GEMEENTE VIJFHEERENLANDEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Vijfheerenlanden

Nr. 157660

20 mei

2021

Besluit van het college van burgemeester en wethouders van de gemeente Vijfheerenlanden houdende regels omtrent het strategische informatieveiligheidsbeleid

I Voorwoord

I.I Totstandkoming

In dit document is het strategische informatieveiligheidsbeleid beschreven van de gemeente Vijfheerenlanden. De basis van dit informatieveiligheidsbeleid wordt gevormd door de Baseline Informatiebeveiliging Overheid (BIO). Deze bestaat uit drie delen, te weten een strategisch, tactisch en een operationeel deel. Dit beleid beslaat het strategische deel van de BIO, het tactisch en operationeel beleid wordt apart beschreven en vastgesteld in de directie. Dit maakt het gemakkelijker om aanpassingen door te voeren op tactisch gebied indien nodig. De BIO is afgeleid van de internationale informatieveiligheidsnormen NEN-ISO/IEC 27001:2017 en 27002:2017. De eerste standaard (ISO27001) is een norm voor de implementatie en planmatige borging van informatieveiligheid binnen de organisatie. De tweede standaard (ISO27002) bevat een verzameling van beveiligingsmaatregelen voor een praktische en concrete aanpak van informatieveiligheid binnen de organisatie. In de BIO zijn de methodiek en de terminologie specifiek aangepast voor de situatie bij overheden.

I.II Leeswijzer en ambitieniveau

Dit document bevat strategische beleidsuitgangspunten op het gebied van informatieveiligheid (geheel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van informatie) en de organisatie daarvan. Hierin staat het verantwoordingsmechanisme en de rollen en verantwoordelijkheden aangaande informatieveiligheid beschreven. Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking binnen specifieke onderdelen worden gesteld, zoals de Wet basisregistratie personen (Wet BRP), Algemene Verordening Gegevensbescherming (AVG), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit) en Wet openbaarheid bestuur (Wob). Om te voorkomen dat binnen elk van die gebieden separaat beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit gemeentebrede informatieveiligheidsbeleid op te stellen voor alle organisatieonderdelen.

Met dit document worden de uitgangspunten ten aanzien van de veiligheid van informatieprocessen bepaald. Dit beleid brengt niet de huidige situatie in beeld maar beschrijft het ambitieniveau aangaande gemeentebrede informatieveiligheid.

I.III Algemene oriëntatie en positionering

Informatieveiligheid maakt deel uit van de bedrijfsvoering en de primaire processen van de organisatie en haar omgeving. In de uitwerking vormt het een samenhangend geheel van maatregelen van procedurele, organisatorische, fysieke, technische, personele en juridische aard.

Het doel van informatieveiligheid is het behoud van:

- Beschikbaarheid / continuïteit (voorkomen van uitval van systemen);
- Integriteit / betrouwbaarheid (gegevens zijn juist, actueel en volledig);
- Vertrouwelijkheid / exclusiviteit (onbevoegden kunnen geen kennis nemen van gegevens die niet voor hen bestemd zijn);
- Controleerbaarheid.

I.IV Wettelijke basis en controle beveiligingsnormen

De wettelijke basis van informatieveiligheid valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, zoals (niet uitputtend):

- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet;
- Wet computercriminaliteit;
- Algemene verordening gegevensbescherming (AVG);
- Archiefwet / Archiefregeling;
- Databankenwet;
- Wet elektronisch bestuurlijk verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen Burgerservicenummer;

- Paspoortwet;
- Wet basisregistratie personen (Wet BRP);
- Wet openbaarheid bestuur (Wob);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);
- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Basisregistratie grootschalige topografie (BGT);
- Wet Basisregistratie Ondergrond (BRO);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Wet Politiegegevens;
- Wet ruimtelijke ordening (Wro).

Op grond van bovenstaande wet- en regelgeving worden er eisen gesteld aan het niveau van informatieveiligheid, de beheersmaatregelen en de controle (interne controle (ic)/interne audit) daarop.

I.V Forum Standaardisatie
De overheid is verplicht de te voldoen aan de normen NEN-ISO/IEC 27001:2013 en NEN-ISO/IEC 27002:2013[1] waarop de Baseline Informatiebeveiliging Overheid is gebaseerd. Deze normen zijn opgenomen in de lijst met verplichte standaarden voor de publieke sector van het Forum Standaardisatie. De gemeente Vijfheerenlanden volgt de standaarden uit de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Bij de aanbesteding van nieuwe producten of diensten of het verlengen van bestaande producten of diensten worden de relevante open standaarden uit de lijst van het Forum Standaardisatie uitgevraagd.

1. Informatieveiligheidsbeleid

Doelstelling
Het bieden van ondersteuning aan het bestuur, management en organisatie bij de sturing op en het beheer van informatieveiligheid.

Resultaat
Beleid waarin de taken, bevoegdheden en verantwoordelijkheden voor informatieveiligheid alsmede het vereiste beveiligingsniveau zijn vastgelegd.

1.1 Strategisch beleidsdocument voor informatieveiligheid
Het college van B en W behoort dit gemeentebreed strategische beleidsdocument voor informatieveiligheid goed te keuren en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen[2]. Dit doet het college aan de hand van de 10 bestuurlijke principes voor informatieveiligheid zoals opgenomen in bijlage 2 van dit document.

Dit beleidsdocument bevat de onderstaande punten:
- De doelstellingen en strategische uitgangspunten van informatieveiligheid voor de gemeente;
- De beveiligingseisen;
- De organisatie van informatieveiligheid (zie hoofdstuk 2);
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende informatieveiligheidsrollen (zie hoofdstuk 2);
- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging (zie II.II) en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (zie II.VI);
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst (zie hoofdstuk 1.5).

1.2 Scope van het informatieveiligheidsbeleid
De scope van dit beleid omvat alle gemeentelijke informatieprocessen, hieronder vallen zowel de ambtelijke als bestuurlijke informatieprocessen. Organisatorisch zijn de uitgangspunten uit dit beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) het college, dit geldt ook voor

1) Het Forum Standaardisatie spreekt van de norm uit 2013 waar in de BIO 2017 wordt genoemd. Het Forum Standaardisatie licht dit als volgt toe: "Na plaatsing op de 'pas toe of leg uit'-lijst zijn zowel ISO 27001 als ISO 27002 Europese normen geworden. Inhoudelijk zijn de normen niet gewijzigd. Hierdoor is het meest actuele specificatiedocument NEN-EN-ISO/IEC27002:2017. Inhoudelijk is het gelijk aan de specificatie NEN-ISO/IEC27002:2013 die getoetst is voor opname op de 'pas toe of leg uit'-lijst." (Bron: https://www.forumstandaardisatie.nl/standaard/nen-isoiec-27001)
2) [5.1.1.1 BIO]

de Gemeenteraad en de Griffie, tenzij zij zelf een informatieveiligheidsbeleid opstelt. Alle strategische beleidsuitgangspunten met betrekking tot informatieveiligheid en de organisatie van informatieveiligheid zijn in dit gemeentebreed document samengebracht.

Externe partijen moeten een zelfde beveiligingsniveau hanteren zoals opgenomen in dit beleid, zij moeten tevens aan kunnen tonen dat zij voldoen aan dit niveau van beveiliging. Specifieke informatie op het gebied van informatiebeveiliging van relevante expertisegroepen, leveranciers van hardware, software en diensten en de IBD wordt gebruikt om de informatiebeveiliging te verbeteren[3]. De gemeente heeft uitgewerkt met welke instanties contact wordt onderhouden en door wie[4]. Dit overzicht wordt minimaal jaarlijks bijgewerkt[5].

Op basis van dit strategische beleidsdocument, dat door het college van burgemeester en wethouders (B en W) wordt vastgesteld, wordt door de directie een "Tactisch gemeentebreed informatieveiligheidsbeleid" vastgesteld. Hierin wordt beschreven op welke manier de gemeente informatieveiligheid gaat borgen, rekening houdend met de risico's. De kernelementen in het "Tactische gemeentebreed informatieveiligheidsbeleid" zijn de uitwerkingen van de volgende onderwerpen:

- Autorisatiebeleid;
- ICT ontwerp(en);
- Beleid leveranciers/externe partijen;
- Bedrijfsprocessen;
- Beheerrichtlijnen ICT;
- Configuratiebeheer;
- Continuïteitsbeheer;
- Interne controle;
- Fysieke beveiliging (beveiliging die met behulp van fysieke middelen gerealiseerd wordt);
- Gedragsregels;
- HR proces;
- Incidentenbeheer;
- Loggingbeleid;
- Wijzigingsproces.

Vervolgens zal de gemeente aanvullende procedures en andere operationele documentatie opstellen. Deze zullen de praktische uitwerking vormen van het Tactische beleid.

1.3 Borging van het informatieveiligheidsbeleid
Om de borging van het informatieveiligheidsbeleid en de daarvan afgeleide plannen te realiseren, wordt naast een toebedeling van rollen (zie hoofdstuk 2), onderstaande Plan, Do, Check, Act (PDCA) cyclus doorlopen. Alhoewel altijd tussentijds documenten kunnen worden bijgesteld, worden onderstaande uitgangspunten gehanteerd voor het doorlopen van de PDCA-cyclus resulterend in een Information Security Management System (ISMS)[6] (zie figuur 1):

1. Informatieveiligheidsbeleid (zowel strategisch als tactisch)
Bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Dit is een organisatiebreed beleid dat de uitgangspunten, de normen en de kaders biedt voor de veiligheid van alle onderliggende gemeentelijke informatieprocessen. Uitzonderingen hierop zijn toegestaan, maar dan wel duidelijk gemotiveerd én verifieerbaar, dit wordt ook wel het 'pas toe of leg uit' principe genoemd. Bijstelling van het informatieveiligheidsbeleid vindt plaats rond een cyclus van 3 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats[7];

2. Informatieveiligheidsanalyse
Stap twee is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een informatieveiligheidsanalyse. Hiertoe wordt allereerst een overzicht opgesteld van de gegevensverzamelingen/applicaties in de gemeentelijke organisatie. Deze worden toegewezen aan een eigenaar en geclassificeerd op de risicoklassen beschikbaarheid, integriteit en betrouwbaarheid van de informatie (ook wel dataclassificatie genoemd). Tevens wordt het Basis Beveiligingsniveau (BBN) per informatiesysteem vastgesteld. Hierbij geldt dat gemeentebreed het BBN2 wordt gehanteerd, hiervan kan bij in-

3) [12.6.1 BIO]
4) [6.1.3.1BIO]
5) [6.1.3.2 BIO]
6) [18.2.1.1 BIO]
7) [5.1.2.1 BIO]

dividuele informatiesystemen slechts voldoende beargumenteerd (vastgelegd) worden afgeweken. Hierna wordt de praktijksituatie in de gemeente getoetst aan het gemeentebrede informatieveiligheidsbeleid en aan de beveiligingsmaatregelen uit de BIO, middels het uitvoeren van een risico inventarisatie en evaluatie (RI&E), GAP-analyse, rondgang van het gebouw en een (eventuele) evaluatie van het vorige actieplan. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar;

3. Actieplan Informatieveiligheid
Op basis van de informatieveiligheidsanalyse wordt in stap drie een actieplan opgesteld. De in de analyse geconstateerde risico's worden gewogen en waar nodig van maatregelen voorzien. Prioritering van de acties wordt gedaan op basis van de risico's die vanuit de RI&E zijn geconstateerd, de beschikbare tijd en de beschikbare middelen. Hierdoor ontstaat een compact actieplan waarmee de gemeente vaststelt welke verbeteracties gedurende een periode van 1 of 2 jaar worden uitgevoerd. Dit actieplan vormt een praktische leidraad voor de verbetering en borging van informatieveiligheid in de organisatie. De informatieveiligheidsorganisatie komt bij elkaar om de implementatie van het actieplan informatieveiligheid te evalueren te bewaken en waar nodig bij te stellen. Dit vindt conform de bespreking in het informatieveiligheidsoverleg (zie paragraaf 2.2) minimaal tweemaal per jaar plaats.

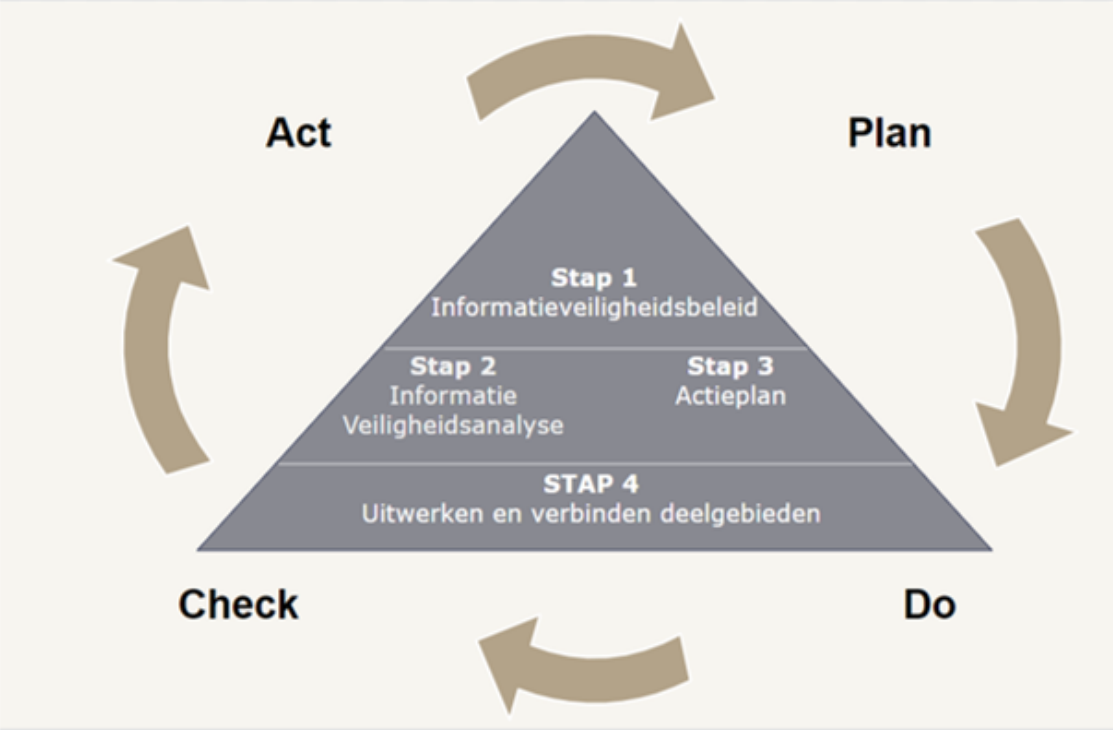
4. Technische en organisatorische maatregelen
Stap vier bestaat uit het opleveren van een complete set aan technische en organisatorische maatregelen die gericht is op de specifieke eisen van een onderdeel. Het kan gaan om maatregelen uit de BIO, maar ook om applicaties zoals de BRP, SUWI, de BAG, het financiële systeem, of om de primaire processen van de organisatie, ICT-beheerprocessen of de inrichting van de ICT-platformen. Dit betreft met name het opstellen van procedures en werkinstructies.

1.4 Audits en naleving

De directie beoordeelt regelmatig de naleving van de informatieverwerking en -procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging[8]. Dit mondt uit in het jaarverslag. Daarin wordt in lijn met de P&C-cyclus en ondersteund door een In Control Verklaring (ICV) gerapporteerd over het doorlopen van de beschreven cyclus met betrekking tot informatieveiligheid. In deze rapportage worden ook andere voor informatieveiligheid en privacy relevante onderwerpen – zoals auditresultaten en de uitkomsten van interne controles – behandeld[9].

Om te beoordelen of de gemeente haar informatieveiligheidsbeleid- en doelstellingen heeft behaald, worden periodieke onafhankelijke audits - waarbij een onafhankelijke deskundige partij een toets uitvoert op de opzet, bestaan en werking van beheersmaatregelen - en controles uitgevoerd. Hiertoe kan een externe (erkende) partij worden ingeschakeld of de eigen afdeling concern control/auditafdeling. Jaarlijks wordt een auditplan (intern controleplan) opgesteld waarin wordt vastgelegd welke interne controles en audits in het komende jaar plaatsvinden en op welke informatiesystemen deze betrekking hebben[10]. In dit plan wordt tevens een beschrijving van de uit te voeren controles opgenomen, evenals de uitvoerders en verantwoordelijken (lijnniveau) voor de controles gekoppeld aan een tijdsplanning. Ook de jaarlijkse controle op de technische naleving van beveiligingsnormen bij informatiesystemen, zoals penetratietesten, zijn onderdeel van dit plan[11]. Over de resultaten van de uitgevoerde audits wordt door de lijnverantwoordelijken gerapporteerd aan de CISO. De CISO bundelt deze bijdragen en rapporteert hierover periodiek aan het bestuur.

8) [18.2.2 BIO]
9) [18.1.4.2, 18.2.2.1 BIO]
10) [18.2.1.2 BIO]
11) [18.2.3.1 BIO]



Figuur 1: De informatieveiligheidspiramide met PDCA cirkel

2. Organisatie van de informatieveiligheid

Doelstelling
Het benoemen van het eigenaarschap van de bedrijfsprocessen met bijbehorende informatieprocessen en/of (informatie)systemen en het verankeren van de hieraan verbonden verantwoordelijkheden.[8.1.2]

Resultaat
Verankering in de gemeentelijke organisatie van verantwoordelijkheden, taakomschrijvingen en coördinatie- en rapportagemechanismen met betrekking tot informatieveiligheid.

2.1 Verantwoordelijkheidsniveaus binnen de gemeente Vijfheerenlanden

Binnen de gemeente Vijfheerenlanden worden – waar relevant in lijn met geldende wet- en regelgeving – de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatieveiligheid onderscheiden[12]:

2.1.1 controle en toetsing door de Raad

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, zo ook voor informatieveiligheid. Het college legt in lijn met de P&C-cyclus jaarlijks verantwoording af aan de raad, door middel van een collegeverklaring opgenomen in het jaarverslag met een passage over informatieveiligheid in de paragraaf bedrijfsvoering[13].

2.1.2 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau

Het college van B en W van de gemeente Vijfheerenlanden draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatieveiligheid. Verder stellen ze met het voorliggende beleidsdocument de kaders ten aanzien van informatieveiligheid op basis van landelijke en Europese wet- en regelgeving vast. Het college informeert de Raad over de informatieveiligheid van de gemeente, door een aparte paragraaf op te nemen in de jaarrekening van de gemeente. Hierin wordt de Raad op de hoogte gebracht over de stand van zaken, de uitgevoerde plannen van het afgelopen jaar en de planning en plannen van het volgende

12) [6.1.1.2 BIO]
13) [18.2.2.1 BIO]

jaar. Daarnaast worden de Chief Information Security Officer (CISO) en de controller informatieveiligheid op basis van een vastgesteld functieprofiel aangesteld door het college van B en W[14].

2.1.3 Gemandateerde verantwoordelijkheden en taken op organisatieniveau
De gemeentesecretaris voert onder mandaat van het college activiteiten uit voor informatieveiligheid. Dit wordt in een mandaatbesluit vastgelegd. Deze stelt in overleg met de directie en de CISO het gewenste niveau van informatieveiligheid vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar (deze is verantwoordelijk voor het stellen van eisen aan een systeem en de inrichting van de controle hierop, zodat voldaan wordt aan het informatieveiligheidsbeleid en aan de wettelijke eisen) aan[15].

De *gemeentesecretaris* heeft in ieder geval de volgende verantwoordelijkheden:
- Het vaststellen van operationele kaders en het geven van sturing ten aanzien van informatieveiligheid;
- Het sturen op risico's omtrent informatieveiligheid;
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatieveiligheidscomponenten en -systemen;
- Het in laten richten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatieveiligheid om fraude en/of fouten te voorkomen.

2.1.4 Verantwoordelijkheden en taken op afdelingsniveau
De netwerkmanagers zijn eigenaar van en integraal verantwoordelijk voor de (informatie)veiligheid van de informatieprocessen en -systemen binnen hun afdeling.

De *netwerkmanagers* hebben in ieder geval de volgende verantwoordelijkheden:
- Het classificeren van opgeslagen data in applicaties en gegevensverzamelingen;
- Medewerkers attenderen op hun verantwoordelijkheid ten aanzien van informatieveiligheid in hun dagelijkse werkprocessen;
- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling van toepassing zijn;
- Het opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen;
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, bedrijfscontinuïteit en op naleving van regels en richtlijnen;
- het oplossen van beveiligingsincidenten (Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de Informatievoorziening verstoort, en daarmee de informatieveiligheid kan aantasten)[16];
- het expliciet vaststellen van relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen voor elk informatiesysteem (een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen) en de organisatie[17];
- het waarborgen van privacy en bescherming van persoonsgegevens conform relevante wet- en regelgeving[18];
- Opdrachtgeven tot en toezien op het uitvoeren van periodieke beveiligingsaudits;
- Het rapporteren, via de coördinator informatieveiligheid, over compliance (voldoen) aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C rapportages.

2.1.5 Chief Information Security Officer (CISO)
Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's, evenals het opstellen van rapportages.

De *CISO* heeft in ieder geval de volgende verantwoordelijkheden:

14) [18.2.2.1 BIO]
15) [8.1.2 BIO]
16) [16.1.2.5 BIO]
17) [18.1.1 BIO]
18) [18.1.4 BIO]

- Rapporteert rechtstreeks aan de gemeentesecretaris en het bestuur;
- Coördineert het formuleren van informatieveiligheidsbeleid;
- Coördineert de uitvoering van de informatieveiligheidsanalyse en zorgt voor de actualisatie hiervan;
- Coördineert de prioritering van informatieveiligheidsmaatregelen uit de informatieveiligheidsanalyse en de uitvoering van het actieplan informatieveiligheid;
- Stelt een plan op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de gemeentesecretaris en de directie met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is het aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- Geeft gevraagd én ongevraagd advies over informatieveiligheid aan de gehele organisatie;
- Bevordert het beveiligingsbewustzijn in de organisatie;
- Houdt de registratie van informatiebeveiligingsincidenten bij in een incidentenregister en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Ondersteunt het college bij het maken van de rapportage over de informatieveiligheid van de gemeente in het jaarverslag.
- Onderhoudt contact met de Informatiebeveiligingsdienst;
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages vergezeld van een in control statement. Hierbij bundelt de coördinator informatieveiligheid de deelbijdragen van het afdelingsmanagement.

2.1.6 De controller informatieveiligheid
Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van het informatieveiligheidsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten.

De *controller informatieveiligheid* is in ieder geval verantwoordelijk voor:
- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid, dit gebeurt in samenwerking met de beveiligingsbeheerders.
- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en actieplan informatieveiligheid;
- De controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse;
- De bewaking van het niveau van informatieveiligheid;
- De toetsing van evaluatieproces van beveiligingsincidenten.
- De rapportage van bevindingen aan gemeentesecretaris en het college van B en W

2.1.7 De beveiligingsbeheerder
Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid binnen een specifiek deelgebied. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van specifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan en gedefinieerd als beveiligingsbeheerder. Hierbij volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: DigiD, WOZ, Sociaal domein BRP, Waardedocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations en Autorisatiebevoegde Rijbewijzen), SUWI (officieel Security Officer SUWI) en de BAG, BRO en BGT. Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering (zoals Facilitaire Zaken, ICT, DIV (Archivering) en Personeelszaken) en de primaire processen (bijvoorbeeld Sociaal Domein, Financiën, Veiligheid & Handhaving, publieksdiensten (eventueel gecombineerd met BRP en Waardedocumenten), Ruimte/omgeving).

Specifiek verplichte beveiligingsbeheerdersrollen:
- *Autorisatiebevoegde Reisdocumenten/Aanvraagstations*: Verantwoordelijk voor het beheer van de autorisaties (het toekennen van rechten in informatiesystemen aan personen of groepen) voor de reisdocumentenmodules (RAAS en aanvraagstations).
- *Autorisatiebevoegde Rijbewijzen*: Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.
- *Security Officer SUWI*: verantwoordelijk voor het beheer van beveiligingsprocedures en maatregelen in het kader van Suwinet. De Security Officer verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de beveiligingsstatus van Suwinet aan het college en vraagt daar-

naast meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente.

De *beveiligingsbeheerder* is voor het toegewezen deelgebied verantwoordelijk voor het geheel van activiteiten gericht op de toepassing en naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de maatregelen die op de audit en zelfevaluatie onderdelen gelden.

2.1.8 Verantwoordelijkheden afdeling overstijgende (informatie)systemen
Afdelingsoverstijgende (informatie)systemen binnen de gemeente worden onder de verantwoordelijkheid van het A-team gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdelingsoverstijgend (informatie)systeem heeft de directie het primaat dit te mandateren aan een of meerdere organisatieonderdelen die daarmee verantwoordelijk worden voor de gehele gegevensverzameling of het (informatie)systeem. De procesverantwoordelijke van een afdelingsoverstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften worden nageleefd en dat de verantwoordelijkheden voor beveiliging voor alle betrokken partijen duidelijk omschreven zijn.

De gemandateerd eigenaar maakt minimaal de volgende schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie die van het afdeling overstijgend (informatie)systeem gebruik maakt:
- Voorwaarden voor het toegestane gebruik van het afdelingsoverstijgend (informatie)systeem;
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het afdeling overstijgend (informatie)systeem;
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens;
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatieveiligheid;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van afspraken en oplossen van eventuele geschillen;
- Het recht op inzage in de resultaten van de externe audits en zelfevaluaties bij de gebruikende partij waaruit blijkt in welke mate deze aan het gemeentelijk informatieveiligheidsbeleid voldoet.

2.1.8 Functionaris gegevensbescherming
De FG is conform de Algemene Verordening Gegevensbescherming (AVG) de interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente[19]. De FG heeft de volgende wettelijke taken (AVG Art 39), vertaald naar de situatie bij de gemeente:

Het takenpakket van de FG bestaat uit de volgende punten (art. 39 lid 1 AVG):
- Informeren en adviseren van het college, het management, de raad en de medewerkers over hun verplichtingen met betrekking tot gegevensbescherming;
- Toezien op naleving van zowel de AVG en andere wetten met betrekking tot gegevensbescherming als het beleid met betrekking tot de bescherming van persoonsgegevens van de verwerkingsverantwoordelijke of de verwerker. Hierbij hoort tevens toewijzing van verantwoordelijkheden, bewustmaking en opleiding van de bij de verwerking betrokken personeel en de betreffende audits;
- Desgevraagd adviseren omtrent gegevensbeschermingseffectbeoordeling, ook wel Data Protection Impact Assessment (DPIA) genoemd, en toezien op de uitvoering daarvan;
- Toezicht houden op de registraties en afhandeling van beveiligingsincidenten waarbij persoonsgegevens betrokken zijn en toezicht houden op het melden van een datalek bij de Autoriteit Persoonsgegevens en bij de betrokkenen.
- Samenwerken met en als contactpunt optreden voor de Autoriteit Persoonsgegevens (AP);
- Rekening houden met risico's naar de aard, omvang en context van verwerkingen van persoonsgegevens;
- Contactpersoon binnen de organisatie omtrent privacy.
- Rapporteren aan de hoogste leidinggevende van de verwerkingsverantwoordelijke, zijnde in veel gevallen het college of de burgemeester en in sommige gevallen de gemeenteraad.

De FG heeft voor privacy een toezichthoudende taak, vergelijkbaar met de taak van controller informatieveiligheid voor informatieveiligheid. De uitvoering en implementatie van het beleid is belegd bij een of meerdere privacybeheerders, al dan niet specifiek voor een bepaalde afdeling, zoals bijvoorbeeld het sociaal domein.

2.1.9 De privacybeheerder

19) [18.1.4.1 BIO]

Deze rol is gericht op de uitvoering en de naleving van de Algemene Verordening Gegevensbescherming (AVG). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

De *privacybeheerder* heeft in ieder geval de volgende verantwoordelijkheden:
- Beoordelen van de verwerking van persoonsgegevens tegen de achtergrond van de kaders van privacywetgeving en adviseert het management en netwerkmanagers bij wijzigingen in proces-uitvoering, bedrijfsvoering en de toepassing van een privacy impact assessment.
- Als adviserend lid deelnemen aan programma's en projecten waarvan het resultaat gevolgen kan hebben voor de wijze van verwerking van persoonsgegevens.
- Uitleggen van de privacy voorschriften in de AVG, en daarnaast in de sectorale wetgeving;
- Coördineren van de privacy werkzaamheden, informeren en het verzorgen van meldingen bij de FG;
- Coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente;
- Coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
- Rapporteren aan de directie;
- Inrichten van procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
- Beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
- Adviseren en ondersteunen bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen.

Op twee specifieke deelgebieden heeft de privacybeheerder een voorgeschreven benaming en kan deze als onafhankelijk controleur optreden. Dit betreft het gebied van reisdocumenten en rijbewijzen. Het betreft de volgende benamingen:
- *Beveiligingsfunctionaris reisdocumenten*: verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
- *Beveiligingsfunctionaris rijbewijzen*: verantwoordelijk voor het toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

2.1.10 De medewerkers

Alle medewerkers dragen verantwoordelijkheid voor de veiligheid van de activiteiten die behoren tot hun eigen functie en taken. Zij betrachten zorgvuldigheid en discipline bij het omgaan met informatie en (informatie)systemen. Zij zijn zich bewust van de eisen ten aanzien van de betrouwbaarheid, de integriteit, de beschikbaarheid en de controleerbaarheid van de informatieprocessen waarbij zij zijn betrokken. In het tactisch informatieveiligheidsbeleid zijn gedragsregels in het kader van informatieveiligheid uitgewerkt. Iedere medewerker wordt geacht deze gedragsregels te kennen en uit te dragen bij het uitoefenen van zijn of haar functie.

Figuur 3: Functies en rollen in informatieveiligheidsorganisatie

2.2 Overleg en afstemmingsorganen
De CISO is voorzitter van het overleg informatieveiligheid dat minimaal tweemaal per jaar bij elkaar komt. Bij dit overleg kunnen aanwezig zijn:
- De CISO;
- De controller Informatieveiligheid;
- Beveiligingsbeheerders t.a.v.: BRP/Waardedocumenten, BAG, BGT, BRO, SUWI, DigiD en WOZ;
- Beveiligingsbeheerders t.a.v.: FZ, ICT, DIV, P&O en Sociaal Domein;
- Privacybeheerder en functionaris gegevensbescherming;
- Agendaleden: MT lid of specialist.

Mogelijk onderwerpen:
- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het actieplan Informatieveiligheid;
- Evaluatie van beveiligingsincidenten;
- Planning en voorbereiding van audits, controles en zelfevaluaties;
- Evaluatie en actualisatie informatieveiligheidsbeleid en de informatieveiligheidsanalyse.

Daarnaast vindt afstemming plaats tussen de CISO en de functioneel-, applicatie- en gegevensbeheerder(s) en de procesverantwoordelijke van (informatie)systemen.

2.3 Informatiebeveiligings-crisisbeheersing
Voor interne crisisbeheersing dient een kernteam informatieveiligheid geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten (gebeurtenis die een zodanige verstoring van informatiesystemen of processen tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen). Naar gelang de situatie wordt aangesloten bij de crisisorganisatie. Directie stelt vast in welke gevallen en door wie er contacten met autoriteiten (brandweer, toezichthouders, IBD[20] enz.) wordt onderhouden[21]. De criteria voor de handels- en werkwijze tijdens grote incidenten of calamiteiten worden nader in een procedure uitgewerkt. Dit team bestaat in ieder geval uit:
- Gemeentesecretaris (voorzitter);
- Betrokken portefeuillehouder
- CISO;
- De beveiligingsbeheerder ICT;
- De verantwoordelijke beveiligingsbeheerder (afhankelijk van het incident of de calamiteit);
- Relevante experts (indien nodig);
- Een lid van de afdeling communicatie;
- Een notulist.

20)[12.6.1 BIO]
21)[6.1.3 BIO]

BIJLAGE 1 Rollen en namen informatieveiligheidsorganisatie van de gemeente Vijfheerenlanden

Rol	Naam	Vervanger (eventueel)
Chief Information Security Officer (CISO)		
Controller Informatieveiligheid		
Beveiligingsbeheerder BRP Beveiligingsbeheerder WD		
Beveiligingsbeheerder BAG Beveiligingsbeheerder BGT Beveiligingsbeheerder BRO Beveiligingsbeheerder DigID Beveiligingsbeheerder WOZ		
Security Officer SUWI		
Beveiligingsbeheerder Facilitair		
Beveiligingsbeheerder Sociaal Domein		
Beveiligingsbeheerder Automatisering		
Beveiligingsbeheerder DIV		
Beveiligingsbeheerder P&O		
Privacy beheerder Functionaris gegevensbescherming		

Bijlage 2: De 10 bestuurlijke principes van informatieveiligheid

1 Bestuurders bevorderen een veilige cultuur

Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.

Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

2 Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt.

3 Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4 Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten en risicomanagement is van groot belang.

U kunt als bestuurder alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. De gemeente dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6 Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.

Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.

7 Informatiebeveiliging kost geld

Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.

Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieveen/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.

8 Onzekerheid dient te worden ingecalculeerd

De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.

Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.

9 Verbetering komt voort uit leren en ervaring
Risicobeheer wordt voortdurend verbeterd door leren en ervaring.
Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.

10 Het bestuur controleert en evalueert
Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.
Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie Vereniging van Nederlandse Gemeenten 7 omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.