INFORMATIE-BEVEILIGINGSBELEID

GEMEENTE AA EN HUNZE 2018-2019

Colofon

Naam document
Strategisch informatiebeveiligingsbeleid gemeente Aa en Hunze 2018-2019-v*2.5.*docx

Versienummer
2.5

Classificatie
Bedrijfsvertrouwelijk

Versiedatum
december 2018

Versiebeheer
Het beheer van dit document berust bij de CISO van de gemeente.

Versie	Wijziging	Datum wijziging	Auteur
1.0	Creatie, kopie van IBD	december 2013	A.Bijvoet
1.1	Diverse kleine wijzigingen inhoud; incl. versiebeheer	februari 2014	A.Bijvoet
1.11	Figuur 1 aangepast aan rollen	maart 2014	A.Bijvoet
1.12	Tekstuele aanpassingen	april 2014	E.Muntinga
1.13	Invulling geven aan de beveiliging voor de gemeente Aa en Hunze	januari 2015	E.Muntinga
1.14	Beleid afstemmen met Assen en Tynaarlo	maart 2015	E.Muntinga
2.0	Geplande herziening van het strategisch Informatiebeveiligingsbeleid	september 2018	A.Bijvoet
2.1	Verwerken opmerkingen Edwin Muntinga (snelle versie DigiD)	september 2018	A.Bijvoet
2.2	Verwerken opmerkingen Marcel en Aaldert (snelle versie DigiD)	september 2018	A.Bijvoet
2.3	Concept voor College (snelle versie DigiD)	oktober 2018	A.Bijvoet
2.4.1	Verwerken opmerkingen Aaldert, Edwin en Bert, Wouter	november 2018	A.Bijvoet
2.4.2	Aanpassingen nav. overleg directie team	december 2018	A. Bonder
2.5	Tekstuele wijzigingen consistentiecheck	december 2018	E.Muntinga

Inhoud

1 Voorwoord

Voor u ligt de tweede versie, voor de periode 2018-2019, van het strategisch informatiebeveiligingsbeleid van de gemeente Aa en Hunze.

Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging. Deze uitgangspunten hebben een sterk normerend karakter en toepassingsmogelijkheden weer. Met dit document kan de gemeente verdere in- en aanvulling geven aan haar tactisch en operationeel beleid.

Dit strategisch beleidsdocument is de kapstok voor de verdere professionalisering van informatiebeveiliging. Het ondersteunt het Collegeprogramma en is afgeleid van het strategisch informatiebeleid van de gemeente Aa en Hunze en onderdeel van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Het legt de basis voor het vakgebied 'informatiebeveiliging' binnen de gemeente Aa en Hunze.

Dit document in strategisch van aard. Het bevat, naast de organisatie van informatiebeveiliging, geen specifieke inrichtingsvoorschriften of werkwijzen, acties en technieken.
Onderdeel van dit document is een beheerstructuur (inrichting) voor informatiebeveiliging, waarmee verantwoordelijkheden voor informatiebeveiliging worden belegd en informatiebeveiliging wordt ingebed in de reguliere planning- en control cyclus binnen de (kwaliteit handhaving van de) bedrijfsvoering processen.

Omdat naar verwachting vanaf 2020 de Baseline Informatiebeveiliging Overheid (BIO, zie[1]) de BIG formeel vervangt, is de geldigheid van dit document beperkt tot en met 2019.

[1] BIR + BIG + BIWA + IBI = BIO. BIR: baseline informatiebveiliging rijk BIWA: baseline informatiebeveiliging voor de waterschappen IBI interprovinciale baseline informatiebeveiliging

2 Leeswijzer

2.1 Doel
Dit document geeft algemene beleidsuitgangspunten over informatiebeveiliging van de gemeente.

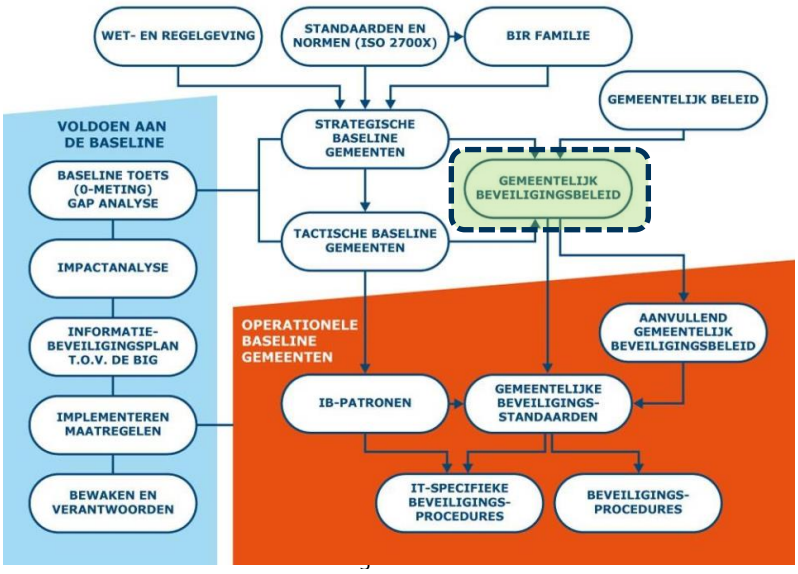
2.2 Doelgroep
Alle in- en externe medewerkers van de gemeente en digitale ketenpartners (cloud leveranciers).

2.3 Indeling document
Vanwege de leesbaarheid is dit document opgedeeld in hoofdstuk 1 t/m 5 die de essentie van het strategisch informatiebeveiligingsbeleid weergeeft. In de bijlagen zijn voor specifieke IB onderwerpen de strategische doelstellingen, principes en risico's (bij niet voldoen) opgenomen. De bijlagen zijn een onlosmakelijk onderdeel van dit strategische informatiebeveiligingsbeleid.

Het document is verder als volgt opgebouwd:
- In hoofdstuk 3 wordt een inleiding op informatiebeveiliging gegeven.
- Daarna in hoofdstuk 4 wordt het belang voor informatiebeveiliging voor de gemeente Aa en Hunze uiteengezet.
- In hoofdstuk 5 van dit document worden de rollen, eisen en verantwoordelijkheden benodigd voor informatiebeveiliging benoemd.
- In de daarop volgende bijlagen worden voor een aantal belangrijke IB onderwerpen de strategische doelstellingen, de risico's bij afwezigheid en eventuele principes nader uiteengezet. Deze bijlagen vormen een onlosmakelijk geheel met het strategisch informatiebeveiligingsbeleid van de gemeente Aa en Hunze en corresponderen met de hoofdstukken 6 t/m 15 uit de tactische variant van de BIG. Ze geven een nadere invulling van het gemeentelijk strategisch informatiebeveiligingsbeleid. De hoofdstukken lopen qua onderwerp en inhoud parallel aan die van de tactische BIG.

2.4 Relatie met andere documenten
Dit document legt de basis voor het vakgebied 'informatiebeveiliging' binnen de gemeente en is afgeleid en onderdeel van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Dit document geeft, na akkoord van het College van Burgemeester en Wethouders (het College) invulling aan maatregel 5.1.1 van de tactische BIG.

In de onderstaande figuur is dit informatiebeveiligingsbeleid gearceerd in het landschap van relevante wet en regelgeving, baselines, methodes en procedures schematisch weergegeven.



Figuur 1, Positie IB beleid in IB landschap van regels, procedures en baselines

3 Inleiding

3.1 Informatiebeveiliging

Informatiebeveiliging is de verzamelnaam voor de processen, die ingericht worden om de betrouwbaarheid van gemeentelijke processen, de gebruikte informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijk onheil. Het begrip 'informatiebeveiliging' heeft betrekking op:

- *beschikbaarheid / continuïteit:* het zorg dragen voor het beschikbaar zijn van informatie en informatie verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- *exclusiviteit / vertrouwelijkheid*: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn;
- *integriteit / betrouwbaarheid:* het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.

Daar waar het gaat over 'informatieveiligheid' wordt enerzijds gerefereerd aan het niveau, de stand van zaken aangaande de informatiebeveiliging. Anderzijds refereert het begrip informatieveiligheid meer naar het borgen van de bedrijfscontinuïteit, de doelstelling. Informatiebeveiliging refereert meer naar de te nemen maatregelen, het proces. In de praktijk worden de termen door elkaar heen gebruikt.

3.2 Waarom informatiebeveiliging?

Informatie is één van de belangrijkste bedrijfsmiddelen van een gemeente. Toegankelijke en betrouwbare overheidsinformatie is essentieel voor een gemeente, die zich verantwoordelijk gedraagt, aanspreekbaar en servicegericht is, die transparant en proactief verantwoording aflegt aan burgers en raadsleden en die met minimale middelen maximale resultaten behaalt. De bescherming van waardevolle informatie is hetgeen waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden om deze te beschermen.

3.3 Reikwijdte en afbakening informatiebeveiliging

Bij informatiebeveiliging richten we ons op de aspecten de 'mens', de 'organisatie' en de 'techniek'. Informatiebeveiliging is meer dan ICT, computers en automatisering. Het gaat om alle uitingsvormen van informatie (analoog, digitaal, tekst, video, geluid, geheugen, kennis), alle mogelijke informatiedragers (papier, elektronisch, foto, film, CD, DVD, beeldscherm et cetera) en alle informatie verwerkende systemen (de programmatuur, systeemprogrammatuur, databases, hardware, netwerk en bijbehorende bedrijfsmiddelen), maar vooral ook mensen (kennis, houding en gedrag) en (werk)processen. Studies laten zien dat de meeste incidenten niet voortkomen uit gebrekkige techniek, maar vooral uit menselijk handelen, gebrek aan bewustzijn en een tekort schietende organisatie. Voorbeelden van informatiebeveiligingsmaatregelen zijn: clean desk policy, hoe om te gaan met mobiele devices en aanwijzingen voor telewerken.

3.4 Digitale ketenpartners

Het gaat bij informatiebeveiliging ook steeds vaker over digitaal samenwerken in de keten en in de cloud. In het verlengde van cloud computing overlapt informatiebeveiliging de cybersecurity die zorg dient te dragen voor een veilige cyberspace.

3.5 Van BIG naar BIO in 2019

De aanleiding voor de nieuwe baseline, de BIO, komt voort uit de verandering van de ISO (International Organization for Standardization).
De BIG[2] die tot nu toe van toepassing was is nog hoofdzakelijk gebaseerd op de oudere internationale beveiligingsstandaard NEN/ISO 27001/27002 :2005/2007 terwijl de BIO gebaseerd is op de nieuwere NEN/ISO 27001/27002:2013 aangevuld met de update hierin: NEN/ISO 27001/27002:2017.

Het feit dat de BIO een gezamenlijke baseline is, voorkomt dat alle overheidslagen voor zichzelf een nieuwe baseline moeten opstellen. De BIO zal gezamenlijk beheerd worden, onder regie van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Er wordt een wijzigingsproces ingericht waarin alle overheidslagen wijzigingen kunnen voorstellen.

Vanaf 2016 is door vertegenwoordigers van de rijksoverheid, de provincies, waterschappen, gemeenten (VNG) en het Centrum voor Informatiebeveiliging en Privacy (CIP), gewerkt aan een gezamenlijke baseline die alle bestaande losse overheidsbaselines zal gaan vervangen. Diverse gemeenten hebben in de afgelopen tijd meegewerkt aan de review van deze BIO. Waarbij alle commentaar is gewogen en verwerkt in de versie 1.0 die aangenomen is per 01 juni 2018.

De BIO verschilt op een aantal punten van de BIG. De grootste verschillen zijn:

- Minder maatregelen (bijna 60% minder)
- Maatregelen zijn altijd verplicht
- Meer risicomanagement (het begint met een QuickScan, de QIS)
- 3 BasisBeveiligingNiveaus (BBN)
- Selectie van ontbrekende maatregelen vooraf
- Toewijzing van maatregelen op eindverantwoordelijke
- Een baselinetoets die nu QIS heet en die rekening houdt met die 3 BBN niveaus

Een van de grote verandering is dat ENSIA[3] compleet opnieuw moet worden ingericht. Is nog veel werk. Ook een grote verandering is dat de aanpak anders is dan bij de BIG en dat betekent ook een wijziging in het ondersteuningsaanbod van de IBD door middel van operationele BIO-producten voor gemeenten.

Wanneer de BIO in 2018 wordt aangenomen dan zal met ingang van 1-1-2019 de BIO het nieuwe normenkader worden voor alle overheidslagen en overheidssamenwerkingsverbanden. Het jaar 2019 zal dan gelden als overgangsjaar. Vanaf 1-1-2020 wordt daadwerkelijk volgens de BIO gewerkt en verantwoord via ENSIA. Zie de site van de VNG.

In 2019 gaat de gemeente Aa en Hunze werken aan de implementatie van de BIO, als opvolger van de BIG.

[2] De Tactische Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) is geheel gestructureerd volgens NEN/ISO 27001, bijlage A en NEN/ISO 27002. Met klem vermeldt zij dat de Tactische BIG deze normen niet vervangt. De overheid is conform de voorschriften van het College Standaardisatie, verplicht omaan ISO 27001 en ISO 27002 te voldoen. De basisrichtlijn Informatiebeveiliging Rijksdienst (BIR) is een toepassingshandleiding voor NEN/ISO 27001 en 27002 voor de rijksoverheid. De BIR beschrijft de aanvullingen op NEN/ISO27001 en 27002 voor de overheid. In de Tactische Baseline zijn die aanvullingen gemerkt met een [A].

[33] **ENSIA**: Eenduidige Normatiek Single Information Audit. Verantwoorden over informatieveiligheid.

3.6 Gebruik ISMS

Het bijhouden van een actueel strategisch informatiebeveiligingsbeleid met alle bijbehorende procedures, richtlijnen, checklists en rapportages is van groot belang. Het gaat hier om de vertaling van de maatregelen uit de bijlagen, die bij elkaar oplopen tot ruim 100 documenten. De bijbehorende procedures zijn van belang voor professionalisering van de organisatie, voorgeschreven IT-audits, zelfevaluaties (ENSIA) en de jaarrekeningcontrole van de accountant.

Met behulp van een modern Information Security Management System (ISMS) kan op relatief eenvoudige manier een goed overzicht gemaakt worden welke zaken al zijn opgepakt, welke wanneer opgepakt gaan worden en welke we als Aa en Hunze niet gaan implementeren –'pas toe of leg uit', risico gebaseerd.

Dit geheel vormt een overzicht en wordt door het directie team vastgesteld waarmee het de zogenaamde 'verklaring van toepasselijkheid' (VVT) vormt. Aanpassingen in dit overzicht worden besproken met het directie team. Teamleiders sturen in hun team op het toepassen van deze maatregelen en leggen de argumenten vast wanneer een maatregel niet wordt geïmplementeerd. Mede hierdoor zal het bestuur zijn verantwoordelijkheid kunnen nemen. Wijzigingen in landelijke wet –en regelgeving worden automatisch doorgevoerd door de leverancier van het ISMS. Aa en Hunze waarborgt op deze manier haar beveiligingsdocumenten en heeft met deze set aan documenten een goed middel in handen om de P&C cyclus voor informatiebeveiliging op gang te brengen.

4 Belang van informatieveiligheid voor Aa en Hunze

Informatie is één van de voornaamste bedrijfsmiddelen van de gemeente Aa en Hunze. Het verlies van gegevens, uitval van ICT, of het door onbevoegden kennisnemen of manipuleren van bepaalde informatie kan ernstige gevolgen hebben voor de bedrijfsvoering maar ook leiden tot imagoschade. Ernstige incidenten hebben mogelijk negatieve gevolgen voor burgers, bedrijven, partners en de eigen organisatie met waarschijnlijk ook politieke consequenties. Informatieveiligheid is daarom van groot belang. Informatiebeveiliging (IB) is het proces dat dit belang dient.

4.1 Visie

De komende jaren zet de gemeente Aa en Hunze in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie en regie op digitale ketens. Een betrouwbare informatievoorziening – zowel in- en extern- is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven[4]-door bijvoorbeeld het borgen van de AVG. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Alle interne teams en digitale ketenpartners zijn hierbij betrokken.

Informatiebeveiliging is een 'enabler' van de business. Hierbij gaan we uit van het principe 'informatiebeveiliging en 'privacy by design'. Door vooraan bij nieuwe ontwikkelingen betrokken te zijn, worden privacy en informatieveiligheid een logisch onderdeel van deze nieuwe ontwikkelingen zodat er weinig extra lasten zijn. Als er bijvoorbeeld bij de onderhandelingen over cloud diensten de juiste afspraken worden gemaakt en vastgelegd over informatieveiligheid en privacy, kan de regie op deze clouddienst goed worden uitgevoerd.

Daarnaast is het proces van informatiebeveiliging primair gericht op bescherming van gemeentelijke informatie, zowel intern, binnen samenwerkingsverbanden[5] als in de cloud, met digitale ketenpartners.

De focus is informatie uitwisselen in alle verschijningsvormen, zoals elektronisch, op papier en mondeling. Het gaat niet alleen over bescherming van privacy, maar ook over bescherming van vitale maatschappelijke functies die worden ondersteund met informatie (verkeer, vervoer, openbare orde en veiligheid, etc.). Het gaat bij informatieveiligheid ook zeker niet alleen over ICT. Maar ook over verantwoordelijkheid, actuele kennis, houding en gedrag van medewerkers ten aanzien van het gebruik van informatie(systemen).[6]

Als laatste genoemd, maar niet de minste, gaat informatieveiligheid over het proces van de continuïteit van de bedrijfsvoering (dienstverlening) ook wel Business Continuity Management (BCM) genaamd.

[4] Met betrouwbaarheid wordt bedoeld: beschikbaarheid (continuïteit van de bedrijfsvoering), integriteit (juistheid, volledigheid) en vertrouwelijkheid (geautoriseerd gebruik) van gegevens en informatie.
[5] SDA, BSDA, Attenta, RUD, …
[6] Medewerker = (1) ambtenaar in de zin van het Ambtenarenreglement of (2) degene die op arbeidsovereenkomst of anderszins betaalde of niet-betaalde werkzaamheden voor de gemeente Aa en Hunze verricht.

4.2 Doelstelling

Dit strategisch informatiebeveiligingsbeleid (Informatiebeveiligingsbeleid) is het kader voor passende technische en organisatorische maatregelen om gemeentelijke informatie te beschermen en te waarborgen, dat de gemeente voldoet aan relevante wet en regelgeving. De gemeente Aa en Hunze streeft er naar om 'in control' te zijn en daarover op professionele wijze verantwoording af te leggen (ENSIA[7]).

In control betekent in dit verband dat de gemeente weet welke maatregelen genomen zijn en dat er een SMART-planning is van de maatregelen die nog niet genomen zijn en als laatste dat dit geheel verankerd is in de PDCA-cyclus.

De individuele doelstellingen van de onderstaande onderwerpen zijn verder uitgewerkt in de bijlagen: Het betreft overeenkomende onderwerpen uit de BIG.

Bijlage 1	Organisatie van informatiebeveiliging;
Bijlage 2	Beheer van bedrijfsmiddelen;
Bijlage 3	Beveiliging van personeel;
Bijlage 4	Fysieke beveiliging;
Bijlage 5	Beheer van communicatie- en bedieningsprocessen;
Bijlage 6	Toegangsbeveiliging;
Bijlage 7	Verwerving, ontwikkeling en onderhoud van informatiesystemen;
Bijlage 8	Beheer van informatiebeveiligingsincidenten;
Bijlage 9	Bedrijfscontinuïteitsbeheer;
Bijlage 10	Naleving

[7] ENSIA eenduidige normatiek single information audit: de verantwoordingssystematiek van de gemeente over de kwaliteit en het veilig gebruik van informatie in brede en specifieke zin.

4.3 Uitgangspunten

- Het strategisch informatiebeveiligingsbeleid van de gemeente Aa en Hunze is in lijn met het algemene beleid van de gemeente en ondersteunt de doelstellingen van het Collegeprogramma.
- Dit Informatiebeveiligingsbeleid is gebaseerd op de relevante landelijke en Europese wet- en regelgeving.[8]
- Het Informatiebeveiligingsbeleid is gebaseerd op de Code voor Informatiebeveiliging (NEN/ISO 27001:2005) en de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) die naar verwachting in 2020 vervangen wordt door de Baseline Informatiebeveiliging Nederlandse Overheden (BIO) waarna ook het Informatiebeveiligingsbeleid moeten worden geactualiseerd.
- Het Informatiebeveiligingsbeleid wordt vastgesteld door het College. Het directie team stuurt minimaal jaarlijks op het actualiseren van het Informatiebeveiligingsbeleid. In 2019 wordt, volgens planning, dit beleid vervangen door één gebaseerd op de BIO.

4.4 Risicobenadering

- De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) in Aa en Hunze is 'risk based'. Dat wil zeggen: beveiligingsmaatregelen worden getroffen op basis van een toets tegen de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) van VNG/KING (GAP-analyse). Indien een systeem meer maatregelen nodig heeft, wordt een (verdiepende) risicoanalyse uitgevoerd. Daartoe inventariseert de proceseigenaar/systeemeigenaar de kwetsbaarheid van zijn werkproces/informatiesysteem en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beschermingseisen van de informatie. Het risico is de kans dat een beveiligingsincidenten zich voordoet en de impact daarvan op het werkproces en wordt bepaald door de proceseigenaar/systeemeigenaar: **risico = kans x impact**.

Er dient altijd een balans gezocht te worden tussen het nemen van risico's en het treffen van maatregelen.

4.5 Scope

- De scope van dit beleid omvat de meeste gemeentelijke processen, onderliggende informatiesystemen, informatie en gegevens van de gemeente en externe partijen (bijv. politie), samenwerkingsverbanden en digitale ketenpartners, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.
- Dit gemeentelijke Informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving specifieke (aanvullende) beveiligingseisen.[9]
- Domein specifiek beleid voor bijvoorbeeld de Basis Registratie Personen (BRP) is te vinden in het handboek Informatiebeveiliging BRP en Waardedocumenten.
- Onderhavig tactische en operationeel beleid zijn gebaseerd en gaan uit van dit strategisch informatiebeveiliging beleid.

[8] Daarbij geldt het 'comply or explain' principe (pas toe of leg uit)
[9] Bijvoorbeeld BRP, SUWI (Structuur Uitvoeringsorganisatie Werk en Inkomen) en gemeentelijke basisregistraties.

5 Rollen en verantwoordelijkheden Aa en Hunze

Het bestuur en management speelt een cruciale rol bij het uitvoeren van dit strategisch informatiebeveiligingsbeleid. Het management bestaat uit het directie team en de teamleiders. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben. Op basis van deze inschatting stelt het directie team vast welke risico's de gemeente loopt en voor welke risico's aanvullende maatregelen worden getroffen. Deze acties worden opgenomen in het jaarplan informatiebeveiliging. Op deze manier geeft het management een duidelijke richting aan informatiebeveiliging. Het is de rol van de teamleiders om dit beleid uit te dragen in de organisatie, de medewerkers hierin te ondersteunen en de naleving ervan te bewaken.

Om de naleving van het beleid verder te verbeteren is de organisatie van informatiebeveiliging ingericht op basis van het zgn. 'Three lines of defence' model (3LoD). De functionaris informatieveiligheid helpt waar nodig de teamleiders en medewerkers met het implementeren van dit beleid. De CISO controleert of de implementatie voldoet aan de eisen. Dit model is verder uitgewerkt in Bijlage 1.

Het streven is dat medewerkers en management intrinsiek gemotiveerd zijn de beveiligingseisen na te leven. Deze motivatie wordt versterkt wanneer het management nauw betrokken is bij de totstandkoming van het beleid en in de uitvoering daarvan voorleeft voor de hele gemeente inclusief samenwerkingsverbanden en (keten) partners. Dit beleid is dan ook van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen) en de (creatie van) overeenkomsten met derden. Het strategisch informatiebeveiligingsbeleid van de gemeente sluit aan bij de nieuwe sturingsfilosofie en informatiebeleid van de gemeente en is in lijn met de relevante landelijke en Europese wet- en regelgeving. De gemeente is verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid. Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: BRP, SUWI, BAG en PUN, maar ook de archiefwet en de AVG.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Naar verwachting gaat deze in 2019 over in de BIO.
- Het College stelt dit normenkader vast, waarbij er ruimte is voor risicoafweging en prioritering door het directie team.

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2005) en de BIG, zie ook bijlage 1:

1. Veel informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. De verantwoordelijkheid voor informatiebeveiliging ligt bij het management, met het **College van B&W als eindverantwoordelijke**. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Door **de periodieke controle, organisatie brede planning en coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het strategisch informatiebeveiligingsbeleid vormt samen met het jaarplan informatiebeveiliging het fundament onder een betrouwbare informatievoorziening. In het jaarplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het jaarplan wordt jaarlijks bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en uitgevoerde risicoanalyses.
3. Informatiebeveiliging is een **continu verbeterproces**. 'Plan, do, check en act' vormen samen het **management systeem** van informatiebeveiliging.

4. De **Centrale Informatie Security Officer** (CISO) controleert vanuit een **onafhankelijke positie** op de uitvoering van het Informatiebeveiligingsbeleid en rapporteert daarover aan het management.
5. Teamleiders stellen de benodigde **mensen en middelen beschikbaar** om de door hun ondersteunde eigendommen en werkprocessen te beveiligen en de gestelde strategische (informatiebeveiligings-) doelstellingen te behalen.
6. **Regels en verantwoordelijkheden van medewerkers** ten behoeve van het beveiligingsbeleid dienen te worden vastgelegd en **vastgesteld**. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
7. Iedere medewerker, zowel vast als tijdelijk, intern of extern is **verplicht waar nodig gegevens en informatiesystemen te beschermen** tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

Dit Informatiebeveiligingsbeleid treedt in werking na vaststelling door College van B&W.

Aldus vastgesteld door burgemeester en wethouders van de gemeente Aa en Hunze:

Ondertekening (namens) portefeuillehouder

Naam:_____

Functie:_____

Datum: _____

Handtekening:

Bijlage 1: Organisatie van de informatiebeveiliging

Interne organisatie

Doelstelling:

Beheren van de informatiebeveiliging (IB) binnen de organisatie.

Vaststelling van het strategisch informatiebeveiligingsbeleid door het College, betrokkenheid van het directie team, de toewijzing en coördinatie van andere rollen in de organisatie en beoordeling van de feitelijke implementatie van het beleid.

Bij de inrichting van de informatiebeveiligingsorganisatie wordt uitgegaan van het model van de '3 lines of defence' ofwel **3LoD** genoemd. Hierbij is rekening gehouden met de nieuwe sturingsfilosofie van het management waarbij verantwoordelijkheid voor uitvoering zo dicht mogelijk bij de medewerkers ligt.

Het **'Three Lines of Defence model'** maakt duidelijk dat medewerkers primair –**in de eerste lijn**- verantwoordelijk zijn voor de realisatie van de strategie, voor de daarvan afgeleide doelstellingen en voor de beveiliging van de gebruikte informatie. Hierin worden de medewerkers ondersteund door de teamleiders aanspreekbaar zijn op de goede operationele aansturing van individuele medewerkers en functioneren van het team als geheel. Het directie team weegt de in beeld gebrachte risico's af die met veilig gebruik van informatie samenhangen. De controle op volledigheid en betrouwbaarheid van verantwoordingsinformatie is een gezamenlijke inspanning.

De tweede lijn is verantwoordelijk voor de inrichting van de organisatie van informatiebeveiliging. Het gaat daarbij bijvoorbeeld om het ontwikkelen van voorschriften over de toe te passen wet- en regelgeving. De tweede lijn ondersteunt de eerste lijn en derde lijn door:

- het identificeren en bewaken van risico's (kwetsbaarheden en bedreigingen);
- ontwikkelt een aanpak en beheersmethode en legt daarvan verslag;
- ondersteunt bij het afleggen van (horizontale-) verantwoording;
- de implementatie van technische-, organisatorische- of persoonsgerichte maatregelen voor het verbeteren van de informatieveiligheid.

De derde lijn staat voor de interne auditfunctie (IAF) voor informatiebeveiliging en privacy. Deze rol is ingevuld door de CISO voor informatiebeveiliging en door de FG voor privacy. Werkzaamheden zijn:

- regie houden over de betreffende beleidsstukken;
- toezicht houden op naleving van informatiebeveiliging en het aanspreken van medewerkers hier op.
- Het rapporteren over de realisatie aan het directie team, de teamleiders en het college;

Risico's

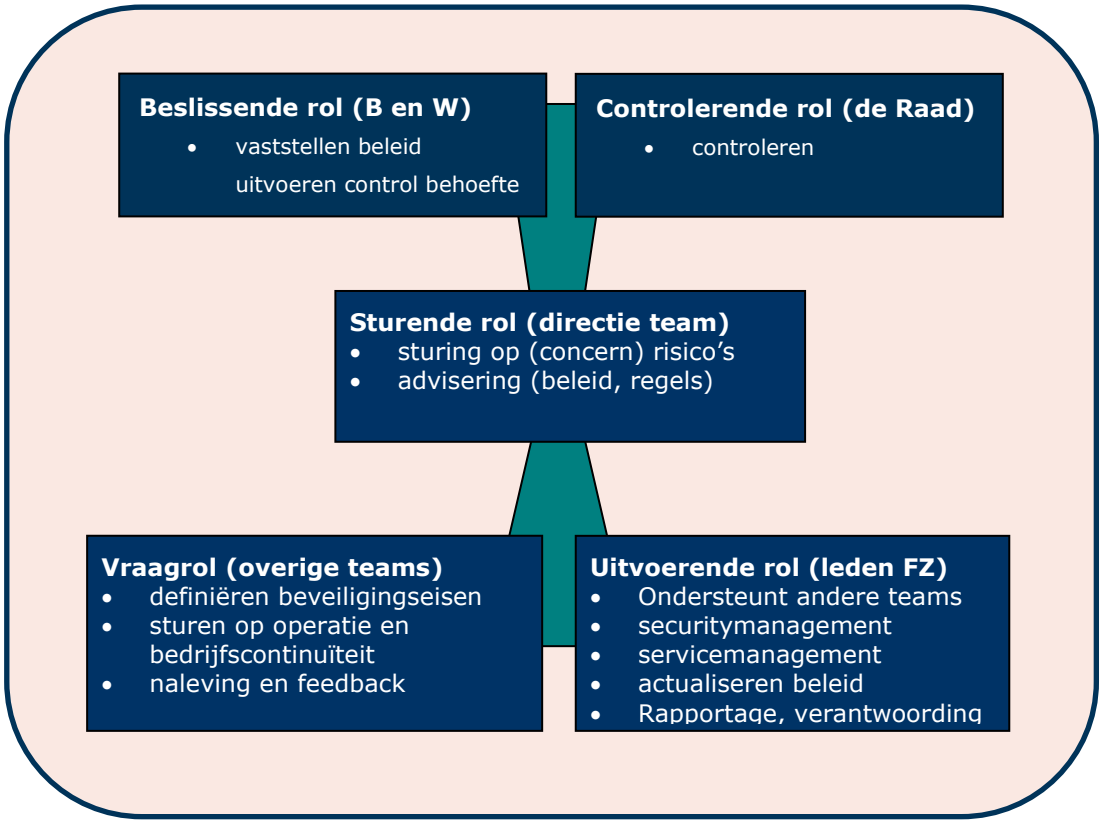
- Het is belangrijk dat verantwoordelijkheden worden belegd om te voorkomen dat er (mogelijk) onveilige situaties ontstaan.

Verantwoordelijkheden

- Het College van Burgemeester en Wethouders is (beslissend) eindverantwoordelijk voor de beveiliging van informatie binnen de werkprocessen van de gemeente.[10]
  - ze stelt de kaders vast voor informatiebeveiliging op basis van Nederlandse- en Europese wet- en regelgeving en de landelijke normenkaders.
- Het directie team is (sturend) verantwoordelijk voor risicobeheersing en sturing. Het directie team:
  - is vroegtijdig betrokken bij relevante ontwikkelingen;
  - stelt het jaarplan informatiebeveiliging vast en stuurt op (concern-) risico's;
  - evalueert de beleidsstukken en geeft advies bij het actualiseren daarvan;
  - heeft kennis van de maandelijkse beveiligingsrapportages en neemt zonodig deel aan het tactisch/stragische informatiebeveiligings- en privacyoverleg.
- De medewerkers zijn zelf verantwoordelijk voor de integrale beveiliging van hun werkprocessen, informatiesystemen en data.[11] De medewerker:
  - heeft een sleutelrol in het uitvoeren van het concern brede informatiebeveiligingsbeleid;
  - heeft als inhoudelijk specialist namens het management de rol van proces- of systeemeigenaar;
  - legt op basis van een risicoafweging beschikbaarheids-, integriteits- of vertrouwelijkheidseisen vast voor de informatiesystemen (dataclassificatie);
  - implementeert maatregelen die voortvloeien de dataclassificatie;
  - levert een bijdrage in bewustwording, bedrijfscontinuïteit en in naleving van (gedrags-) regels.
- De teamleiders ondersteunen de medewerkers bij het voldoen aan het beveiligingsbeleid. Ze:
  - creëren draagvlak en tonen voorbeeldgedrag;
  - sturen de teams operationeel aan op een wijze die past bij het informatiebeveiligingsbeleid;
  - geven advies bij de uitvoering en doorontwikkeling van dit beleid;
  - faciliteren medewerkers in de noodzakelijke middelen.
- Specialistische medewerkers van het team Facilitaire Zaken begeleiden andere medewerkers (van bode- tot burgemeester) in dit proces. Indien nodig coördineren ze de uitvoering van de plannen voor informatiebeveiliging.[12] Ze:
  - doen voorstellen over te nemen beveiligingsmaatregelen;
  - coördineren de implementatie van beveiligingsmaatregelen die voortvloeien uit dataclassificatie;
  - zijn verantwoordelijk voor toezien op de adequate inrichting van de beheeraspecten van informatiebeveiliging, zoals logisch toegangsbeheer, ICT security management, incident-, problem- en wijzigingsbeheer, facilitaire en personele informatiebeveiliging;
  - helpen bij afhandeling van incidenten en calamiteiten;
  - adviseren en ondersteunen bij het inrichten van logging, monitoring en rapportage;
  - leveren stakeholders technisch-, organisatorisch- of persoonsgericht beveiligingsadvies;
  - rapporteren over het voldoen aan wet- en regelgeving en over het algemeen beleid van de gemeente.

[10] Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
[11] Zie ook: strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten
[12] Let op, het team Facilitaire Zaken is tegelijk ook klant, het gaat hier echter om de uitvoerende rol.

Figuur 2: relaties rollen en taken



Taken en rollen

- Het college stelt formeel het Informatiebeveiligingsbeleid vast. De uitvoering van het beleid moet gecontroleerd worden, zowel het College als de Raad (controle functie) kunnen hiervoor opdracht geven om dit te (laten) controleren.
- Het directie team wordt betrokken bij ontwikkelingen met een concern brede impact en geeft daarover advies;
- Het management (directie team en teamleiders) geeft feedback en creëert draagvlak bij bestuur en organisatie;
- De Centrale Informatie Security Officer (CISO) heeft de volgende taken:
  - regisseert het strategisch informatiebeveiligingsbeleid;
  - houdt namens het management toezicht op de naleving van het strategisch informatiebeveiligingsbeleid;
  - controleren van- en rapporteren over het jaarplan informatiebeveiliging aan het directie team, waaronder bewustwording en risicoanalyses;
  - is primair vertrouwelijk contactpersoon informatie beveiliging voor de IBD;
  - regiseert de horizontale verantwoording (ENSIA);
  - kan gevraagd en ongevraagd adviseren over informatieveiligheid;
  - controleert diverse regisers zoals de actiepuntenlijst en risicoregiser;
  - controle van het beleid en plannen voor bedrijfscontinuïteit;
  - zoekt verbinding met de vakgroep en gemeenten en informeert over nieuwe wetgevingseisen;
- De functionaris informatiebeveiliging heeft de volgende taken:
  - geeft op dagelijkse basis invulling aan het strategisch informatiebeveiligingsbeleid door collega's te ondersteunen bij het realiseren van maatregelen. Levert als specialist vooral een bijdrage om de kwaliteit en professionaliteit te vergroten. Als hoeksteen veelal betrokken bij alle voorkomende taken die hieruit voortvloeien;
  - bespreekt (ernstige) beveiligingsincidenten en risico's met de CISO en andere stakeholders;
  - organiseert een beveiligings- en privacy overleg en legt verslag daarvan;
  - beheert diverse regisers zoals de actiepuntenlijst, datalekkenregiser en risicoregiser;
  - is tweede vertrouwelijk contactpersoon informatie beveiliging voor de IBD;
  - ondersteunt bij de horizontale verantwoording (ENSIA);
  - zoekt verbinding met vakgroep en gemeenten en informeert over nieuwe ontwikkelingen;
- Automatisering heeft een medewerker aangesteld in de rol van 'technische security officer' (TSO).
  - Dit voor dagelijks beheer van de technische IB-aspecten en terugkoppeling naar het beveiligingsplatform. Als technisch specialist en spreekbuis naar automatisering is hij onmisbaar om goed uitvoering te kunnen geven aan adequaat informatiebeveiligingsbeleid.
- Informatiemanager
  - De informatiemanager kent als geen ander de samenhang van processen, systemen en applicaties binnen de organisatie. Als informatie expert kan hij bij relevante ontwikkelingen worden betrokken zodat hij instaat is de samenhang te bewaken en de kwaliteit te verbeteren.

Wie	Plan: Kaderstelling	Do: Uitvoering	Check: Controle	Act: Verbetering
Sturen: **CISO** **(directie dagelijkse uitvoering)**	Ontwikkelen van kaders (beleid en architectuur); reglementen; meerjarenplanning. Leidende principes.	Inbedding landelijke en EU-richtlijnen, advisering, handreikingen, crisisbeheersing en incident respons.	Controle, audit, pentesten. ENSIA.	Bijsturen: opdrachtverstrekking voor verbeteracties. Rapportage aan directie/ B&W
Vragen: **Teamleiders**	Ondersteunings- visie medewerkers en laten formuleren van beveiligingseisen (classificatie van gegevens)	Stimuleren van beveiligingsbewustzijn bij medewerkers, risico- en bedrijfscontinuïteit-management.	Interne controle (IC), sturen op naleving van regels door medewerkers (gedrag).	Verbeteren bedrijfscontinuïteit. Mondelinge of schriftelijke feedback aan ISO/CISO en directie team.
Uitvoeren: **ISO / (TSO)** **(ondersteuning/advies)** **(medewerkers van teamleiders voeren uit)**	Beleidsvoorbereiding, (technische) onderzoeken en marktverkenningen.	Leveren van security management en services (ICT), incidentbeheer, logging, monitoring en advies.	Kwetsbaarheden / bedreigingen scanning, evaluatie en rapportage.	Uitvoeren verbeteracties. Advies aan de ISO/CISO over aanpassingen aan de informatievoorziening.

Functioneel overleg

De functionaris informatieveiligheid (ISO) richt een organisatie op van security gerelateerde functionarissen binnen de gemeente en richt zich met name, van uit het strategisch beleid, op tactisch/operationele informatiebeveiliging kwesties.

Het onderwerp informatiebeveiliging wordt een vast onderdeel op de agenda van de teamleiders. Zodat er sturing plaatsvindt op de uitgevoerde activiteiten en in hun gesprekken met medewerkers waarvoor informatiebeveiliging van belang is in hun functie[13].

ICT crisisbeheersing en landelijke samenwerking

- Voor interne crisisbeheersing, bedrijfscontinuïteit en uitwijk, dient er een kernteam informatiebeveiliging en privacy geïnstalleerd te zijn, bestaande uit CISO of functionaris informatiebeveiliging (informatiemanager/CIO), security functionaris ICT Service organisatie, relevante experts en het gemeentelijke communicatieteam.
- De gemeente Aa en Hunze participeert in relevante landelijke platforms en onderhoudt contacten met andere sectoraal georganiseerde IB-platforms.

[13] BIG 8.2.2.2: Bespreek het onderwerp informatiebeveiliging in functionerings- en beoordelingsgesprekken van medewerkers die risicovolle functies bekleden

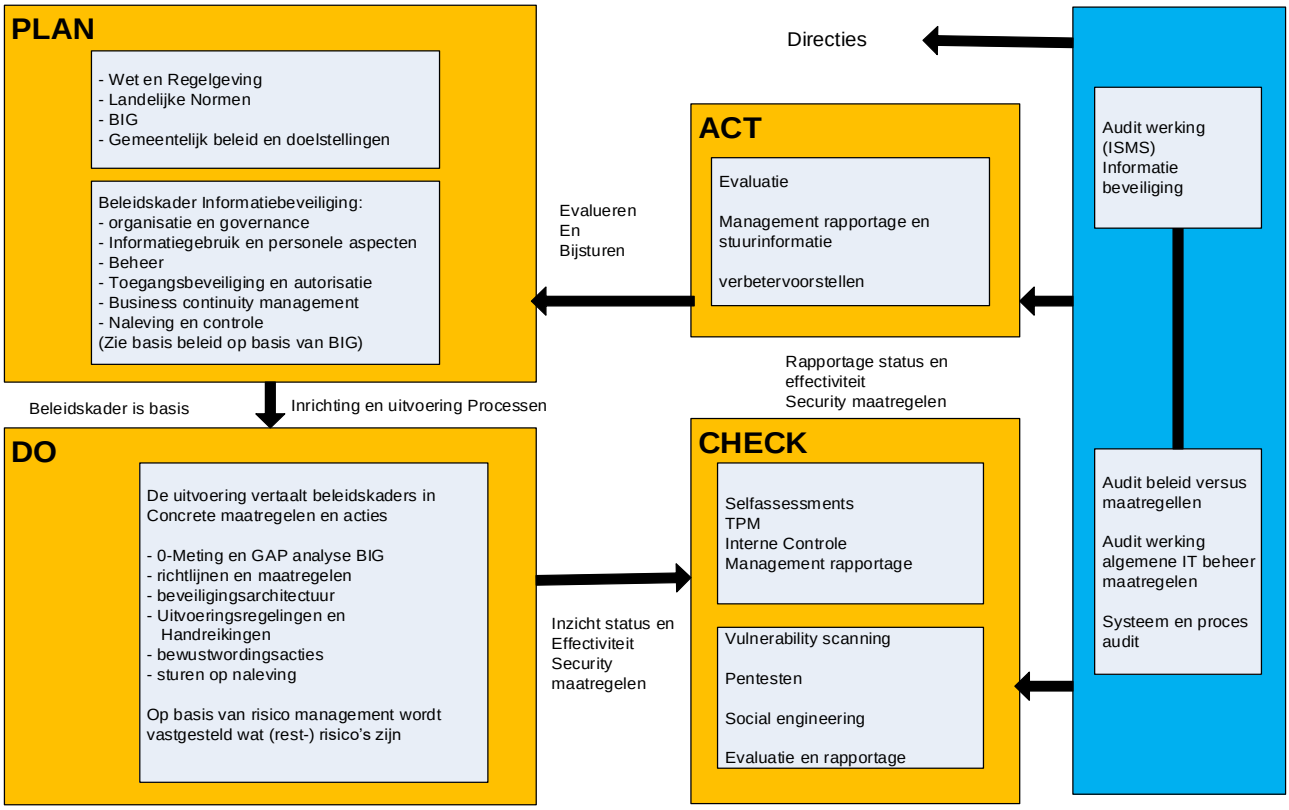
Rapportage en escalatielijn voor IB

Onderwerp	Escalatieladder
Beveiligingsincident/calamiteit	ISO/ TSO → CISO/CIO[14] → portefeuillehouder directie team → portefeuillehouder College[15] ISO ←→ IBD … ISO/ TSO /CISO ←→ ketenpartner
Veiligheidsoverleg	ISO (verslag); ISO/TSO/FG/CISO/CIO (voorzitter per toerbeurt)
Halfjaarlijkse rapportage IB	ISO/ TSO → CISO/CIO → portefeuillehouder directie team
ENSIA jaarrapport	CISO→ teamleider→ directie team → College → Gemeenteraad
ENSIA Collegeverklaring	CISO→ directie team → College → gemeenteraad
Crisis/bedrijfscontinuïteit/uitwijk	Kernteam IB/Privacy: ISO/TSO/FG/CISO/CIO/portefh. directie team/portefh. College

PDCA

- Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het management systeem van informatiebeveiliging.[16] Deze kwaliteitscyclus is in onderstaande figuur weergegeven.
- Toelichting figuur 2:
  - Plan: De cyclus start met Informatiebeveiligingsbeleid, gebaseerd op wet- en regelgeving, landelijke normen zoals de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld. De planning op hoofdlijnen is onderdeel van de I&A projectenkalender en uitgewerkt in het informatiebeveiligingsplan van de gemeente.
  - Do: Uitvoering van plan: (technische) maatregelen en bevordering van beveiligingsbewustzijn. Uitvoering geschiedt op dagelijkse basis en maakt integraal onderdeel uit van het werkproces.
  - Check: Control is onderdeel van het werkproces met als doel: waarborgen van de kwaliteit van informatie en ICT, en compliance aan wet- en regelgeving. Zie 3LoD aanpak.
    - Interne controle: jaarverslag/jaarrekening informatiebeveiliging, horizontale verantwoording aan de raad (ENSIA) en maandverslagen van het beveiligingsoverleg aan het directie team.
    - Externe controle: in het kader van de IT-audit voor de jaarrekening. ENSIA (verticale verantwoording) IT-audit voor DigiD en SUWInet. Collegeverklaring aan rijksdiensten.
  - Act: De cyclus is rond met de selectie van verbeteracties op basis van check en externe controle (jaarplan/ENSIA/accountant) zoals vastgelegd in het jaarplan. De cyclus is een continu proces; de bevindingen van controles zijn weer input voor de nieuwe jaarplanning en beveiligingsplannen. Bevindingen worden via de maandrapportages gerapporteerd aan het directie team.

[14] CIO: chief information officer ofwel de senior informatiemanager
[15] De CISO is adviseur van de gemeentelijke directie en rapporteert tegelijkertijd direct aan de wethouder
[16] NEN/ISO 27001



Figuur 3: Information Security Management System

Bijlage 2: Beheer van bedrijfsmiddelen

Verantwoordelijkheid voor bedrijfsmiddelen

Doelstellingen

Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

Voor alle bedrijfsmiddelen is de eigenaar vastgelegd alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen.

Risico's:

- Bedrijfsmiddelen en informatie zijn blootgesteld aan risico's zoals diefstal, beschadiging of onoordeelkundig gebruik, waarbij niet voor alle ICT-configuratie items is vastgelegd wie de eigenaar/hoofdgebruiker is.
- Onduidelijkheid wie verantwoordelijk is voor gegevensbestanden, waardoor ook niemand verantwoordelijk is voor de beveiliging en kan optreden bij incidenten.

Classificatie van informatiesystemen (data/processen)

Doelstellingen

Informatie heeft bepaalde waarde en dientengevolge een geschikt niveau van bescherming.

Classificatie uitvoeren op het niveau van informatiesystemen (data/proces) waarbij de impact op het bedrijf, de mogelijke schade wordt bepaald en de noodzakelijke bescherming wordt bepaald en aangebracht. Geclassificeerd wordt op de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.

Adequate niveaus van bescherming van informatie zijn gedefinieerd en de noodzaak voor aparte verwerkingsmaatregelen is gecommuniceerd.

Risico's:

- Geen inzicht in welke componenten, zowel hardware als software, het belangrijkst zijn voor de primaire processen.
- Onjuiste classificatie draagt bij aan het onjuist beschermen van informatie en bedrijfsmiddelen met als risico, dat deze verloren kunnen gaan of openbaar worden gemaakt terwijl dat niet de bedoeling is.

Bijlage 3: Beveiliging van personeel

Doelstelling

Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

De verantwoordelijkheden ten aanzien van beveiliging is vóór het dienstverband vastgelegd in passende functiebeschrijvingen en in de arbeidsvoorwaarden.

Alle kandidaten voor een aanstelling, ingehuurd personeel en externe gebruikers worden gescreend, in het bijzonder voor vertrouwensfuncties.

Werknemers, ingehuurd personeel en externe gebruikers, die ICT-voorzieningen gebruiken tekenen een overeenkomst over hun beveiligingsrollen en –verantwoordelijkheden.

Risico's

- Het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door externe medewerkers verdient extra aandacht, omdat menselijk falen en bedreigingen van menselijke aard significante invloed kunnen hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Bijlage 4: Fysieke beveiliging en beveiliging van de omgeving

Doelstelling

Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie, bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

ICT-voorzieningen, die kritieke of gevoelige bedrijfsactiviteiten ondersteunen, behoren fysiek te worden ondergebracht in beveiligde ruimten, beschermd door afgegrensde beveiligde gebieden, in een gecontroleerde omgeving, beveiligd met geschikte beveiligingsbarrières en toegangsbeveiliging. Ze behoren fysiek te worden beschermd tegen toegang door onbevoegden, schade en storingen.

Het voorkomen van verlies, schade of diefstal van apparatuur en bescherming tegen fysieke bedreigingen en gevaren van buitenaf.

Risico's

- Onbevoegde toegang tot kritieke systemen of waardevolle informatie. Bij het ontbreken van registratie zijn incidenten bovendien niet herleidbaar tot individuen.
- Door bijvoorbeeld de inzet van externen, de toeloop van leveranciers en andere niet-medewerkers of het feit dat de medewerkers op meerdere locaties op geruime afstand van elkaar gevestigd zijn, is het betrekkelijk eenvoudig voor niet-medewerkers om toegang tot de panden te krijgen door tegelijk met een geautoriseerde medewerker naar binnen te gaan.
- Als informatie zichtbaar op bureaus ligt, is er een verhoogd risico m.b.t. de vertrouwelijkheid.
- Geen procedures voor het veilig verwijderen of hergebruiken van ICT-apparatuur.

Bijlage 5: Beveiliging van apparatuur en informatie

Doelstelling

Waarborgen van een correcte en veilige bediening van ICT-voorzieningen.

Vastgestelde verantwoordelijkheden en procedures voor beheer en bediening van alle ICT-voorzieningen. Dit omvat tevens de ontwikkeling van geschikte bedieningsinstructies.

Toepassing, waar nodig, van functiescheiding om het risico van nalatigheid of opzettelijk misbruik te verminderen.

Risico's

- Het ontbreken van documentatie kan leiden tot fouten, niet-uniforme wijze van gegevensinvoer, of in geval de beheerder/bediener uitvalt, tot problemen rondom de continuïteit.
- Onjuiste autorisaties kunnen leiden tot foutieve handelingen, fraude en verduistering.
- Het niet uitvoeren en vastleggen van technische en functionele applicatietesten en/of de resultaten hiervan, kan in bepaalde omstandigheden (tijdsdruk, vakantieperiodes, etc.) leiden tot een verhoogd risico van uitval of gegevens verlies.
- De gemeente gaat steeds meer samenwerken (en informatie uitwisselen) in ketens en besteedt meer taken uit. Bij beheer van systemen en gegevens door een derde partij, kan ook informatie van de gemeente op straat komen te liggen. De gemeente blijft verantwoordelijk voor de informatiebeveiliging van haar gegevens in dat deel van de keten, waarbij het beheer bij een andere partij ligt.
- Programmatuur en ICT-voorzieningen zijn kwetsbaar voor malware.
- Het ontbreken van een regeling voor malware bescherming bij medewerkers thuis leidt tot hogere beveiligingsrisico's.

Behandeling van media

Doelstelling

Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van informatie en bedrijfsmiddelen.

Media worden beheerst en fysiek beschermd.

Vastgestelde procedures om documenten, opslagmedia (bijvoorbeeld USB-sticks, back-up tapes, schijven), in- en uitvoergegevens en systeemdocumentatie te beschermen tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.

Risico's

Verwijderbare media kan informatie bevatten, die in onbevoegde handen kan vallen bij onjuist gebruik, verlies of diefstal.

Uitwisseling van informatie

Doelstelling

Handhaven van beveiliging van informatie en programmatuur, die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

Een formeel uitwisselingsbeleid m.b.t. de uitwisseling van informatie en programmatuur tussen organisaties, dat in lijn is met de uitwisselingsovereenkomsten en relevante wetgeving.

Vastgestelde procedures en normen ter bescherming van informatie en fysieke media, die informatie bevatten die wordt getransporteerd.

Uitgangspunten

- Geformaliseerde situatie rondom het transport van de back-ups en de mogelijkheden van leveranciers om toegang tot het netwerk te verkrijgen.
- Een basisraamwerk met randvoorwaarden voor gegevensuitwisseling met ketenpartners.
- Gevoelige informatie (classificatie vertrouwelijk en zeer geheim) wordt nooit bekend gemaakt via telefoon of fax, in verband met bijvoorbeeld afluisteren.
- Bewustzijn en sociale controle om het risico op het lekken van informatie via telefoon e.d. te laten afnemen.

Risico's

Verlies of diefstal van 'smart devices' zoals laptops, USB-sticks, iPads, smart phones e.d., waarbij bovendien informatie in verkeerde handen komt.

Bijlage 6: Logische toegangsbeveiliging

De identiteit van een gebruiker die toegang krijgt tot gemeentelijke informatie dient te worden vastgesteld.[17] Logische toegang is gebaseerd op de classificatie van de informatie. Toegang wordt alleen op basis van identiteit gegeven.

Doelstelling

Beheersen van de toegang tot informatie, ICT-voorzieningen en bedrijfsprocessen op grond van regelgeving, bedrijfsbehoeften en beveiligingseisen.

Beleid ten aanzien van informatieverspreiding en autorisatie is van toepassing.

Risico's:

- Wanneer toegangsbeheersing niet expliciet gebaseerd is op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en/of een aanvullende risicoanalyse, is niet duidelijk of het juiste niveau van beveiliging wordt gehanteerd.
- Verstoringen door onjuist gebruik van ICT-ruimtes of ICT-componenten (m.n. waar ook niet ICT-teams toegang hebben).

[17] Een gebruiker kan een medewerker, leverancier, burger, bedrijf, samenwerkingspartner of applicatie zijn.

Bijlage 7: Beveiliging van informatiesystemen

Doelstelling

Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

Risico's

Als voorbeeld de volgende zaken. Slecht ontworpen informatiesystemen die onvoldoende gepatcht worden; geen beheer; slecht uitgevoerde implementatie van software; geen software by design principe; geen IB vereisten bij de aanbesteding opnemen.

Bijlage 8: Beveiligingsincidenten

Doelstelling

Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden, die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

Formele procedures voor rapportage van gebeurtenissen en escalatie. Alle werknemers, ingehuurd personeel en externe gebruikers zijn op de hoogte van deze procedures voor het rapporteren van de verschillende soorten gebeurtenissen en zwakke plekken die invloed kunnen hebben op de beveiliging van de bedrijfsmiddelen.

Er is een verplichte meldingssystematiek in werking om alle informatiebeveiligingsgebeurtenissen en zwakke plekken zo snel mogelijk te rapporteren aan de aangewezen contactpersoon.

Risico's

Als incidenten niet geregistreerd worden, is niet duidelijk waar en wanneer er zich incidenten voor doen of voor hebben gedaan. Op deze wijze kan er geen lering worden getrokken uit deze incidenten om deze in de toekomst te voorkomen of om preventief betere maatregelen te implementeren.

Bijlage 9: Bedrijfscontinuïteit

Beleidsuitgangspunt

Er zijn voor de belangrijkste processen en systemen continuïteits-/uitwijkplannen welke door middel van een beheerst proces tot stand komen. Continuïteitsplannen moeten regelmatig worden getest en actueel worden gehouden.

Doelstelling

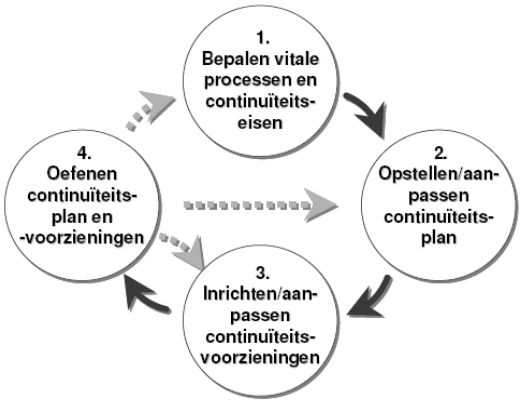
Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

Een adequaat beheerproces van bedrijfscontinuïteit om de uitwerking op de organisatie, veroorzaakt door het verlies van informatie en het herstellen daarvan tot een aanvaardbaar niveau te beperken.

Informatiebeveiliging is een integraal onderdeel van het totale bedrijfscontinuïteitsproces en andere beheerprocessen binnen de organisatie.

Risico's

- Wanneer er niet of nauwelijks invulling gegeven wordt aan de continuïteitsplanning is er naast een vals gevoel van veiligheid, ook grote kans op ad hoc maatregelen als een calamiteit zich voordoet.
- Het uitvallen van medewerkers (ziekte, sterven, ontslag) kan een reële bedreiging zijn. Zie ook de rollen en verantwoordelijkheden bij crisisbeheersing.



Figuur 4:● BCM Cyclus

Bijlage 10: Naleving

Doelstelling

Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van beveiligingseisen. Het vergroten van het beveiligingsbewustzijn.

Risico's

Naleving is een kwestie van gedrag. Op het vereiste gedrag dient toegezien te worden. Door het niet naleven van de beveiligingsvereisten en de controle daarop, worden de aanwezige bedreigingen manifest en worden kwetsbaarheden uitgebuit.

Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle gemeentelijke processen waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke team stuurt. De kwaliteit wordt gemeten aan:

- de mate waarin een volledige set aan maatregelen is geïmplementeerd, gebaseerd op vastgesteld beleid;
- efficiency en effectiviteit van de geïmplementeerde maatregelen;
- de mate waarin de informatiebeveiliging het bereiken van de strategische doelstellingen ondersteunt.

Bijlage 11: Relevante documenten en bronnen

Intern

- De gemeente kan hier zelf verwijzen naar eigen standaarden en procedures. Vanuit VNG/KING worden in 2013 nog meerdere producten geleverd die hier benoemd kunnen worden.
- Algemene Inkoop Voorwaarden, gemeente Aa en Hunze en de GIBIT.

Extern

- NEN/ISO 27001 (2005) en 27002 (Code voor Informatiebeveiliging) (2007)
- Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), KING, 2013-2015
    - Strategische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en de BIO
    - Tactische variant van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)
- AVG: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg
- GEMMA: http://www.kinggemeenten.nl/king-kwaliteitsinstituut-nederlandse-gemeenten/e-dienstverlening-verbeteren/gemma

Bijlage 12: Beveiligingseisen aan leveranciers

Inleiding

Bij het verwerven van producten of diensten is het van belang om in een vroegtijdig stadium aan mogelijke leveranciers kenbaar te maken welke beveiligingseisen de gemeente wenst te nemen, of door haar leverancier uitgevoerd wenst te zien. Dit zodat hier niet achteraf discussie over kan ontstaan. Het vroegtijdig aangeven van beveiligingseisen zorgt ervoor dat leveranciers hier ook tijdig op in kunnen spelen. De verantwoordelijkheid voor informatiebeveiliging kan niet zomaar bij een leverancier worden belegd, neem bijvoorbeeld het outsourcen van ICT-services, Cloud Computing of het bewerken van persoonsgegevens.

Doelstelling

Het aantoonbaar borgen van het IB beleid bij de leverancier

Risico's:

- Het IB beleid van de gemeente wordt niet uitgevoerd bij de leverancier.

Uitgangspunten

De beveiligingsvereisten en maatregelen dient per leverancier vastgesteld te worden. Er moeten voldoende vereisten aan leveranciers gesteld kunnen worden om dit beveiligingsbeleid te kunnen borgen. Daarom wordt ten minste het volgende vereist aan elke leverancier:

- Bij aanschaf van cloud ICT diensten wordt uitgegaan van de GIBIT (www.gibit.nl).
- Op basis van een risicoanalyse (dataclassificatie/baselinetoets) wordt vastgesteld welke normenkaders gelden en eventuele specifieke vereisten gesteld en welke maatregelen getroffen dienen te worden bij de aanbesteding van een ICT dienst/product in (in de cloud). Dit dient in een overeenkomst (verwerkersovereenkomst, SLA,…) te worden vastgelegd en geaccordeerd (handtekening management) voor leveranciers en hun onderleveranciers. Hierbij valt te denken aan:
    - Wet en regelgeving (AVG, BRP,…)
    - ISO 27001/27002 met VVT en certificaat
    - ISAE 3402 Type 1/2
    - Vereisten, maatregelen uit de BIG/BIO
    - Specifieke vereisten en maatregelen
- Mochten bestaande leveranciers nog geen beveiligingsvereisten hebben gekregen van de gemeente, dan dient dit in een (jaar)gesprek met de leverancier aan de de orde te worden gesteld en te leiden tot passende beveiligingsafspraken met de leverancier.
- Het is ten minste jaarlijkse noodzakelijk een geautoriseerde rapportage te ontvangen van de leverancier (en onderaannemers) over de werking van het beveiligingsbeleid (normenkader).
- Het functioneren van het IB beleid bij leverancier wordt ten minste jaarlijks besproken, vastgelegd en zo nodig bijgesteld. Waarvan een verslag wordt opgesteld.
- Wanneer het naar oordeel van de gemeente Aa en Hunze nodig is, kan deze een onderzoek (laten) uitvoeren naar de informatiebeveiliging bij leverancier. Deze afspraak moet worden vastgelegd in een overeenkomst met de leverancier.
- Een teamleider zorgt er voor dat aan bovenstaande binnen zijn eigen team aandacht wordt bestee, afspraken worden nageleefd en risico's aantoonbaar worden afgewogen (dataclassificatie/risicoregister).