gemeente
Het Hogeland

Informatiebeveiligings-beleid

Gemeente Het Hogeland

01-01-2020

Kenmerk:	Z.HHL.002292
Versie:	1.0
Versiedatum:	16 februari 2019
Gemaakt door:	P. Nouwen
Portefeuillehouder	Dhr. H.J. Bolding
Goedgekeurd door:	College van B&W Het Hogeland
Classificatie:	Vertrouwelijk

Versiebeheer

Versie	Datum	Auteur	Opmerkingen
0.23C	15-10-2018	Patriek Nouwen	Concept gereed voor afstemming met organisatie
1.0C	22-10-2018	Patriek Nouwen	Concept gereed voor afstemming met directieteam
1.0C	20-11-2018	Patriek Nouwen	Samengesteld college van B&W stelt beleid vast
1.0	16-02-2019	Guido Groot	Tekstuele aanpassingen

Managementsamenvatting

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor gemeenten om hun processen uit te voeren. Gemeenten beschikken over een schat aan (zeer) vertrouwelijke informatie over zowel burgers als bedrijven. Daarnaast zijn gemeenten verantwoordelijk voor een betrouwbare en continue dienstverlening. Dit informatiebeveiligingsbeleid biedt een kader voor de gemeente Het Hogeland om informatie op een passende wijze te beveiligen.

Dit kader, en daarmee ook dit beleid, is gebaseerd op de Baseline Informatiebeveiliging Gemeenten BIG. Daarnaast verwijst het beleid naar wet- en regelgeving waar altijd aan voldaan moet worden. De reikwijdte van dit beleid omvat daarom de bedrijfsvoeringprocessen, onderliggende informatiesystemen en informatie van de gemeente in de meest brede zin van het woord.

Belangrijke uitgangspunten hierbij zijn:

- Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement, met het college van B&W als bestuurlijk eindverantwoordelijke.
- Het primaire uitgangspunt voor informatiebeveiliging is en blijft risicomanagement: een gestructureerde manier om risico's en gevolgen in kaart te brengen, te evalueren en proactief te beheersen door het treffen van maatregelen.

Daarnaast beschrijft het beleid de rollen, taken en verantwoordelijkheden in de gemeente ten aanzien van informatiebeveiliging en hoe ervoor gezorgd kan worden dat informatiebeveiliging geborgd blijft binnen de gemeente.

In het beleid is middels een groeimodel aangegeven waar de gemeente naar toe wilt groeien om de beveiliging op een hoger niveau te brengen om aan gestelde normen te voldoen. Hierbij sluit het informatiebeveiligingsbeleid direct aan op de visie van Het Hogeland.

Het informatiebeveiligingsbeleid dient minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld en zo nodig te worden bijgesteld. Het beleid wordt jaarlijks uitgewerkt in een informatiebeveiligingsplan, aan de hand van nieuwe ontwikkelingen en op basis van risico's.

Inhoudsopgave

Managementsamenvatting **3**

Inhoudsopgave **5**

1 Inleiding **7**

2 Reikwijdte & afbakening **9**

3 Kader & uitgangspunten **11**

3.1 Kader 11

3.2 Uitgangspunten 12

4 Visie Het Hogeland & informatiebeveiliging **14**

4.1 Visie Het Hogeland 14

4.2 Visie en informatiebeveiliging 14

5 Organisatie van Informatiebeveiliging **17**

5.1 Rollen & verantwoordelijkheden 17

5.2 Borging van informatiebeveiliging 21

6 Risicomanagement **24**

7 Groei naar informatiebeveiliging **26**

7.1 Beveiligingsbeleid – *BIG Hfst. 5* 27

7.2 Organisatie van informatiebeveiliging – *BIG Hfst. 6* 27

7.3 Beheer van bedrijfsmiddelen – *BIG Hfst. 7* 27

7.4 Beveiliging van personeel – *BIG Hfst. 8* 27

7.5 Fysieke beveiliging en beveiliging van de omgeving – *BIG Hfst. 9* 28

7.6 Beheer van communicatie- en bedieningsprocessen – *BIG Hfst. 10* 28

7.7 Toegangsbeveiliging – *BIG Hfst. 11* 28

7.8 Verwerving, ontwikkeling en onderhoud van informatiesystemen – *BIG Hfst. 12* 28

7.9 Beheer van informatiebeveiligingsincidenten – *BIG Hfst. 13* 29

7.10 Bedrijfscontinuïteitsbeheer – *BIG Hfst. 14* 29

7.11 Naleving – BIG Hfst. 15 29

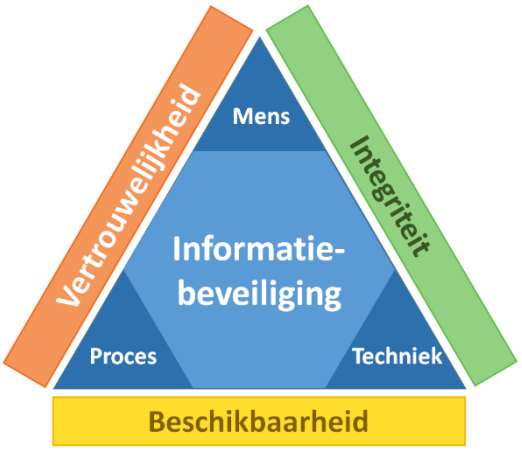
8 Bijlage I – Begrippenlijst **32**

1 Inleiding

Toegankelijke en betrouwbare overheidsinformatie is essentieel voor gemeenten om hun processen uit te voeren. Gemeenten beschikken over een schat aan (zeer) vertrouwelijke informatie over zowel burgers als bedrijven en daarnaast zijn gemeenten verantwoordelijk voor een betrouwbare en continue dienstverlening. Onze inwoners vertrouwen erop dat de gemeente hun vertrouwelijke gegevens afdoende beveiligt. Het is daarom belangrijk dat gemeenten op passende wijze hun informatie beveiligen.

Bij informatiebeveiliging is het belangrijk dat de juiste maatregelen, procedures en processen (op de gebieden Mens, Proces en Techniek) ervoor zorgen dat de beschikbaarheid, integriteit (juistheid, volledigheid en tijdigheid) en vertrouwelijkheid van informatie op het juiste niveau is beschermd. Voor het ene proces is vertrouwelijkheid van informatie belangrijker, voor het andere beschikbaarheid of integriteit. Mogelijk zijn alle aspecten van belang. Hier is weergegeven wat de gemeente verstaat onder deze begrippen.

Beschikbaarheid / continuïteit:	Het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
Integriteit / betrouwbaarheid:	Het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.
Vertrouwelijkheid / Exclusiviteit:	Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.



De gemeente wil informatiebeveiliging op een gestructureerde wijze benaderen, zodat de beveiliging op een passend niveau is en blijft, en dat beveiligingsmaatregelen effectief en efficiënt worden ingezet. Dit informatiebeveiligingsbeleid biedt algemene beleidsuitgangspunten over informatiebeveiliging. Deze uitgangspunten hebben een sterk normerend karakter en geven keuzes weer. Dit beleid is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG). Daarnaast is gebruik gemaakt van handreikingen van het Kwaliteitsinstituut Nederlandse Gemeenten (KING) en de informatiebeveiligingsdienst (IBD).

In dit beleid is weergegeven welke onderdelen vallen onder informatiebeveiliging. Vervolgens staat in het beleid welke kaders en uitgangspunten gelden voor informatiebeveiliging (zoals wet- en regelgeving) en dat risicomanagement de basis is om beveiliging toe te passen. Daarnaast is de relatie tussen de visie van de gemeente en informatiebeveiliging weergegeven. Informatiebeveiliging ontstaat niet vanzelf. In het beleid staat hoe dit moet zijn georganiseerd en hoe de rollen en verantwoordelijkheden zijn belegd. Tenslotte is op basis van de BIG weergegeven welke informatiebeveiligingsdoelen bereikt moeten worden om ook de visie van de gemeente te verwezenlijken.

Het informatiebeveiligingsbeleid moet daarnaast gezien worden als een overkoepelend beleidsstuk, waarbij in onderliggende plannen, documentatie, procedures en instructies verdere detaillering en afspraken zijn of moeten worden vastgelegd.

2 Reikwijdte & afbakening

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 (waaronder in ieder geval papier, elektronisch, foto, film, CD, DVD, USB, SD-kaart en beeldscherm) en alle informatie verwerkende systemen (applicaties, systeemprogrammatuur, databases, hardware, bijbehorende bedrijfsmiddelen), maar vooral ook mensen en processen.

De reikwijdte van dit beleid omvat daarom:

- Verantwoord en bewust gedrag van medewerkers ten aanzien van informatieveiligheid;
- De bedrijfsvoeringprocessen, onderliggende informatiesystemen en informatie van de gemeente, inclusief bescherming van privacy en vitale maatschappelijke functies onder verantwoordelijkheid van de gemeente (verkeer, vervoer, openbare orde en veiligheid, etc.);
- Alle ruimten van een gemeentehuis en aanverwante gebouwen, alsook op apparaten die door medewerkers van de gemeente (intern en extern) gebruikt worden bij de uitoefening van hun taak op diverse locaties;
- Informatie die namens de gemeente wordt verwerkt door externe partijen (zowel samenwerkingsverbanden, afnemers en leveranciers). Ook als de hiervoor gebruikte systemen niet binnen de gemeente draaien.

3 Kader & uitgangspunten

Het bestuur en het directieteam spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo maakt het directieteam een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente hebben, de risico's die de gemeente loopt in de informatievoorziening en welke van deze risico's onacceptabel hoog zijn. Op basis hiervan draagt het directieteam dit beleid voor informatiebeveiliging uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het directieteam geeft duidelijke richting aan informatiebeveiliging en laat zien in woord en daad dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van dit informatiebeveiligingsbeleid van en voor de hele gemeente. Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

3.1 Kader

De gemeente is zelf verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hierbij geldt:

- Er is wet- en regelgeving waar altijd aan voldaan moet worden, zoals (niet uitputtend!) bijvoorbeeld voor:
  - Uitvoeringswet) Algemene Verordening Gegevensbescherming – (U)AVG;
  - asisregistratie Personen – BRP;
  - aspoortuitvoerregeling Nederland 2001 – PUN;
  - tructuur Uitvoeringsorganisatie Werk en Inkomen – SUWI;
  - igiD;
  - urgerservicenummer – BSN;
  - asisregistratie Adressen en Gebouwen – BAG;
  - asisregistratie Grootschalige Topografie – BGT;
  - asisregistratie Ondergrond – BRO;
  - urgerlijk Wetboek – BW;
  - et openbaarheid van bestuur – Wob;
  - et hergebruik van overheidsinformatie – Who;
  - uteurswet – Aw;
  - lgemene wet bestuursrecht – Awb;

- et elektronisch bestuurlijk verkeer; en de,
- rchiefwet 1995.

De wet- en regelgeving kan tot gevolg hebben dat hieruit maatregelen ontstaan op het gebied van informatiebeveiliging.

- De gemeente hanteert de Baseline Informatiebeveiliging Gemeenten (BIG) als normenkader. Dit normenkader wordt door alle Nederlandse gemeenten gehanteerd op basis van de door de Bijzondere Algemene Ledenvergadering (BALV) van de VNG in 2013 vastgestelde resolutie “Informatieveiligheid, randvoorwaarde voor de professionele gemeente”. De BIG is gebaseerd op de ISO 27001:2005 en ISO 27002:2007.
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor risicoafweging en prioritering op basis van het ‘pas toe of leg uit’ principe.

3.2 Uitgangspunten

De volgende uitgangspunten zijn ontleend aan de Code voor Informatiebeveiliging (NEN/ISO 27002:2007) en de Baseline Informatiebeveiliging Gemeenten (BIG):

1. Informatie en informatiesystemen zijn van kritiek en vitaal belang voor de gemeente. Informatiebeveiliging is en blijft een verantwoordelijkheid van het lijnmanagement. De ambtelijke verantwoordelijkheid voor informatiebeveiliging ligt bij de directie, met het **college van B&W als bestuurlijk eindverantwoordelijke**. Proceseigenaren, applicatie-eigenaren en gegevenseigenaren hebben hierbij ieder hun eigen, maar ook gezamenlijke verantwoordelijkheid ten aanzien van informatiebeveiliging en het uitdragen van het belang hiervan. De verantwoordelijkheden voor de bescherming van gegevens en voor het uitvoeren van beveiligingsprocedures zijn expliciet gedefinieerd.
2. Het primaire uitgangspunt voor informatiebeveiliging is en blijft **risicomanagement**.
3. Door **periodieke controle, organisatiebrede planning én coördinatie** wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses.
4. Informatiebeveiliging is een **continu verbeterproces** en is opgenomen in de Planning & Control-cyclus. Informatiebeveiliging sluit daarbij aan op de voor gemeenten gehanteerde verantwoordingssystematiek (ENSIA) en bijbehorende termijnen. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
5. Dit informatiebeveiligingsbeleid is leidend. Processen of organisatieonderdelen kunnen een specifiek informatiebeveiligingsbeleid hebben dat aansluit bij dit overkoepelende beleid.
6. De organisatiebrede CISO - binnen de gemeente Het Hogeland aangeduid als de CISO of informatiebeveiligingsfunctionaris - ondersteunt vanuit een **onafhankelijke positie** de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover.
7. De organisatie kent deelfuncties ten aanzien van informatiebeveiliging:
   - oor Suwinet: Security Officer Suwinet

- oor reisdocumenten en rijbewijzen: Beveiligingsfunctionaris Burgerzaken
  Deze functies zijn uitgewerkt in het specifieke informatiebeveiligingsbeleid en/of -procedures voor deze processen.

8. Om de informatiebeveiliging af te stemmen op interne en externe ontwikkelingen wordt (tenminste) tweejaarlijks een risicoanalyse uitgevoerd. Of zodra wijzigingen in de omgeving, technische wijzigingen of dreigingsveranderingen hier aanleiding voor geven.
9. De gemeente (en daarmee de gemeenteraad, het college van B&W, het directieteam, proceseigenaren, applicatie-eigenaren en gegevenseigenaren) stelt de benodigde **mensen, tijd en middelen** beschikbaar om haar eigendommen en werkprocessen, alsmede de fysieke en digitale veiligheid van medewerkers, te kunnen beveiligen volgens de wijze gesteld in dit beleid.
10. **Regels en verantwoordelijkheden** voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld. Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
11. 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.

4 Visie Het Hogeland & informatiebeveiliging

Een informatiebeveiligingsbeleid dient afgestemd te zijn op de (interne en externe) omgeving waarin het beleid wordt gebruikt, op de toekomst en op het beleid en de visie van de organisatie. In dit hoofdstuk wordt ingegaan op de visie van Het Hogeland en haar relatie met informatiebeveiliging.

4.1 Visie Het Hogeland

De gemeente Het Hogeland streeft naar een organisatie die ongeacht haar grote woonoppervlak en de vele dorpskernen, dicht bij haar inwoners staat. In een tijd van snelle veranderingen is het van groot belang dat de overheid de vragen en de behoeften van haar inwoners kent, en van maatschappelijke organisaties en bedrijven, om daar adequaat op te kunnen inspelen en reageren.

De dienstverlening is daarbij dienstbaar, maar ook modern, klant- en servicegericht, flexibel, snel, effectief en efficiënt. Digitale dienstverlening wordt steeds belangrijker: e-mail, website, telefoon, sociale media, digitale berichtenservices en apps zijn logische onderdelen van de dienstverlening.

Dit vraagt om een wendbare organisatie die regelarm is en maatwerk kan bieden. Een organisatie waarin integraal gewerkt kan worden. Het Hogeland wil een gemeente zijn die een wendbare organisatiestructuur heeft, die slagvaardig handelen mogelijk maakt. Verschillende organisatieonderdelen moeten daar waar nodig met elkaar in verbinding kunnen staan. Zowel intern als extern.

De ruimtelijke verspreiding van de gemeente, de noodzaak tot integraal werken, en de behoefte van medewerkers die steeds meer zelfstandigheid willen over hoe, waar en wanneer zij hun werk indelen leiden tot de wens van tijd- en plaatsonafhankelijk werken.

De gemeente wil daarbij medewerkers de ruimte bieden om haar processen zelf in te richten, waarbij zelforganiserende teams het uitgangspunt zijn. Eigenaarschap van medewerkers of teams is het middel om dit te realiseren. Eigenaarschap is niet vrijblijvend – het gaat gepaard met het nemen en voelen van verantwoordelijkheid. De leidinggevenden gaan hierbij niet zozeer over de inhoud, maar beschikken over coachende vaardigheden om het team en de medewerkers te laten groeien naar zelfstandigheid en verantwoordelijkheid.

4.2 Visie en informatiebeveiliging

De informatievoorziening van de gemeente moet erin kunnen voorzien om bovenstaande visie te kunnen realiseren. Ook zijn er normen waaraan iedere gemeente zich dient te houden. Zo dient de gemeente zich te houden aan wet- en regelgeving, heeft zij afspraken gemaakt met andere partijen en mogen burgers van de gemeente verwachten dat integer met hun informatie wordt omgegaan. Om binnen de visie van Het Hogeland en binnen de gestelde kaders de informatievoorziening optimaal te kunnen laten werken, zijn op zowel technisch als organisatorisch vlak acties vereist.

- Indien de gemeente goed wil kunnen inspelen op de behoeftes van de samenleving vraagt dit om juiste, volledige en tijdige informatie.
- Een zelforganiserende organisatie vraagt om verantwoordelijkheid voor en eigenaarschap van het proces, maar ook van applicaties en de gegevens waarmee gewerkt wordt.

- Integraal werken gebeurt binnen de kaders van wet- en regelgeving, waarbij het belang van de burger voorop staat. Informatie-uitwisseling gebeurt op een veilige wijze waarbij de fysieke en logische toegang voor ongeautoriseerden wordt voorkomen.
- Een zelforganiserende organisatie met een flexibele organisatiestructuur vereist strak autorisatiemanagement en change management die de flexibiliteit van de organisatie kan ondersteunen.
- Tijd- en plaatsonafhankelijk werken vraagt om zowel technisch als fysiek flexibele werkplekken, waarbij informatie ook tijd- en plaatsonafhankelijk beschikbaar is. Dit vraagt om een meer digitale manier van werken en veilige oplossingen voor het bewaren (en transporteren) van fysieke informatie.
- Een goede digitale dienstverlening vraagt om technisch volwassen oplossingen, een organisatie die haar basis op orde heeft en deze oplossingen ondersteunt. Dit geldt voor oplossingen die binnen onze gemeente draaien, maar evenzeer zo voor externe oplossingen.

Dit informatiebeveiligingsbeleid zal samen met het informatiebeveiligingsplan en –procedures een kader bieden waarbinnen de organisatie kan opereren, maar zal ook ondersteunend zijn om de visie van de organisatie te kunnen realiseren.

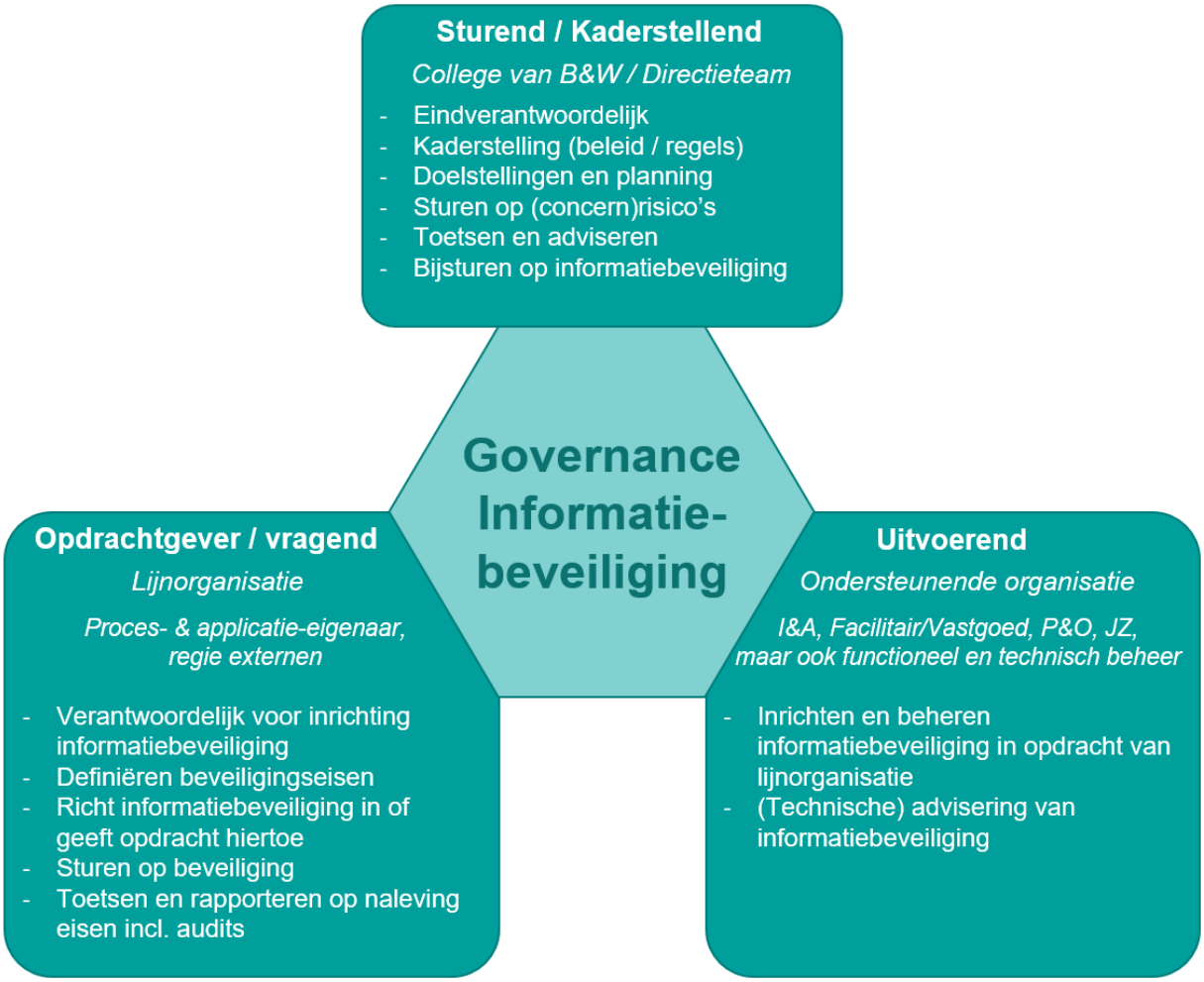
5 Organisatie van Informatiebeveiliging

Dit hoofdstuk gaat in op rollen en verantwoordelijkheden (5.1) en op de borging van informatie-beveiliging (5.2). Een adequaat opgezette informatiebeveiliging vereist een governance structuur waarin rollen en verantwoordelijkheden op het gebied van Informatiebeveiliging zijn gedefinieerd en waarmee de besluitvorming, rapportage en escalatiestructuren met betrekking tot dit onderwerp zijn gereguleerd. Zoals eerder in 3.2 Uitgangspunten is gesteld dient de Plan-Do-Check-Act-cyclus te worden toegepast op alle informatiebeveiligingsaspecten om informatiebeveiliging te borgen in de organisatie. Het beleid biedt hiermee een kader voor waar de gemeente naar toe dient te groeien ten aanzien van de organisatie van informatiebeveiliging.

5.1 Rollen & verantwoordelijkheden

In dit onderdeel zijn de belangrijkste rollen en verantwoordelijkheden ten aanzien van informatiebeveiliging beschreven. De precieze invulling van de rollen en verantwoordelijkheden dient te zijn beschreven in (onderliggende) beleidstukken, kaderstellingen, procedures en werkinstructies.

De aansturing ten aanzien van informatiebeveiliging moet vooral komen vanuit organisatieonderdelen die verantwoordelijk zijn voor de bedrijfsprocessen en hun behoefte/vraag naar informatiebeveiliging. Er moet dus een duidelijk onderscheid zijn tussen regie en uitvoering. Dit houdt mede in dat de lijnorganisatie de rol van opdrachtgever op zich neemt en ondersteunende organisatieonderdelen de uitvoerende rol op zich nemen. Het college van B&W en de directie bevinden zich in de sturende rol. Zij zetten de kaders uit en bepalen de doelen die behaald moeten worden.



Gemeenteraad
De gemeenteraad stelt middelen beschikbaar voor informatiebeveiliging. Daarnaast heeft de gemeenteraad een controlerende functie ten aanzien van de informatiebeveiliging.

College van Burgemeester & Wethouders
Het college van B&W is in de sturende rol eindverantwoordelijk voor de adequate beveiliging van informatie binnen de gemeente. Een lid van het college heeft informatiebeveiliging expliciet in de portefeuille. Het is de verantwoordelijkheid van het college om dit proces te faciliteren door:

- Het informatiebeveiligingsbeleid vast te stellen;
- Toezicht te houden op de uitvoering van het informatiebeveiligingsbeleid;
- Ervoor te zorgen dat voldoende middelen beschikbaar gesteld worden voor de adequate inrichting van informatiebeveiliging;
- Risico's te beoordelen en keuzes te maken.

Directieteam
Het directieteam is in haar sturende rol verantwoordelijk voor de kaderstelling en de invulling van het informatiebeveiligingsbeleid. Een lid van het directieteam heeft informatiebeveiliging expliciet in het takenpakket. De directie zorgt ervoor dat zij:

- Stuurt op bedrijfsrisico's;
- Controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
- Toezicht houdt op de uitvoering van het informatiebeveiligingsplan;
- Een positieve en actieve houding heeft ten aanzien van informatiebeveiliging;
- Zorg draagt dat de medewerkers voldoende security training krijgen om de taken goed te kunnen uitvoeren;
- Fungeert als voorbeeld richting de medewerkers.

Chief Information Security Officer (Informatiebeveiligingsfunctionaris)
De CISO is verantwoordelijk voor de *organisatie* van informatiebeveiliging. Dit is een rol op strategisch niveau binnen de gemeentelijke organisatie. De CISO heeft als taak informatieveiligheid op een hoger niveau te brengen en om het vervolgens structureel te laten borgen in de organisatie. De lijnorganisatie blijft zelf verantwoordelijk voor informatiebeveiliging. De belangrijkste bevoegdheid van de CISO is om op elke plek binnen de organisatie gevraagd en ongevraagd onderzoek te kunnen (laten) doen en zo nodig zaken voor te schrijven. De taken van de CISO ten aanzien van informatiebeveiliging zijn als volgt samen te vatten:

- Beleid & Coördinatie
- Controle & Registratie
- Communicatie & Voorlichting
- Advies & Rapportage

Functionaris Gegevensbescherming
De Functionaris Gegevensbescherming (FG) houdt zich bezig met alle privacyaspecten binnen de gemeente. De functie is onafhankelijk van de lijn belegd en de functionaris heeft de bevoegdheid om rechtstreeks naar de gemeentesecretaris of het college van B&W te rapporteren. De taken van de FG zijn:

- Adviseren (zowel gevraagd als ongevraagd) over vraagstukken die te maken hebben met de omgang met persoonsgegevens;
- Toezien op de naleving van de AVG en andere privacy-gerelateerde wet- en regelgeving binnen de organisatie;
- Het informeren van de organisatie betreffende de AVG en andere privacy-gerelateerde wet- en regelgeving;
- Het zijn van een contactpunt voor betrokkenen (dit kunnen zowel inwoners als medewerkers zijn) m.b.t. de omgang met persoonsgegevens. De FG is daarbij gehouden aan geheimhouding;
- Het coördineren van de afhandeling van datalekken conform de vastgestelde datalekprocedure;
- Het contactpunt met de Autoriteit Persoonsgegevens.

Beveiligingsfunctionaris Burgerzaken

De beveiligingsfunctionaris is bevoegd om een jaarlijks intern onderzoek in te stellen naar de werking van de beveiligingsprocedures ten aanzien van reisdocumenten en rijbewijzen. Het college van B&W krijgt inzicht in de rapportage van bevindingen.

Security Officer Suwinet

De Security Officer Suwinet is binnen de organisatie toezichthouder betreffende alle activiteiten op het gebied van informatiebeveiliging rondom Suwinet en rapporteert direct aan B&W.

Veiligheidscommissie

De veiligheidscommissie bestaat uit de CISO, de FG en medewerkers van verscheidene teams en waarborgt dat informatiebeveiliging met een integrale blik wordt bekeken. Dit heeft als doel:

- een brede, structurele betrokkenheid vanuit de organisatie ten aanzien van informatiebeveiliging;
- het (sneller) signaleren van risico’s op het gebied van informatiebeveiliging;
- een verbeterde afstemming, formulering en implementatie van verbeteracties en maatregelen;
- verschillende disciplines met elkaar in contact te brengen ten aanzien van informatiebeveiliging;
- het doen van voorstellen voor het prioriteren en plannen van beveiligingsmaatregelen op basis van risicoanalyse;
- klankbord voor de organisatie en directieteam ten aanzien van informatiebeveiliging.

Proceseigenaren

Ieder proces dient een proceseigenaar te hebben. De proceseigenaar (opdrachtgevende / vragende rol) heeft de bevoegdheid om te bepalen hoe een proces verloopt, en heeft de verantwoordelijkheid ervoor te zorgen dat het proces aan het gemeentelijk beleid, de klantverwachtingen en bedrijfsdoelstellingen blijft voldoen.

Degene gaat dus over de inrichting en het ontwerp van het proces, als ook over de resultaten van het proces. Hiervoor dient de proceseigenaar het proces te hebben geanalyseerd, risico’s in kaart te hebben gebracht en passende maatregelen te hebben getroffen.

Proceseigenaren dienen de teamcoaches, de directie en bestuur van voldoende informatie te voorzien, zodat deze in staat zijn om geïnformeerde beslissingen te nemen ten aanzien van informatiebeveiligings-kwesties betreffende het proces.

Applicatie-eigenaren

Voor iedere significante vakapplicatie dient in de lijnorganisatie een applicatie-eigenaar te zijn belegd. De applicatie-eigenaar (opdrachtgevende / vragende rol) heeft de bevoegdheid om te bepalen hoe de applicatie is ingericht, en heeft de verantwoordelijkheid ervoor te zorgen dat de applicatie aan het gemeentelijk beleid, informatiebeleid, de klantverwachtingen en bedrijfsdoelstellingen blijft voldoen.

Degene gaat dus over de inrichting en het ontwerp van applicatie, als ook over de resultaten van de werking van de applicatie. Hiervoor dient de applicatie-eigenaar de applicatie en bijbehorende bedrijfsproces(sen) te hebben geanalyseerd, risico's in kaart te hebben gebracht en passende maatregelen te hebben getroffen.

Applicatie-eigenaren dienen de teamcoaches, de directie en bestuur van voldoende informatie te voorzien zodat deze in staat zijn om geïnformeerde beslissingen te nemen ten aanzien van informatiebeveiligings-kwesties betreffende de applicatie. Het kan zijn dat de proces- en de applicatie-eigenaar in één persoon gecombineerd zijn.

Applicatiebeheerders

De applicatiebeheerder (uitvoerende rol) zorgt ervoor dat de applicatie is ingericht conform de daarvoor gestelde eisen en richtlijnen van de applicatie-eigenaar. De applicatiebeheerder is verantwoordelijk voor het in stand houden van de programmatuur waarmee de functionaliteit van een applicatie wordt gerealiseerd en van de gegevensverzamelingen waarop die programmatuur verwerkingen uitvoert.

Regierol externen

Voor iedere uitbesteding en bij ieder samenwerkingsverband moet een regierol zijn belegd binnen de gemeente. Deze regierol houdt toezicht op de uitvoering van de uitbestede werkzaamheden en stuurt zo nodig bij. Degene die de regie houdt ten aanzien van externen heeft de bevoegdheid om te bepalen aan welke eisen een extern of uitbesteed proces dient te voldoen, en heeft de verantwoordelijkheid om ervoor te zorgen dat dit proces aan de klantverwachtingen en bedrijfsdoelstellingen blijft voldoen.

Degene heeft de bevoegdheid om eisen te stellen aan de aannemer van externe of uitbestede processen. Hiervoor dient de regisseur het externe proces te hebben geanalyseerd, risico's in kaart te hebben gebracht en passende maatregelen te hebben afgestemd of getroffen.

Zij dienen de teamleiders/coaches, de directie en bestuur van voldoende informatie te voorzien zodat deze in staat zijn om geïnformeerde beslissingen te nemen ten aanzien van informatiebeveiligings-kwesties betreffende de regie van externen.

Ondersteunende teams

De ondersteunende teams (I&A, Facilitair, Vastgoed, HRM, Juridische Zaken, e.d. in de uitvoerende rol) zijn verantwoordelijk voor:

- de beveiliging van de informatievoorziening en implementatie van beveiligingsmaatregelen, die voortvloeien uit betrouwbaarheidseisen (classificaties) voor zover deze maatregelen niet in het proces door de proceseigenaar getroffen kunnen worden;
- voor alle beheeraspecten van informatiebeveiliging;
- logging, monitoring en rapportage;
- (technisch) beveiligingsadvies klanten.

De lijnorganisatie blijft als opdrachtgevende en vragende partij eindverantwoordelijk voor de informatiebeveiliging van haar processen. Er is geen overdracht van verantwoordelijkheden.

Teamcoaches

De teamcoach is primair gericht op het managen en regisseren van mensen en processen (volgens de principes van integraal management) en leert de medewerkers zelforganiserend te zijn. Dit kan betekenen dat ten aanzien van informatiebeveiliging de coach ook de proceseigenaar zal zijn en mogelijk de applicatie-eigenaar. Daarnaast betekent dit dat de coach:

- waarborgt dat de medewerkers over voldoende kennis en kunde (blijven) beschikken ten aanzien van informatiebeveiliging om hun functie goed uit te kunnen voeren. Dit is inclusief digitale vaardigheden. De benodigde kennis en kunde kunnen van functie tot functie verschillen;
- stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- rapporteert over compliance aan wet- en regelgeving en algemeen beleid van de gemeente.

Medewerkers

Op basis van het integriteitsbeleid Het Hogeland, is iedere medewerker in het kader van informatiebeveiliging verplicht tot:

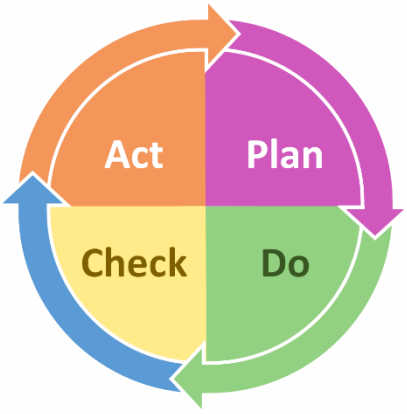
- het vertrouwelijk houden van informatie en wachtwoorden en andere vormen van toegangscodes in het bijzonder;
- het voldoen aan alle wettelijke verplichtingen;
- het conform interne regelgeving op veilige manier gebruiken van ICT middelen;
- het gebruik van software in overeenstemming met de voorwaarden uit licentieovereenkomsten;
- het dusdanig omgaan met informatie en informatiemiddelen dat de beschikbaarheid, integriteit en betrouwbaarheid daarvan niet in gevaar komt.

Naast deze persoonlijke verantwoordelijkheid geldt voor iedere medewerker van de gemeente dat het gemeenschappelijke belang vereist dat men oog heeft voor de wijze waarop collega’s omgaan met informatie en dat incidenten op dit punt worden gesignaleerd.

5.2 Borging van informatiebeveiliging

Informatiebeveiliging is een continu verbeterproces. Om te waarborgen dat informatiebeveiliging niet slechts een eenmalige actie is, dient informatiebeveiliging te zijn geborgd in de organisatie. Hiertoe hanteert de gemeente de Plan-Do-Check-Act-cyclus voor alle informatiebeveiligingsaspecten. Dit vormt de basis voor het Information Security Management Systeem (ISMS). De CISO houdt (middels ISMS) bij wat de status is van informatiebeveiliging en houdt in de gaten hoe de organisatie dit borgt. Iedere medewerker die verantwoordelijk is voor een aspect van informatiebeveiliging, past de Plan-Do-Check-Act-cyclus toe op de informatiebeveiligingsaspecten waar degene bij betrokken is.

In de Plan-fase wordt vastgesteld welke maatregelen benodigd zijn om het risico tot een acceptabel niveau terug te brengen en wie verantwoordelijk is voor implementatie. Maatregelen moeten zo zijn opgebouwd dat al in de (combinatie van) maatregelen de PDCA-cyclus is opgenomen. Als dit plan is gerealiseerd, kunnen de maatregelen worden getroffen (Do). Vervolgens wordt gecontroleerd of die maatregelen het gewenste effect sorteren



(Check). Indien noodzakelijk kan men beslissen om bij te sturen (Act), waarna opnieuw de PDCA-cyclus begint bij het vaststellen wat veranderd dient te worden en hoe dit gerealiseerd wordt.

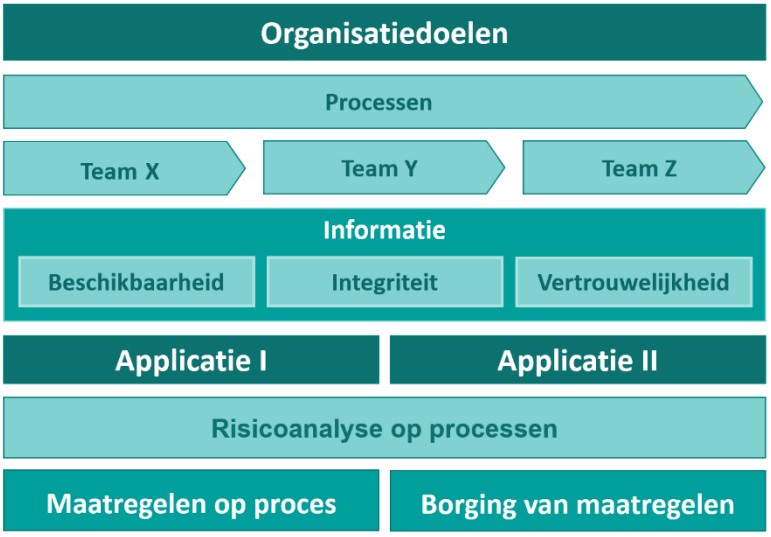
Ook als bijsturing na een eerste implementatie niet noodzakelijk is, dient met regelmaat gecontroleerd te worden of de maatregelen nog steeds het gewenste effect sorteren. Maatregelen kunnen in de tijd gezien veranderen (omdat bedreigingen en risico's ook veranderen). Dus de controle kan aanleiding geven tot bijsturing in de maatregelen. Daarnaast kan het totaalpakket van eisen, maatregelen en controle aan een herijking toe zijn (evaluatie). Het goed doorlopen van de stappen kan op elk moment zorgen voor een passend beveiligingsniveau.

Bijsturing informatiebeveiligingsbeleid en -plan

Ook ten aanzien van het overkoepelende beleid geldt de PDCA-cyclus. Het informatiebeveiligingsbeleid dient minimaal één keer per drie jaar, of zodra zich belangrijke wijzigingen voordoen, te worden beoordeeld en zo nodig te worden bijgesteld. Bij dit informatiebeveiligingsbeleid hoort ook een informatiebeveiligingsplan opgesteld te zijn. Hierin is concreet gemaakt welke acties en welke maatregelen genomen moeten worden en zijn deze acties en maatregelen in een planning opgenomen. De gemeente dient dit plan (tenminste jaarlijks) aan de hand van nieuwe ontwikkelingen en op basis van risico's te actualiseren. Het college stelt het informatiebeveiligingsbeleid vast, waar de directie het informatiebeveiligingsplan vaststelt. De eventuele benodigde middelen worden conform de P&C-cyclus van de gemeente in de begroting aangevraagd.

6 Risicomanagement

Informatiebeveiliging wordt vaak gezien als iets wat er extra bij komt. Informatie-beveiliging ligt echter ten grondslag aan het organisatiedoel dat bereikt dient te worden. Om een doel te bereiken, dienen processen uitgevoerd te worden waarvoor informatie (vaak in meerdere softwareapplicaties) wordt verwerkt. Een goede afweging van de risico's helpt om de juiste maatregelen te treffen om de gegevens in deze processen te beschermen. Hoe waardevoller of gevoeliger de informatie, hoe meer maatregelen er getroffen moeten worden. Tenslotte moeten deze maatregelen in de organisatie geborgd worden, zodat de gemeente aantoonbaar grip houdt op de veiligheid.



100% beveiliging bestaat echter niet en dient ook niet nagestreefd te worden. De kosten van beveiliging moeten in verhouding zijn tot de risico's (geen dubbeltje met een kwartje beveiligen). De aanpak van informatiebeveiliging (Informatiebeveiligingsbeleid) in Het Hogeland is daarom ook 'risk based'. Bij informatiebeveiliging gaat het om het vinden van een optimale balans tussen risico's, maatregelen, kosten en werkbaarheid. Hierbij kan het voorkomen dat een risico zich manifesteert, ondanks de getroffen maatregelen. Het is wel van belang dat de risico's bekend zijn en dat een bewuste afweging is gemaakt over de te nemen risico's. Daarnaast dient de gemeente goed te zijn voorbereid op incidenten en crises. Het informatiebeveiligingsrisico is de som van de kans op beveiligingsincidenten en de impact daarvan op het werkproces: **risico = kans x impact**.

Risicomanagement is gestructureerde manier om risico's en gevolgen in kaart te brengen, te evalueren en pro-actief te beheersen door het treffen van maatregelen. De proceseigenaar dient periodiek de risico's te beoordelen. Daartoe inventariseert de proceseigenaar de kwetsbaarheid van zijn werkproces en de dreigingen die kunnen leiden tot een beveiligingsincident, rekening houdend met de beveiligingseisen van de informatie. De proceseigenaar neemt indien nodig maatregelen om de risico's te beperken. De CISO kan hierbij ondersteunen in zowel techniek van risicoanalyse als bij de inhoudelijke analyse zelf. Hierbij kunnen ook applicatie-eigenaren en procesdeskundigen ondersteunen.

De risk-based benadering betekent ook dat gefundeerd afgeweken kan worden van de baseline (BIG) indien de gemeente hier een geaccepteerd risico loopt. Tegelijkertijd houdt dit in dat mogelijk meer maatregelen getroffen moeten worden ten opzichte van de baseline indien de gemeente een hoog risico loopt. Risicomanagement is dus de eerste stap bij informatiebeveiliging.

Op deze wijze worden tijd, geld en middelen passend besteed met als gevolg een stelsel van beveiligingsmaatregelen dat bij de gemeente past.

7 Groei naar informatiebeveiliging

In de voorgaande hoofdstukken van het beleid is het speelbord beschreven (reikwijdte & afbakening), zijn de spelregels beschreven (kader & uitgangspunten), is aangegeven wat ieders rol is en hoe informatiebeveiliging geborgd kan worden (Organisatie van Informatiebeveiliging en Risicomanagement). Ofwel, de structuur is beschreven.

In dit hoofdstuk is aangegeven welke stappen de gemeente tenminste dient te nemen om te groeien naar een voldoende niveau van informatiebeveiliging. Een beleid is niet alleen een stuk waar de organisatie aan dient te voldoen. Het is ook een stuk dat een leidraad biedt voor waar de organisatie naar toe groeit. Hierbij zetten we in op 11 informatiebeveiligingsgebieden die aansluiten bij de BIG. Proceseigenaren en applicatie-eigenaren zijn geacht op basis van risicoanalyse de BIG-normen toe te passen op hun eigen verantwoordelijkheidsgebied. Hierbij mag gefundeerd worden afgeweken, maar de gemeente dient in ieder geval te voldoen aan wet- en regelgeving en steeds verder te professionaliseren waardoor risico's beperkt worden.

Per informatiebeveiligingsgebied is een ontwikkeldoel weergegeven hoe de organisatie gaat voldoen aan de baseline en hoe de organisatie op een hoger volwassenheidsniveau komt. Hierbij is het doel om voor alle structurele processen in de organisatie om tenminste op *volwassenheidsniveau 3* te opereren. Hierbij ligt een focus op de informatiebeveiligingsprocessen bij I&A, Facilitair, Vastgoed, en P&O en bij teams die met gevoelige informatie of (bijzondere) persoonsgegevens werken.

Volwassenheidsniveau's:

Niveau	Naam	Omschrijving	Criteria
1	**Initieel**	Beheersmaatregelen zijn niet of gedeeltelijk gedefinieerd en/of worden op inconsistente wijze uitgevoerd. Grote afhankelijkheid van individuen.	• Geen of beperkte beheersmaatregelen geïmplementeerd • Niet of ad-hoc uitgevoerd • Niet/deels gedocumenteerd • Wijze van uitvoering afhankelijk van individu
2	**Herhaalbaar maar intuïtief**	Beheersmaatregelen zijn aanwezig en worden op consistente en gestructureerde, maar op informele wijze uitgevoerd.	• Maatregelen zijn geïmplementeerd • Uitvoering is consistent en standaard • Informeel en grotendeels gedocumenteerd • Inconsistente wijze van meten en controleren
3	**Gedefinieerd**	Beheersmaatregelen zijn gedocumenteerd en worden op gestructureerde en geformaliseerde wijze uitgevoerd. De uitvoering is aantoonbaar.	• Maatregelen zijn gedefinieerd o.b.v. risico assessment • Gedocumenteerd en geformaliseerd • Verantwoordelijkheden en taken eenduidig toegewezen • Controle en monitoring ontstaat • Opzet, bestaan en effectieve werking aantoonbaar
4	**Beheerst en meetbaar**	De effectiviteit van de beheersmaatregelen wordt periodiek geëvalueerd en kwalitatief gecontroleerd.	• Periodieke (control) evaluatie en opvolging vindt plaats • Rapportage richting management vindt plaats
5	**Continu verbeteren**	Een ecosysteem is verankerd en draagt zorg voor een continue en effectieve controle en risico beheersing	• Self-assessment, gap en root cause analyses • Real time monitoring • Inzet automated tooling

Handreiking bij Volwasssenheidsmodel Informatiebeveiliging, NBA (2016)

In dit beleid is per deelgebied het voornaamste (groei)doel van de gemeente beschreven. Daarnaast is het voornaamste risico beschreven indien de maatregelen op dit deelgebied niet toereikend zijn. Er zijn echter nog andere beheersdoelstellingen en beveiligingsmaatregelen. Hiervoor dienen verantwoordelijken van informatiebeveiligingsaspecten de tactische BIG te raadplegen. Hiervoor is een verwijzing naar het hoofdstuk van de BIG opgenomen.

7.1 Beveiligingsbeleid – *BIG Hfst. 5*

Ontwikkeldoel

Onderliggende beleidstukken, kaderstellingen, procedures en werkinstructies dienen te zijn opgesteld zodat processen op gestructureerde en geformaliseerde wijze worden uitgevoerd en informatiebeveiliging in overeenstemming met het beleid is. De uitvoering is aantoonbaar.

7.2 Organisatie van informatiebeveiliging – *BIG Hfst. 6*

Zie voor de governance en borging van informatiebeveiliging ook hoofdstuk 6: Organisatie van informatiebeveiliging. Dit dient inhoudelijk verder uitgewerkt te zijn in (onderliggende) beleidstukken, kaderstellingen, procedures en werkinstructies.

Ontwikkeldoel

Informatiebeveiliging borgen in de organisatie door duidelijk gedefinieerd te hebben wie waarvoor verantwoordelijk is en een proces op te zetten dat zorgt voor continue borging en verbetering.

Hierbij groeit de gemeente toe naar een zelforganiserende organisatie waarbij een transitie plaatsvindt van controle en beheersing van informatiebeveiliging door management en teamleiders naar controle en beheersing vanuit regiehouders van externen, proceseigenaren en applicatie-eigenaren. De directie stuurt op eigenaarschap.

Bij veranderingen en vernieuwingen (onder andere van applicaties) zorgt de eigenaar voor een gedegen risicoanalyse waarbij informatiebeveiliging standaard wordt beoordeeld.

7.3 Beheer van bedrijfsmiddelen – *BIG Hfst. 7*

Ontwikkeldoel

Elk bedrijfsmiddel dat een (significant) belang heeft voor de organisatie is verbonden aan een verantwoordelijke proces-, applicatie-, of data-eigenaar. De verantwoordelijke kent (in overleg met stakeholders) op basis van de mate van beschikbaarheid, integriteit en vertrouwelijkheid de classificatie toe aan het bedrijfsmiddel. Dit bedrijfsmiddel is beschermd in overeenstemming met de hieraan toegekende classificatie. De gemeente handhaaft de bescherming van bedrijfsmiddelen zodat de informatie op een passend niveau beschermd blijft.

7.4 Beveiliging van personeel – *BIG Hfst. 8*

Ontwikkeldoel

(Externe) medewerkers zijn afdoende getraind en beschikken over de kennis van informatiebeveiliging die voor hun functie benodigd is. Hierbij is speciaal aandacht voor teamleiders/coaches, projectmanagers, proceseigenaren, applicatie-eigenaren, applicatiebeheerders en functies die met gevoelige informatie of (bijzondere) persoonsgegevens werken.

Er is een beheerst instroom-doorstroom-uitstroom-proces dat waarborgt dat de juiste autorisaties en middelen tijdig en uitsluitend voor de juiste functies beschikbaar zijn. Dit proces is goed afgestemd op

het identiteits- en autorisatiemanagementproces en is strak ingericht zodat het tijdig op veranderingen in de organisatie kan inspelen.

7.5 Fysieke beveiliging en beveiliging van de omgeving – *BIG Hfst. 9*

Ontwikkeldoel

De middelen en gegevens, maar ook personen die benodigd zijn om de gemeentelijke processen uit te voeren zijn afdoende fysiek beschermd tegen uitval en tegen onbevoegd gebruik of inzage. Het geheel aan maatregelen kan per omgeving/gebouw verschillen, maar het beveiligingsniveau dient in overeenstemming met de dataclassificatie van de gegevens te zijn. De gemeentehuizen willen openheid en transparantie uitstralen, maar tegelijkertijd is het van belang dat gegevens voldoende beveiligd zijn. Ook het tijd- en plaatsonafhankelijk werken mag niet ten koste gaan van de beveiliging van de gegevens. Ook niet tijdens transport. In ieder geval geldt dat werkplekken waar medewerkers met gevoelige gegevens werken afdoende fysiek zijn beveiligd tegen toegang door onbevoegden.

7.6 Beheer van communicatie- en bedieningsprocessen – *BIG Hfst. 10*

Ontwikkeldoel

Het beheer van communicatie- en bedieningsprocessen omvat onder meer de algehele processen rondom IT Operations (waaronder wijzigingsbeheer, regie en controle ten aanzien van derde partijen, antivirus, back-up, netwerkbeveiliging, fysieke / digitale informatie-uitwisseling en logging). Bij al deze processen is het van belang dat de gemeente op volwassenheidsniveau 3 “Gedefinieerd” opereert waarbij maatregelen zijn gedefinieerd, procedures zijn gedocumenteerd en geformaliseerd, waarbij verantwoordelijkheden eenduidig zijn toegewezen. Hierbij dienen de maatregelen ook aantoonbaar en controleerbaar te zijn ingericht, waardoor onveilige situaties kunnen worden gedetecteerd en structurele verbetering mogelijk is.

7.7 Toegangsbeveiliging – *BIG Hfst. 11*

Ontwikkeldoel

Er is een beheerst identiteits- en autorisatiemanagementproces dat waarborgt dat gebruikers toegang hebben tot de juiste applicaties en dat zij binnen applicaties over de juiste rechten beschikken. Op basis van risicoanalyse wordt geanalyseerd waar autorisaties conform het principe “need to know en need to use” (least privilege) van toepassing is en waar het principe “open, tenzij” is toe te passen. De standaard hierbij is least privilege en geldt in ieder geval voor (bijzondere) persoonsgegevens. Een gebruiker kan hiermee de taken uitvoeren die degene hoort uit te kunnen voeren, maar heeft hierbij niet de mogelijkheid om taken uit te voeren die degene niet uit hoort te voeren of meer informatie te kunnen raadplegen dan benodigd is. Dit proces is goed afgestemd op het instroom-doorstroom-uitstroom-proces en strak ingericht zodat het tijdig op veranderingen in de organisatie kan inspelen.

Voor alle externe verbindingen waarmee toegang verkregen wordt tot gemeentelijke bedrijfsvertrouwelijke informatie dienen voldoende maatregelen te zijn getroffen om ongeautoriseerde toegang te voorkomen. Dit geldt in ieder geval (maar niet uitsluitend) voor het tijd- en plaatsonafhankelijk werken (waaronder mobiele telefonie), extern aangeboden applicaties, en verbindingen van leveranciers met onze omgeving.

7.8 Verwerving, ontwikkeling en onderhoud van informatiesystemen – *BIG Hfst. 12*

Ontwikkeldoel

Er is een beheerst en gedocumenteerd wijzigingsbeheerproces dat waarborgt dat wijzigingen in software en hardware afdoende worden beoordeeld op hun risico´s en worden getest zodat alleen goedgekeurde wijzigingen kunnen worden doorgevoerd en zodat de kans op incidenten en verstoringen wordt beperkt. Naast software en hardware onder beheer van I&A, geldt het wijzigingsbeheerproces ook voor (externe) applicaties onder beheer of regie van de lijnorganisatie. Dit proces is strak ingericht zodat het tijdig op veranderingen in de organisatie kan inspelen.

De gemeente heeft een beheerst en gedocumenteerd proces ingericht voor het beheer van technische kwetsbaarheden. Dit omvat tenminste het tijdig verkrijgen van informatie over mogelijke kwetsbaarheden, risicoanalyse van kwetsbaarheden, het beheerst installeren van patches, en periodieke penetratietesten. Naast software en hardware onder beheer van I&A, geldt het beheer van technische kwetsbaarheden ook voor (externe) applicaties onder beheer of regie van de lijnorganisatie.

Gegevensuitwisseling dient op een passende wijze te zijn beveiligd tegen inbreuken op integriteit en vertrouwelijkheid. Dit geldt voor de uitwisseling:

- binnen de grenzen van de gemeentelijke organisatie;
- tussen de gemeente en andere organisaties of burgers; en,
- (cloud-)applicaties van en voor de gemeente die extern van de gemeentelijke IT-infrastructuur opereren.

Op deze wijze wordt geborgd dat de gemeente gezien wordt als een betrouwbare partner betreffende de vertrouwelijkheid van gegevens en kan de organisatie (en haar partners) vertrouwen op de integriteit van gegevens.

7.9 Beheer van informatiebeveiligingsincidenten – *BIG Hfst. 13*

Ontwikkeldoel

Informatiebeveiligingsincidenten zijn alle (series van) gebeurtenissen die een inbreuk maken op de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens en bijbehorende processen. De gemeente heeft een beheerst en gedocumenteerd incident management-proces ingericht dat een consistent en doeltreffend beheer van informatiebeveiligingsincidenten waarborgt. Dit omvat tenminste het registreren, classificeren en prioriteren, onderzoeken en analyseren, oplossen en reviewen van incidenten.

Incident management geldt voor software en hardware onder beheer van I&A. Echter facilitaire incidenten en incidenten met (externe) applicaties onder beheer of regie van de lijnorganisatie moeten ook op dit incidenten managementproces zijn aangesloten.

7.10 Bedrijfscontinuïteitsbeheer – *BIG Hfst. 14*

Ontwikkeldoel

De gemeente is zodanig ingericht dat de continuïteit van de belangrijkste processen voldoende gewaarborgd kan worden, dan wel dat bij uitval deze processen tijdig genoeg kunnen worden herstart. De gemeente borgt planmatig zowel de technische aspecten als de organisatorische aspecten van crisis- en business continuïteitsmanagement.

7.11 Naleving – BIG Hfst. 15

Ontwikkeldoel

De gemeente past de methodiek van het Informatie Security Management Systeem (ISMS) toe. Dit houdt in dat risico´s worden geanalyseerd, waarna maatregelen en informatiebeveiligingsactiviteiten worden ontworpen en aan actiehouders worden gekoppeld. Deze maatregelen en activiteiten worden uitgezet in een planning, waarbij het team Interne Controle en de CISO toezicht houden. Middels rapportages heeft de organisatie inzicht in de status en vindt bijsturing plaats waar nodig.

8 Bijlage I – Begrippenlijst

Applicatie	Een applicatie is software die bedoeld is voor computers of mobiele apparaten zoals smartphones, tablets en smartwatches.
Bedrijfsmiddel	Elk middel waarin of waarmee bedrijfsgegevens kunnen worden opgeslagen en/of verwerkt en waarmee toegang tot gebouwen, ruimten en ICT-voorzieningen kan worden verkregen: een bedrijfsproces, een gedefinieerde groep activiteiten, een gebouw, een apparaat, een ICT-voorziening of een gedefinieerde groep gegevens.
Beschikbaarheid / Continuïteit	Het zorg dragen voor het beschikbaar zijn van informatie en informatieverwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers.
Beveiliging	Het brede begrip van informatiebeveiliging, d.w.z. inclusief fysieke beveiliging, bedrijfscontinuïteitsbeheer, ofwel beschikbaarheid van bedrijfsprocessen en persoonlijke veiligheid en integriteit.
Beveiligingsincident	Het manifest worden van een beveiligingsrisico (dreiging, oorzaak) als gevolg van een overtreding van beveiligingsregel, bijv. onbevoegde toegang tot ICT-voorzieningen.
BIG	De Baseline Informatiebeveiliging Gemeenten (BIG) bestaat uit de Strategische BIG en de Tactische BIG. De Strategische BIG kan gezien worden als de 'kapstok' waaraan de elementen van informatiebeveiliging opgehangen kunnen worden. Centraal staat de organisatie en de verantwoording over informatiebeveiliging binnen de gemeenten. de Tactische BIG is het normenkader dat de beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke informatie(systemen) bevordert. Deze Tactische BIG is een richtlijn die een totaalpakket aan informatiebeveiligingscontrols en –maatregelen omvat die voor iedere gemeente noodzakelijk is om te implementeren.
Classificatie	Systematische identificatie en/of ordening van bedrijfsactiviteiten en/of records in categorieën overeenkomstig logisch gestructureerde afspraken, methodieken en procedurele voorschriften.
Cloud (applicatie)	Cloud is het via een netwerk – vaak het internet – op aanvraag beschikbaar stellen van software (waaronder applicaties) en gegevens.
ENSIA	Eenduidige Normatiek Single Information Audit is een systematiek om verschillende informatiebeveiligingsonderdelen in audits en zelfevaluaties samen te voegen.
Gegeven	Weergave van een feit, begrip of aanwijzing, geschikt voor overdracht, interpretatie of verwerking door een persoon of apparaat. Gegevens op zich behoeven niet noodzakelijkerwijs te zijn vastgelegd.
Governance	Stelsel van regels met betrekking op goed bestuur, toezicht en verantwoording. Betrokkenen dienen zich, los van vastgestelde regels, te houden aan toepasselijke waarden en normen.

Hardware	Dit is een verzamelnaam voor alle fysieke onderdelen die samenhangen met het computersysteem, zoals de computer zelf, de servers, het fysieke netwerk, de monitor, de printer en de modem.
ICT-voorzieningen	Applicaties en technische infrastructuur waarop deze applicaties zijn geïnstalleerd.
Informatie	Gegevens verzameld en uitgewerkt om te dienen als communicatie tussen personen. Informatie behoeft evenmin als gegevens noodzakelijkerwijs te zijn vastgelegd.
Informatiebeheer	1-Het systematisch verzamelen, verwerken, toegankelijk maken, gebruiken, onderhouden en verwijderen van informatie, opdat deze duurzaam toegankelijk en betrouwbaar is. De informatiebeheerder ondersteunt de gebruiker, die informatie creëert en raadpleegt. 2-De inrichting en uitvoering van het opslaan, het bewaren en beheren, het ontsluiten of (actief) leveren, en waar nodig, het overdragen, verplaatsen, verwijderen of vernietigen van informatie.
Informatiebeveiliging	Het proces van vaststellen van de vereiste betrouwbaarheid van informatieverwerking in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.
Integriteit	Het waarborgen van de juistheid en volledigheid en tijdigheid van informatie en de verwerking ervan. Als de tijdigheid van gegevens bepaald wordt door omstandigheden buiten het systeem, kan deze vanzelfsprekend niet als integriteitseis voor het systeem gesteld worden.
Integriteit / betrouwbaarheid	Het waarborgen van de juistheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking. 1-Informatie is betrouwbaar als zij authentiek en volledig is. 2- Een record is betrouwbaar als de inhoud kan worden vertrouwd als een volledige en nauwkeurige weergave van de transacties, activiteiten of feiten waarvan het getuigt en waarop men zich kan verlaten bij de uitvoering van latere transacties of activiteiten.
IT-infrastructuur	Dit is de fysieke verkeersinfrastructuur ten behoeve van het transport van digitale data, met als hoger doel informatie te delen of aan te bieden en te consumeren

Planning en Control	Planning en control omvat „strategic planning", „management control" en „task control". Het is het proces van besluitvorming over - het bereiken van - de strategische doelen van de organisatie, het toedelen van taken aan leden van een organisatie om deze strategie te implementeren en het waarborgen dat de taken effectief en efficiënt worden uitgevoerd. NB. Control is niet hetzelfde als controle!
Software	Programma's die een computer (of ander apparaat) een bepaalde taak laten vervullen zoals spelletjes, tekstverwerker, webbrowser, etc.
Technische infrastructuur	Het deel van de ICT-infrastructuur dat is gericht op de exploitatie van de systemen (hardware, systeemsoftware, bijbehorende documentatie, etc.). Samen met de applicatiesoftware en de bijbehorende documentatie en procedures vormt dit de ICT-infrastructuur
Toegankelijk	Informatie is toegankelijk als deze vindbaar, interpreteerbaar en uitwisselbaar is voor daartoe bevoegde personen of systemen.
Vertrouwelijkheid / Exclusiviteit:	Het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.
Volledig	Informatie met betrekking tot een proces is volledig als alle informatie is vastgelegd en wordt beheerd die aanwezig zou moeten zijn conform het beheerregime dat voor dat proces is vastgesteld.