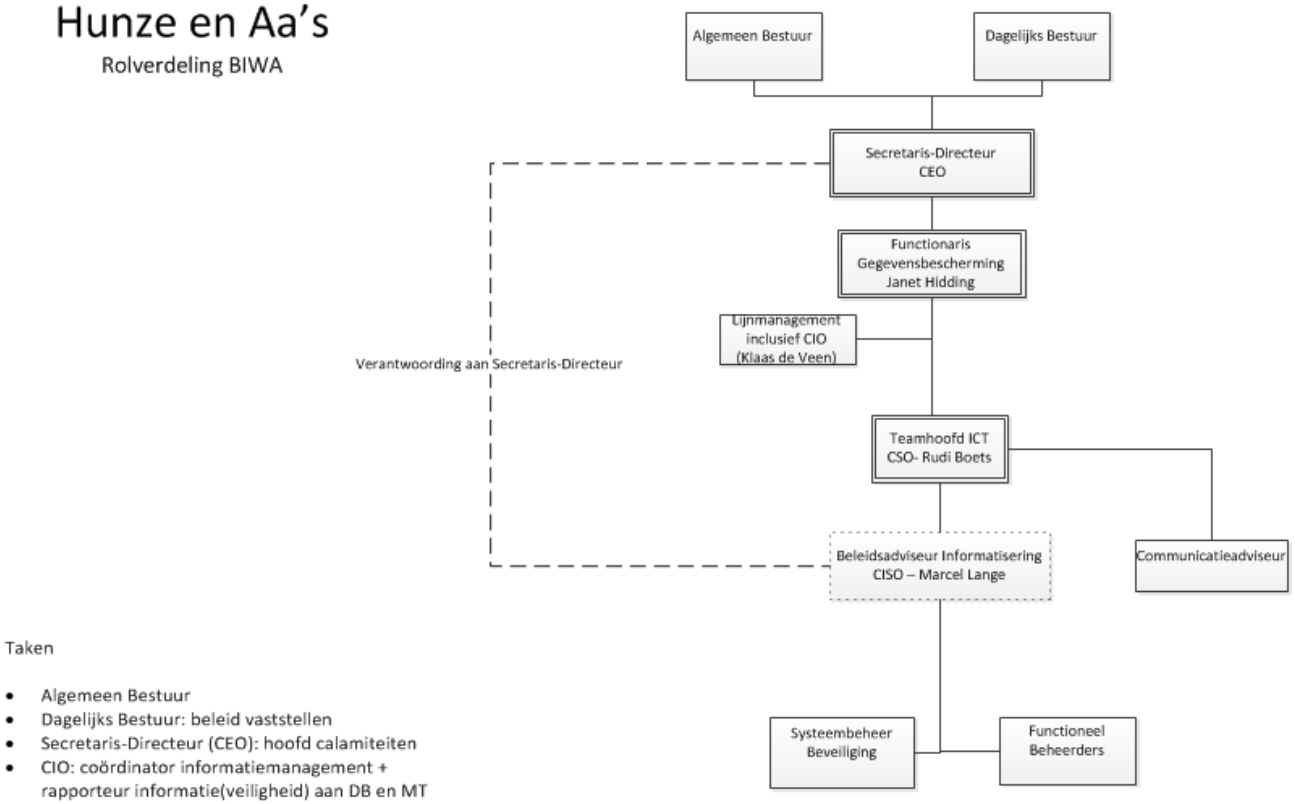
Bijlage 2 Beveiligingsplan

Informatiebeveiliging

De verantwoordelijkheid voor informatiebeveiliging ligt bij het dagelijks bestuur. In de DB-vergadering van 31 augustus 2015 is stilgestaan bij een aantal strategische onderdelen van informatiebeveiliging. De organisatie van informatiebeveiliging, waaronder verantwoordelijkheden, taken en bevoegdheden zijn door het dagelijks bestuur vastgesteld. Ook zijn de verantwoordelijkheden op het gebied van informatiebeveiliging toegewezen. Toegezegd is om de resterende onderdelen van het strategisch informatiebeleid c.q het beveiligingsplan in een later stadium ter vaststelling voor te leggen. Deze onderdelen liggen thans voor.

De rolverdeling zoals deze door het dagelijks bestuur is vastgesteld ziet er schematisch als volgt uit:



Taken

- Algemeen Bestuur
- Dagelijks Bestuur: beleid vaststellen
- Secretaris-Directeur (CEO): hoofd calamiteiten
- CIO: coördinator informatiemanagement + rapporteur informatie(veiligheid) aan DB en MT
- CISO: hoofd informatiebeveiliging + rapporteur informatieveiligheid aan secretaris-directeur
- Systeembeheer Beveiliging: technische beveiliging van systemen + back-ups
- Functioneel beheerders: technisch beheer en beveiliging van applicaties + databases
- Lijnmanagement: hoofden van afdelingen/teams, bovenste laag binnen de desbetreffende afdeling

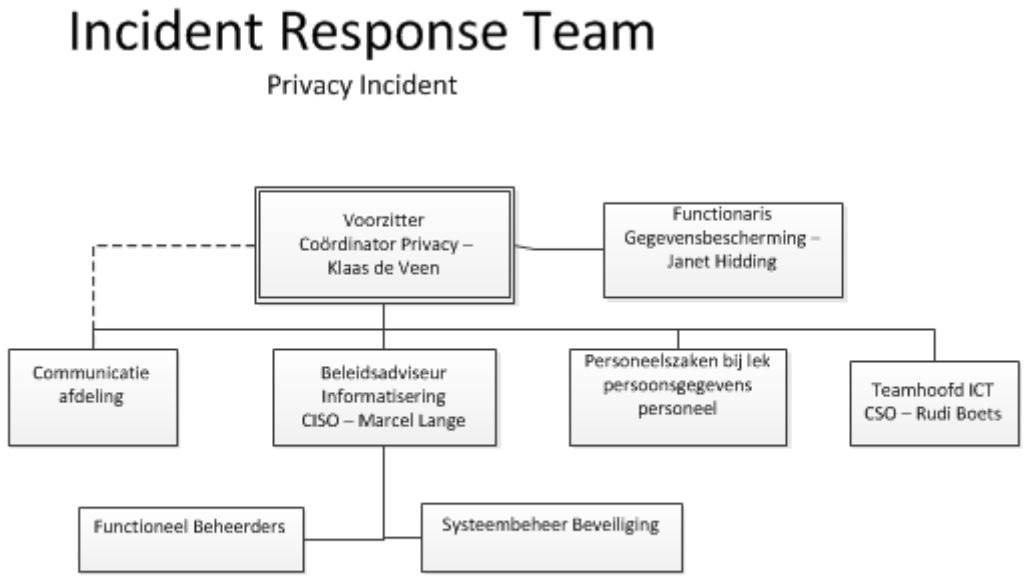
Calamiteitenplan ICT en privacy

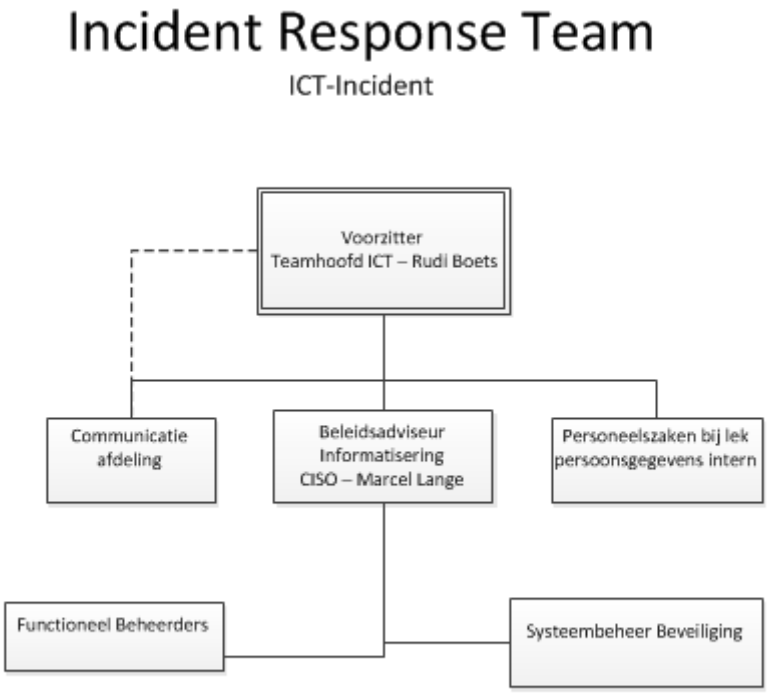
Om adequaat te kunnen reageren op een incident met een grote impact, is het belangrijk een team van experts bij elkaar te kunnen krijgen. Dit team kan door zijn expertise reageren op verschillende incidenten rondom informatieveiligheid, zoals een privacy-incident of een ICT-incident. De ICT-incidenten kunnen uiteenlopen van een datalek tot een virusuitbraak. Bij het verlies van hardware (apparatuur zoals Ipad/USB met bedrijfsgegevens) of documenten geldt het Incident Response Team van ICT-incidenten. Wanneer een incident van dusdanige grootte is dat het imagoschade en bedrijfsschade kan veroorzaken wordt opgeschaald op het niveau van dijkgraaf en secretaris-directeur. Bij incidenten wat een openbaar karakter heeft wordt het team communicatie bijgeschakeld. De verschillende soorten incidenten hebben elk een eigen voorzitter, maar de basis van deelnemers aan het Incident Response Team verandert niet.

De officiële naam voor een Incident Response Team is een CERT (Computer Emergency Response Team). In Nederland was één grote CERT voor de overheid, genaamd GOVCERT. De GOVCERT is nu overgegaan in het NCSC (National Cyber and Security Center).

De standaard bezetting van het Incident Response Team is de CISO, CSO, Systeembeheer, Functioneel Beheerders (afhankelijk van incident en betrokken applicatie), de FG (bij privacy incidenten) en de CIO (afdelingshoofd PFCI) , afhankelijk van het soort incident. Bij een ICT-incident is het teamhoofd ICT de voorzitter, bij een Privacy Incident is de CIO de voorzitter en bij het verlies van Hardware of documenten het teamhoofd ICT of de secretaris-directeur bij een escalatie.

In twee schema's is de bezetting van een crisisteam uitgewerkt. De opzet en werkwijze is overeenkomstig onze calamiteitenorganisatie hoog water georganiseerd.





In november en december 2015 is een test uitgevoerd met het ICT calamiteitenplan. In deze maanden is de organisatie op de hoogte gesteld van het calamiteitenplan en de procedures zoals deze gaan gelden. Alle meldingen komen eerst binnen bij de CISO. Deze gaat aan de hand van het hiervoor aangegeven schema bepalen wie betrokken moeten worden in het crisisteam. Alle documenten voor het calamiteitenplan worden in 2016 in een map in de crisiskamer/DB-kamer opgeslagen. De CISO is verantwoordelijk voor het actueel houden van dit plan. Daarbij wordt ook overleg gepleegd met onze functionaris gegevensbescherming omdat het calamiteitenplan ook moet werken voor privacy-incidenten. In 2016 wordt het calamiteitenplan verder uitgewerkt en operationeel gemaakt.

Beveiligingsplan
Strategische uitgangspunten en randvoorwaarden

De strategische uitgangspunten en randvoorwaarden omvatten twee dingen. Allereerst moet worden geïnventariseerd in hoeverre het Waterschap Hunze en Aa's risico's loopt op het gebied van informatiebeveiliging. Dat is uitgezocht door middel van een risico inventarisatie en evaluatie, welke in de beveiligingswereld ook kan worden uitgevoerd als een A&K analyse (afhankelijkheid en kwetsbaarheden analyse). Deze A&K analyse voeren we in 2016 uit. Daarnaast omvat het informatiebeveiligingsbeleid een, voor het Waterschap Hunze en Aa's, geschikte set aan maatregelen die volgen vanuit de Baseline Informatiebeveiliging Waterschappen (BIWA) en vanuit de huidige en toekomstige wet- en regelgeving. Daarbij geldt het principe 'pas toe of leg uit'. Daarmee wordt bedoeld dat een waterschap specifieke maatregel, zoals deze beschreven is in de BIWA, letterlijk moet worden geïmplementeerd in de organisatie. Dat kan worden gedaan met behulp van een beleidsstuk waarin deze letterlijk is opgenomen of een notitie in het informatiebeveiligingsplan waarin aangetoond is dat de maatregel is toegepast, maar wel is aangepast op de organisatie en de cultuur die heerst binnen de organisatie. Het uitleggen dat een specifiek risico wordt geaccepteerd valt daar ook onder.

Doel van informatiebeveiligingsbeleid

Het doel van informatiebeveiliging is het hebben van een palet aan maatregelen om onze kritieke systemen, informatie en persoonsgegevens te beschermen en een datalek te voorkomen. Per 1 januari 2016 is de Meldplicht datalekken in werking getreden en is Wbp op een aantal punten gewijzigd. De Wbp vereist van de verantwoordelijke (DB) dat deze een passende technische en organisatorische maatregelen neemt om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. Iedere inbreuk op deze beveiliging van persoonsgegevens wordt een 'datalek' genoemd. Een dergelijke inbreuk kan bestaan uit:

- Tekortschietende beveiligingsmaatregelen;
- Beveiligingsmaatregelen die teniet worden gedaan of worden omzeild;
- Niet adequate of niet vakkundig toegepaste beveiliging door de verantwoordelijke zelf;
- Menselijke fouten van ondergeschikten van de verantwoordelijken (bijv. verlies van een usb-stick).

In de gewijzigde Wbp is een meldplicht opgenomen voor datalekken. Een datalek moet worden gemeld bij de AP en de betrokkene(n). Er gelden hiervoor verschillende voorwaarden. Soms kan melding achterwege blijven. Over de mogelijkheid van het opleggen van boetes is hiervoor ingegaan. Daarnaast kan iedereen die als gevolg van het niet-naleven van de Wbp door de verantwoordelijke (DB) schade lijdt, deze schade verhalen op de verantwoordelijke.

Cyberincidenten

Er is een wetsvoorstel in behandeling bij de Tweede Kamer waarin de verplichting is opgenomen om digitale veiligheidsincidenten vertrouwelijk te melden bij het Nationaal Cyber Security Center (NCSC). Het NCSC is ondergebracht bij de Directie Cyber Security (DCS), onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), en valt onder verantwoordelijkheid van het ministerie van Veiligheid en Justitie.
De vertrouwelijke meldplicht moet gaan gelden voor alle organisaties die onderdeel uitmaken van de vitale informatiestructuur. De drinkwaterbedrijven vallen hieronder alsmede Rijkswaterstaat.
De meldplicht geldt voor onderdelen van de vitale infrastructuur binnen de sectoren, energie, gas, kernenergie, drinkwater, telecom, transport, financiën en overheid.

Informatiebeveiligingseisen en normen

De eisen en normen die gelden voor het Waterschap Hunze en Aa's worden voornamelijk in kaart gebracht door de A&K-analyse (afhankelijkheden en kwetsbaarheden). Tevens heeft een risico inventarisatie en evaluatie plaatsgevonden welke is aangevuld met een privacy impact analyse (zie hieronder). Beide instrumenten hebben tot doel gehad om de kritieke processen, systemen en de handelingen van medewerkers in kaart te brengen om te kunnen beoordelen waar op moet worden ingezet in het informatiebeveiligingsplan en beleidsnotities.

Frequentie van evaluatie informatiebeveiligingsbeleid

Om informatiebeveiligingsbeleid zo effectief mogelijk te laten zijn, moet jaarlijks worden geëvalueerd of het informatiebeveiligingsbeleid nog actueel is. Wanneer dat niet het geval is, moet daar op worden geïnvesteerd. De verantwoordelijke voor de evaluatie is de CISO (Beleidsadviseur informatisering/Architect). Deze koppelt zijn bevindingen vanuit de evaluatie terug aan de CSO

(teamhoofd ICT). Jaarlijks wordt door de CSO een rapportage opgesteld in samenwerking met de CISO, welke wordt opgenomen in de jaarrapportage van het Waterschap Hunze en Aa's.

Bevordering van beveiligingsbewustzijn

Om informatiebeveiliging effectief te laten zijn, begint de investering bij de individuele medewerker. Er wordt jaarlijks, in minimaal één sessie, aandacht besteed aan informatiebeveiliging en het beveiligingsbewustzijn van de individuele medewerker in de verschillende afdelingen.
Naast het beveiligingsbewustzijn zal ook privacybewustzijn worden meegenomen. Omdat al eerder is afgesproken om een dergelijk traject te doorlopen waar het gaat om het onderwerp integriteit zal ook koppeling met dit onderwerp plaatsvinden.
Ten aanzien van informatieveiligheid is de week van Alert Online, een periode van twee weken waarin de overheid veel aandacht besteed aan veiligheid op het internet en de omgang met mobiele media, daarvoor een geschikt moment. De reden daarvoor is dat de overheid in die periode veel campagnemateriaal beschikbaar stelt. Tevens wordt via het intranet aandacht besteed aan informatiebeveiliging. Eén tot twee maal per maand wordt er een klein stukje op het intranet geplaatst over een specifiek onderwerp zoals phishing, veiligheid van een smartphone, etc.

Aldus vastgesteld in de vergadering van het dagelijks bestuur op 18 april 2016.

Harm Küpers
secretaris-directeur

Alfred van Hall
dijkgraaf