenticatie (ad 3, 5)

Het wachtwoord telt tenminste 6 posities, waarvan tenminste één hoofdletter en één cijfer of bijzonder karakter.
De toegang tot vertrouwelijke gegevens en vanuit een niet-beheerde werkplek is 2-factor authenticatie noodzakelijk (in de praktijk het gebruik van een token).

Alle toegang en gebruik is klasse-afhankelijk (ad 4)

Toegang tot informatie met een hoge BIV-klassering of informatieklasse Vertrouwelijk/Geheim is alleen mogelijk gemaakt vanuit een beheerde omgeving, dus vanaf een geheel beheerde werkplek, of vanuit het beheerde deel van een eigen apparaat.
Toegang vanuit de niet-beheerde omgeving is soms mogelijk, maar dan beperkt tot alleen 'bekijken van informatie, niet bewerken, down- of uploaden.

De gedeeltelijk of niet beheerde bewerkplek (ad 5)

Om op je werkplek informatie van PNH te kunnen opslaan (up- en downloaden) zijn veiligheidsmaatregelen onmisbaar. Als het apparaat niet in beheer bij PNH), moet jij toestemming geven om software te installeren die een deel van het apparaat afschermt voor PNH-applicaties en informatie. Dit kan beperkt zijn tot je browser of een meer functies van je apparaat omvatten. Dit deel wordt vervolgens beheerd door PNH.

Om *alleen interactief* te werken met een applicatie, zonder dat je informatie uitwisselt *via de werkplek* kun je met een willekeurige internet-browser werken op een willekeurig apparaat, typisch jouw thuis-laptop, -smartphone of die van je oma ;-) Omdat we de beveiliging niet kunnen testen en niet beïnvloeden kun je geen informatie up- of downloaden.
Wil je een bestand verplaatsen (bijvoorbeeld om te delen met derden) dan zijn daarvoor veilige middelen van PNH beschikbaar, zoals Secure Filetransfer en e-Mail. Deze kun je natuurlijk ook vanuit een willekeurige browser bedienen.

PNH-beheerde voorzieningen tussen binnen en buiten (ad 6)

Daaronder verstaan we email en middelen om bestanden te delen en aan documenten te werken. Maar hieronder valt ook 'gewone' internet-toegang met Windows Explorer of Google Chrome. Ook al zit de werkplek vaak niet meer in een besloten domein (op een PNH-netwerk), verbinding met 'buiten' verloopt altijd via deze 'wasstraat', die met diverse middelen aanvallen en besmettingen blokkeert.

Externen

We verlenen ook toegang tot applicaties en informatie van PNH aan samenwerkingspartners en andere externen. Deze zullen van geval tot geval moeten worden beoordeeld, waarbij een risicoanalyse tot de juiste keuze voor toegang en werkplek moet leiden.

Toepasselijke IBI-maatregelen

De Interprovinciale Baseline Informatiebeveiliging[4] en de ISO27002 zijn geraadpleegd als inspiratiebron en ter verantwoording. Alle zakboekjes zijn beschikbaar op Plein, het intranet van Noord-Holland.

Bereik van dit beleid

Onder werkplek verstaan we alle hulpmiddelen die gebruikers toegang verschaffen tot toepassingen en informatie van Provincie Noord-Holland, hieronder begrepen 'vaste computers', laptops, tablets, smartphones en zelfs smartwatches, zowel in eigendom en onder beheer van de provincie alsook van derden en medewerkers.

De risico's – bedreigingen voor de werkplek

De werkplek was en is het kwetsbaarste element in de informatieketen, de zwakste schakel. Dat komt door de diversiteit, complexiteit, vele interactiemogelijkheden met de omgeving en -natuurlijk- de gebruiker. Het NCSC[5] waarschuwt (2017 en verder) voor de hoofdrol voor de werkplek bij aanvallen op de cloud, datagijzeling en spionage. De omgeving van de werkplek thuis en onderweg wordt ondertussen snel gevaarlijker door het 'internet der dingen' (IoT – Internet of Things) dat veel slecht beveiligde apparatuur verspreidt en oude, wijdverspreide aanvalstechnieken doet herleven.
Verder wordt Mobiele ransomware nu echt een probleem op grote schaal voor slecht beveiligde toestellen.

Vaststelling, uitvoering en beheer

Dit document is vastgesteld door de Stuurgroep I&I en voor uitvoering overgedragen aan PNH IT-beheer, vertegenwoordigd door de Sectormanager I&I.
Vaststelling en wijzing van de technische realisatie verloopt via wijzigingsbeheer van IT-beheer, waarbij de toepassing van de principes in dit document worden getoetst en geregistreerd.
De CISO houdt toezicht op de toepassing en werking van dit beleid. Revisie en aanvulling van dit beleid is een doorlopende verantwoordelijkheid van de CISO, die ook zorgt voor afstemming met de betrokkenen. Wijzigingen van de principes leidt tot opnieuw vaststellen van dit beleid door de Stuurgroep I&I.

Publicatie

Dit en alle andere IB-zakboekjes worden gepubliceerd op het 'Plein', het intranet van PNH en zijn vindbaar met de zoekterm 'IB-zakboekje'. Bij het opstellen zijn de informatiemanagers, adviseurs I&I, PNH IT-beheer en Fujitsu betrokken.

---

[4] Van toepassing zijn onderdelen uit de paragrafen 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.4.1, 9.4.2, 10.1.1, 12.1.2, 12.2.1, 12.3.1, 12.6.1, 12.6.2, 14.1.1, 14.2.2, over de onderwerpen toegangsbeveiliging, cryptografie, veilige bedrijfsvoering (beheerprocessen), eisen aan en acceptatie van informatiesystemen.

[5] NCSC = Nationaal CyberSecurity Center van het ministerie van Veiligheid en Justitie

Provincie Noord-Holland

IB-zakboekje 'Identiteiten, rollen en rechten' – beheersing van de toegang

Tactisch beleid informatiebeveiliging Provincie Noord-Holland

versie 1

Status: definitief
Redactie: Concern Information Security Officer
Vastgesteld door: Stuurgroep I&I
Datum: 15 juni 2017

IB-zakboekje 'Identiteiten, rollen en rechten'

IB-zakboekjes gaan over Informatiebeveiliging. Dit IB-zakboekje is een uitwerking van de Interprovinciale Baseline Informatieveiligheid (IBI) voor het onderwerp 'identiteiten, rollen en rechten' (hierna *IRR*) als tactisch beleid, de overbrugging van theorie naar praktijk.. De IBI is geraadpleegd als inspiratiebron en ter verantwoording. Alle IB-Zakboekjes zijn beschikbaar op Plein, het intranet van Noord-Holland (link).

Doel van dit zakboekje – beheersing van toegang & gebruik

De informatie en infrastructuur (ruimten, systemen en netwerken) van de provincie hebben waarde. Inbreuk op de integriteit of vertrouwelijkheid is ongewenst. Een van de belangrijkste maatregelen tegen die risico's is de beheersing van de toegang & gebruik: alleen toegang en gebruik met toestemming. Voor alle anderen is de toegang verboden en (bij voorkeur) onmogelijk gemaakt. In een organisatie met zoveel medewerkers, maar ook zoveel tijdelijke krachten moet je die rechten heel goed regelen.
Dit zakboekje levert principes en regels voor eigenaren, beheerders en gebruikers van informatie en informatiesystemen voor de beheerste toegang.

Bereik (scope)

Dit zakboekje gaat over de *toegang tot en het gebruik van informatie*, door wie en aan wie. Toegangsbeveiliging gaat in zowel de fysieke als in de virtuele wereld over 'deuren' die geopend mogen worden, maar ook over -als je dan eenmaal binnen bent- wát je dan mag doen.
De in dit zakboekje bedoelde rechten op informatie zijn: *maken, lezen, schrijven en verwijderen*.
De Principes en Uitwerkingen zijn zoveel mogelijk algemeen toepasselijk opgesteld en toepasbaar op de *virtuele én fysieke wereld*. Omdat informatiebeveiliging gaat over álle informatie onder verantwoordelijkheid van PNH, *ook die in 'Cloud-systemen'* en PNH-systemen onder beheer van derden. Het betreft de hele levenscyclus van identiteiten, rollen en rechten: van aanmaak, uitgifte, intrekken en beëindigen van identiteiten, rollen en rechten.
IRR heeft betrekking op alle personen én systemen die toegang vereisen tot systemen en informatie. Dit omvat eigen personeel in vast dienst, inhuurkrachten, deeltijdwerkers, externen. Het omvat ook partners van PNH die toegang tot informatie moeten hebben om de samenwerking te kunnen uitvoeren.
Buiten scope
IRR gaat over *identiteiten en hun recht van toegang* (= autorisatie), NIET over de 'sleutels' en NIET over de 'sloten'.

- Sleutels zijn de wachtwoorden, tokens, certificaten en zo meer. Het recht op gebruik wordt geregeld in IRR, keuze, uitgifte en toepassing wordt besproken in het Zakboekje 'Authenticatie'.
- Sloten zijn de beveiligingsfuncties in systemen, die de deur dichthouden of selectief openen voor mensen met een sleutel en met een recht. Deze worden besproken bij systeembeveiliging en fysieke beveiliging.

Beveiligingsprincipes voor 'IRR'

Basis

- Alle rechten voor toegang tot interne, intern vertrouwelijke en geheime informatie, systemen, diensten en fysieke infrastructuur en het feitelijk gebruik van die rechten zijn herleidbaar tot een unieke natuurlijke persoon;
- Alleen de eigenaar van een informatiemiddel of ruimte (of zone) kan daarvoor rechten uitreiken. Daartoe:
    - Worden natuurlijke personen uniek aan elektronische identiteiten gekoppeld;
    - Gebruiken identiteiten account(s), waaraan rechten worden gekoppeld;
    - Zijn accounts persoonlijk (aan één identiteit gekoppeld) en valt alle gebruik onder een gedragscode;
    - Worden alle registraties en gebruik periodiek getoetst;
    - Vervallen alle rechten bij beëindiging van de functie;
- Het IRR-proces heeft een eigenaar die toeziet op de werking en beslist over uitzonderingen op het proces.

Uitwerking

- Het HRM-proces & -register van PNH is de primaire bron van gecontroleerde identiteiten;
    - Door HRM mag ook worden gesteund op identificatie die eerder is uitgevoerd door derden;
    - Andere bronnen van identiteiten kunnen worden toegelaten na een risicobeoordeling en formeel besluit;
- Rollen worden waar mogelijk ingezet om rechten efficiënt aan personen en informatiemiddelen te koppelen;
- De benoemde eigenaar stelt voor zijn toepassing/informatiemiddel een autorisatiematrix op, die:
    - de relatie tussen rollen en rechten binnen de toepassing/informatiemiddel vastlegt;
    - een analyse omvat van mogelijke rechtenconflicten die worden bestreden met effectieve functiescheiding;
    - 'gevoelige' rollen identificeert (met meer dan gemiddelde rechten, zoals beheerders).
    - daarbij het principe 'Open, tenzij' hanteert zoals uitgewerkt in het IB-Zakboekje Classificatie van PNH
- Rollen en rechten worden altijd uitgereikt voor een eindige periode en worden tenminste 3-jaarlijks herbevestigd;

- Functiewijzigingen en -einde leiden automatisch tot intrekken van alle rechten (en her-uitgifte van alle *relevante* rechten).
- Alle uitgereikte relaties tussen identiteiten, rollen en rechten, zowel historisch als actueel worden vastgelegd in een register.
- Jaarlijks vindt controle plaats op alle *gevoelige* rollen en rechten en jaarlijks vindt een steekproef plaats op de overige rollen en rechten;
- Het proces van identiteiten, rollen en rechten wordt onregelmatig (maar minstens 1 x per 3 jaar) door een auditor beoordeeld op opzet, bestaan en werking;
- Gebruik van rollen en rechten in systemen met een BIA-score waar voor vertrouwelijkheid of integriteit tenminste één 'H' is gescoord en alle systemen met persoonsinformatie leggen alle gebruik van rechten vast in een beveiligd log-bestand.

Uitwerking voor fysieke toegangsbeheersing

- Een zone of ruimte in een van de gebouwen van PNH is op dezelfde manier te beschouwen als een informatiesysteem heeft een eigenaar namens PNH, die:
    - een autorisatiematrix aanlegt, wanneer en door wie toegang tot een ruimte mogelijk/noodzakelijk is;
    - bepaalt wanneer alleen begeleide toegang toegestaan is;
    - voor kritische ruimte een register bijhoudt van verleende toegang (fysieke of elektronisch);
    - bepaalt wanneer zichtbare identificatie wordt gedragen;

Randvoorwaarde 'eigendom'

Zonder heldere opvatting van het concept 'eigendom' is een effectieve beheersing van de toegang niet mogelijk. Deze randvoorwaarde kent in relatie tot IRR de volgende verschijningsvormen:

- Eigenaar van het proces van IRR: zorgt voor implementatie van het proces, houdt toezicht op de werking (audits, rapportages), beslist over uitzonderingen, evalueren van storingen.
- Eigenaar van de identiteiten: zorgt voor identificatie van de natuurlijke personen en koppeling aan een unieke (elektronische) identiteit (bijvoorbeeld het personeelsnummer);
    - Bij het vertrouwen op door externen geïdentificeerde personen is een 'eigenaar' nodig van die relatie in PNH. De relatie wordt gezien als een ''; informatiemiddel' en geregistreerd en beheerd als ieder ander informatiemiddel.
- Eigenaar van de informatiemiddelen & ruimten: ieder informatiemiddel (systeem, verzameling, dienst etc.) moet een benoemde eigenaar hebben die zorg draagt voor aanschaf, beheer en onderhoud, wijzigingen, toegang en gebruik;

- Eigenaar van het middel en het verleende recht: de medewerker heeft wel de verantwoordelijkheid om middel en recht zorgvuldig te gebruiken, melding te doen van vermoeden van compromittering en verlies.
    - Voor zowel interne als externe medewerkers

Bijzondere situaties & uitzonderingen

Systeembeheerders

Systeembeheerders met bijzondere verantwoordelijkheid en taken doen al hun niet-kritische werk onder hun 'gewone' werknemersaccount, alleen voor beheer-activiteiten waarbij meer rechten noodzakelijk zijn, wordt met beheeraccounts gewerkt, waarbij de handelingen altijd herleidbaar moeten zijn naar de individuele beheerder.

Functionele of anonieme accounts (indirect-persoonsgebonden)

Niet persoonsgebonden ('functionele' of 'anonieme') accounts vormen -alleen na toestemming van de CISO- een *gedelegeerde* vorm van *rechtenuitgifte* & toegang. Anonieme/functionele toegang is niet toegestaan.
Er is een door de 'eigenaar' van het de te benaderen systeem een door hem benoemde 'eigenaar' van het functioneel account, die gebruik door anderen toestaat en registreert na verificatie van de identiteit. Hij/zij is verantwoordelijk voor de aan het account toegekende rechten en controleert periodiek of het gebruik en de registratie beheerst wordt.
Het account mag steeds maar voor een vooraf bepaalde duur geactiveerd worden onder volgende voorwaarden:

- de beheerder voldoende middelen heeft om de identiteit van de aanvrager te verifiëren en
- de identiteit van de gebruiker en het bewijs daarvan registreert.

Identificatie eerder uitgevoerd door derden

In onze sterk ver-netwerkte en flexibele wereld kan niet meer verondersteld worden dat iedereen via de hoofdpoort elke dag komt en gaat. Daarom is het voor toegang tot applicaties en informatie noodzakelijk te steunen op identiteiten die door anderen zijn geverifieerd. Bekende voorbeelden hiervan zijn DigiD, eID (van de banken), eHerkenning etc.
Daarnaast kan gesteund worden op de identiteitscontrole en rechtentoewijzing van partners of andere overheidsorganisaties. Dit vergt maatwerk per keer, waarbij we moeten kijken naar de basis voor het vertrouwen: kwaliteit van de identificatie die is uitgevoerd, van het gebruikte middel (wachtwoord, SMS) etc.
Deze beoordeling wordt (mede) uitgevoerd door de CISO en het besluit over het gebruik van de identiteiten wordt genomen door de eigenaar van het te banderen systeem.

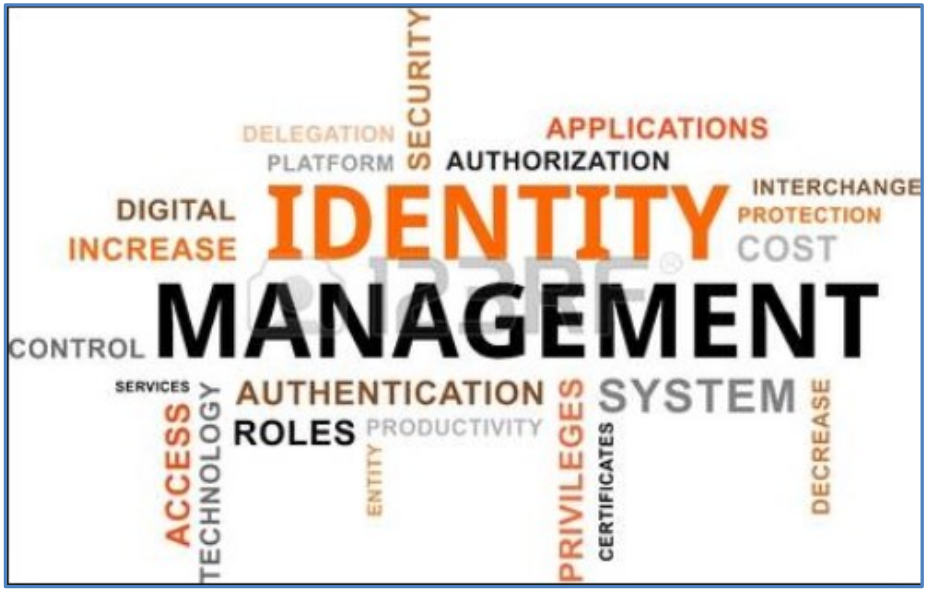
Casussen

- 2016-09 - De repro-kamer heeft enkele anonieme accounts, voor uitzendkrachten die maar één dag komen werken. De afspraak is dat zij activering van een account aanvragen, die maximaal een dag mag duren, bij Fujitsu servicedesk. De identiteit van de uitzendwerker wordt gecontroleerd door de Repro-teamleider, die deze doorgeeft aan Fujitsu. De naam wordt vastgelegd bij het 'ticket' dat de openstelling aanvraagt. Het account wordt max de dag gebruikt en sluit automatisch weer de volgende nacht af.

Totstandkoming, vaststelling, uitvoering en beheer van dit zakboekje

Totstandkoming

De totstandkoming en onderhoud van alle zakboekjes is teamwerk. Informatiemanagement, adviseurs I&I, CISO, I&I-beheer en relevante business-vertegenwoordigerszijn betrokken. Dit document is de vertaling van de eisen uit de Interprovinciale Baseline Informatiebeveiliging naar risicogebaseerde en passende keuzes van PNH. IB-zakboekjes zijn 'levende documenten'.



Uitvoering

Dit document is vastgesteld door de Stuurgroep I&I en voor uitvoering overgedragen aan PNH IT-beheer, vertegenwoordigd door de Sectormanager I&I.
Vaststelling en wijzing van de technische ondersteuning van dit beleid verloopt via wijzigingsbeheer van IT-beheer, waarbij de toepassing van de principes in dit document worden getoetst en geregistreerd.
De CISO houdt toezicht op de toepassing en werking van dit beleid.

Beheer

Revisie en aanvulling van dit beleid (alleen uitwerking en voorbeelden) is een doorlopende verantwoordelijkheid van de CISO, die ook zorgt voor afstemming met de betrokkenen.
Wijzigingen van de principes leiden noodzakelijk tot opnieuw vaststellen van dit beleid door de Stuurgroep I&I.

Publicatie & communicatie

Alle IB-zakboekjes worden gepubliceerd op 'Plein', intranet van PNH en zijn vindbaar met de zoekterm 'IB-zakboekje'.
De rollen en verantwoordelijkheden m.b.t de zakboekjes worden gecommuniceerd naar alle betrokken rolhouders uit het governance-beleid van PNH.

Toepasselijke IBI-maatregelen

Van toepassing zijn van de IBI en de ISO27002 onderdelen uit de volgende paragrafen
9.1 'Bedrijfseisen voor toegangsbeveiliging' → identiteiten controle en registratie, in-, door- en uitstroom
9.2 'Beheer van toegangsrechten van gebruikers' → registratie, aanmaak, intrekken, vergelijken
12.1.4 'Scheiding van ontwikkel-, test- en productieomgevingen' → inloggegevens (account on/of wachtwoord) moeten tussen omgevingen verschillen

Andere bronnen

- Informatiebeveiligingsbeleid PNH 2012
- Governance van Informatiebeveiliging dd 18 april 2017
- Addendum IB-beleid: toepassing van de Interprovinciale Baseline Informatiebeveiliging

Van: [redacted]
Verzonden: vrijdag 6 oktober 2017 10:18
Aan: [redacted]
CC: [redacted]
Onderwerp: offerteaanvraag i.v.m. cybersecurity Abdijtunnel

Geachte heer [redacted]

Wij hebben op 18 juli 2017 een gesprek gehad over de aanvullende wensen van de provincie Noord-Holland op het gebied van cybersecurity voor de Abdijtunnel. Bij dit gesprek waren dhr. [redacted] en dhr [redacted] (ingehuurde deskundige door PNH) aanwezig. Wij hebben aangegeven dat wij u een verzoek doen om hiervoor een offerte uit te brengen.

1. Aanleiding offerteaanvraag

In het kader van de renovatie Abdijtunnel heeft [redacted] een Cybersecurityplan Abdijtunnel aangeleverd. Hieruit is gebleken dat op het gebied van cybersecurity voor de Abdijtunnel verbetermaatregelen noodzakelijk zijn teneinde te bewerkstelligen dat de provincie voldoet aan alle relevante eisen op het gebied van Informatieveiligheid.

2. Doel offerteaanvraag

Informatieveiligheid en cybersecurity gaat over de betrouwbaarheid van de informatievoorziening van de provinciale organisatie, en heeft tot doel risico's tot een acceptabel niveau terug te brengen. Doel is om te komen tot ingevulde en geborgde proces- en systeemdoelen met betrekking tot de cybersecurity Abdijtunnel door Engie en de provincie Noord-Holland. Deze proces- en systeemdoelen vormen een geïntegreerd en consistent geheel met elkaar. Het borgen van deze doelen tezamen met een actueel cybersecurity plan heeft als doel het voorkomen van gevaar of schade veroorzaakt door verstoring, uitval en misbruik van ICT en IA.

3. Vraagstelling

Maatregelen

Naar aanleiding van de beoordeling van het "Cybersecurityplan Abdijtunnel" zijn er door de provincie proceseisen, systeemeisen en beheersdoelen op het gebied van Cybersecurity voor de Abdijtunnel opgesteld. Deze zijn te vinden in de bij deze mail behorende bijlage A.

Uw organisatie dient een plan op te stellen waarin wordt aangegeven wat het uitwerken en implementeren van deze proceseisen, systeemeisen en beheersdoelen kost in tijd en geld.
Daarbij dient u de afzonderlijke eisen en eisnummers te specificeren (eveneens in tijd en geld) en dient u aan te geven wat de implementatie voor impact heeft voor de Abdijtunnel (beschikbaarheid en betrouwbaarheid). Tevens dient een totaalbedrag te worden aangegeven.

Wij merken het volgende op: in bijlage A wordt bij enkele proces- en systeemeisen aangegeven dat bepaalde zaken conform de richtlijnen van de provincie Noord-Holland ingericht moeten worden. In deze gevallen kunt u de richtlijnen zoals uitgevraagd bij de opdracht voor de "24 uurs- Centrale Bediening" aanhouden, of de Rijkswaterstaat richtlijnen hierover. Deze richtlijnen zijn al bij u al bekend.

Borging en onderhoud
De getroffen verbetermaatregelen dienen in de onderhoudsperiode van de Abdijtunnel op niveau te worden gehouden door [redacted] De basis hiervoor is het onderhoudscontract. Wij verzoeken u om de door u aangeven maatregelen op te nemen in dit onderhoudscontract en de kosten daarvan inzichtelijk te maken zoals op de wijze zoals hiervoor is aangegeven.

4. Lijst met eisen

Alle eisen en eisnummers uit bijlage A dienen afzonderlijk uitgewerkt te worden in termen van tijd en geld. De volgorde van uitwerking dient gelijk te zijn aan de aangeleverde volgorde in bijlage A.
U dient daarbij tevens aan te geven wat de impact is voor de Abdijtunnel (beschikbaarheid, betrouwbaarheid).
Als het implementeren van eisen afzonderlijk geen probleem oplevert maar een mogelijke combinatie of opeenvolging van implementaties wel, dan dient u daarvan een inschatting van de impact te geven (beschikbaarheid en betrouwbaarheid Abdijtunnel).
Zoals eerder is aangegeven dienen de getroffen verbetermaatregelen in de onderhoudsperiode van de Abdijtunnel op niveau te worden gehouden door [redacted] Wij verzoeken u om de door u aangeven maatregelen op te nemen in dit onderhoudscontract en de kosten daarvan inzichtelijk te maken zoals op de wijze zoals hiervoor is aangegeven.

5. Offerte

Uw digitale offerte, onder vermelding van het kenmerk van de provincie (cybersecurity Abdijtunnel), dient uiterlijk op 13 november 2017 door mij ontvangen te zijn. De offerte dient te worden verzonden aan mw. [redacted] en dhr. [redacted], e-mailadres [redacted]

Voor vragen kunt u contact opnemen met mw. [redacted]

Voorwaarden offerte:

1. De offerte dient een gestanddoeningstermijn te hebben van 60 dagen. Tijdens deze periode heeft uw offerte het karakter van een onherroepelijk aanbod.
2. De provincie Noord-Holland neemt vrijblijvende aanbiedingen niet in behandeling.
3. Aan het uitbrengen van een offerte zijn voor de provincie Noord-Holland geen kosten verbonden ongeacht of de offerte tot het sluiten van een overeenkomst zal leiden.
4. Op alle offerteaanvragen van de provincie Noord-Holland zijn de Algemene Inkoopvoorwaarden Provincies 2015 voor leveringen en diensten, vastgesteld door Gedeputeerde Staten van de provincie Noord-Holland op 19 mei 2015, van toepassing, met uitsluiting van de algemene voorwaarden van de leverancier of opdrachtnemer. Deze Algemene Inkoopvoorwaarden Provincies 2015 voor leveringen en diensten zijn te downloaden op http://www.noord-holland.nl/Over_de_provincie/Inkoop_en_aanbesteden/Documenten/Algemene_inkoopvoorwaarden.org. Bij het indienen van uw offerte dient u expliciet in te stemmen met de digitale terhandstelling van deze voorwaarden.
5. De provincie Noord-Holland behoudt zich het recht voor om nadere toelichting te vragen op de uitgebrachte offerte(s).

6. Mondelinge mededelingen, toezeggingen of nadere afspraken hebben geen rechtskracht tenzij deze door beide partijen schriftelijk zijn bevestigd.
7. Aanbiedingen dienen te zijn gesteld in het Nederlands. Correspondentie zal eveneens in het Nederlands geschieden.
8. Ontvangst van uw offerte houdt geen aanvaarding van uw aanbod in en leidt niet tot enige verbondenheid van de provincie Noord-Holland. In dat geval is er ook geen enkele verplichting tot het vergoeden van welke schade of kosten dan ook. Een overeenkomst komt slechts tot stand nadat de leverancier c.q. opdrachtnemer een schriftelijke bevestiging van de provincie Noord-Holland heeft ontvangen in de vorm van een opdrachtbrief of een door provincie Noord-Holland ondertekend contract.
9. De Provincie heeft zich gecommitteerd om met ingang van 2015 100% duurzaam in te kopen, omschreven als 'maatschappelijk verantwoord inkopen' (MVI). Onder duurzaam verstaat de provincie: minst belastend voor milieu, klimaat, mens en leefomgeving. Voor dit doel hanteert de provincie de door PIANOo / Rijksdienst voor Ondernemend Nederland (RVO) opgestelde milieucriteria voor zes clusters van producten en diensten. Uitgangspunt is dat door inschrijving op deze offerteaanvraag gegadigde verklaart dat de gevraagde werken, leveringen en/of diensten ten minste voldoen aan de minimum eisen van het bijbehorende milieucriteriadocument. Zie voor de lijst clusters met productgroepen waarvoor milieucriteriadocumenten zijn opgesteld de website van PIANOo http://www.pianoo.nl/duurzaaminkopen/productgroepen.
   Indien van toepassing voor de voorliggende opdracht treft u de minimum eis(en) onder 'milieu minimum eisen' in de bijlage bij deze offerteaanvraag aan.
10. De Provincie ambieert waar mogelijk, tegen afgewogen kostenniveau, een hoger duurzaamheidsniveau. Bovenop de minimum duurzaamheidseisen (punt 9) kan aanbesteder voor deze inkopen één of meer milieuwensen toepassen om meer maatschappelijke waarde te creëren. Indien van toepassing voor de voorliggende opdracht treft u de door aanbesteder gekozen milieuwensen aan in de bijlage bij deze offerteaanvraag.

Door het indienen van uw offerte stemt u in met alle in deze offerteaanvraag genoemde voorwaarden.

Wij zien uw offerte graag tegemoet.

Met vriendelijke groet,

mw. [redacted]
technisch adviseur /adviseur tunnelveiligheid
Beheerstrategie en Programmering Infrastructuur

T [redacted]
Houtplein 33 2012 DE Haarlem
[redacted]
www.noord-holland.nl

Provincie Noord-Holland