Strategisch Informatieveiligheidsbeleid

Versie	: definitief concept
Auteurs	: Hielco Koeze, Peter Bruin, Michel van der Linden, Wim van Schoonhoven, Ineke Weber, Ellen Manshanden
Begeleiding	: Martijn van Engelen MSc (BMC)
Datum	: 25 november 2015

I Voorwoord

I.I Totstandkoming

In dit document is het strategische informatieveiligheidsbeleid beschreven van De Friese Waddeneilanden.

Het informatieveiligheidsbeleid (waaronder voorliggende strategische deel en het tactische deel vallen) is gebaseerd op de internationale standaarden voor informatieveiligheid: NEN/ISO 27001 en NEN/ISO 27002. Op basis van deze standaard is de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) opgeleverd. Deze Baseline Informatiebeveiliging geeft een specifieke invulling aan de wijze waarop de veiligheid van informatie binnen gemeentelijke organisaties moet zijn geborgd.

De basis van dit informatieveiligheidsbeleid wordt gevormd door Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING).

I.II Leeswijzer en ambitieniveau

Dit document bevat een groot aantal strategische beleidsuitgangspunten op het gebied van de veiligheid van gemeentelijke informatieprocessen. In dit voorliggende document worden de rollen en verantwoordelijkheden aangaande Informatieveiligheid en het verantwoordingsmechanisme beschreven. De tactische uitwerking hiervan is terug te vinden in het 'Tactische Informatieveiligheidsbeleid'. Met instemming van voorliggende document wordt direct ingestemd met de verdere uitwerking, zoals beschreven in het Tactische Informatieveiligheidsbeleid.

Tevens is het goed te vermelden dat zowel het Strategische als het Tactische Informatieveiligheidsbeleid niet de huidige situatie in beeld brengen, maar dat in deze documenten de ambitie, de stip op de horizon beschreven zijn. Door middel van een gestructureerde aanpak, waarin weloverwogen keuzes worden gemaakt ten opzichte van ambitie en capaciteit (zie hoofdstuk 1) zal op een verantwoorde manier invulling gegeven gaan worden aan het bepaalde in beide beleidsdocumenten. Het voorliggende document betreft dus het ambitieniveau van De Friese Waddeneilanden aangaande organisatiebrede Informatieveiligheid.

II. Waarom informatieveiligheid?

II.1 Inleiding

De Friese Waddeneilanden is een informatie-intensieve organisatie met een primaire focus op de dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers van de verschillende gemeenten moeten kunnen beschikken over betrouwbare informatie om de klanten optimaal te kunnen bedienen. Voor een optimale moderne dienstverlening is een koppeling van informatiesystemen noodzakelijk. Bovendien moeten burgers en bedrijven er op kunnen vertrouwen dat hun gegevens in goede handen zijn bij de gemeente.

Informatisering speelt een steeds prominentere rol in de gemeentelijke organisatie. Deze rol wordt in het kader van het stelsel van basisregistraties en de toenemende complexiteit van het digitale dienstverleningskanaal steeds belangrijker. Ook De Friese Waddeneilanden richten zich op het koppelen van systemen waardoor grote gegevensverzamelingen ontstaan die vervolgens weer specifieke informatie opleveren voor interne en externe afnemers.

Daarnaast is de gemeente steeds afhankelijker van goed werkende informatievoorziening en -systemen. Dit betekent dat De Friese Waddeneilanden alert zijn op mogelijke verstoringen van of bedreigingen gericht op informatiesystemen, mede omdat veel informatiesystemen niet zijn ontworpen met het oog op veiligheid. De veiligheid die met de technische middelen kan worden bereikt is begrensd en wordt al vanouds ondersteund met passende beheerprocessen en procedures. Daarnaast speelt echter de menselijke factor (het menselijk gedrag) een steeds grotere rol in het daadwerkelijk realiseren van de veiligheid van informatie in de praktijk. Deze factor speelt, door de steeds complexer wordende informatieprocessen, veelal zelfs een doorslaggevende rol.

Informatie komt in verschillende vormen voor. Het kan zijn geschreven, gesproken, gedrukt of digitaal zijn verwerkt en of opgeslagen. Al deze verschijningsvormen van informatie vragen voor een deel eenzelfde generieke aanpak, maar kennen ook verschillen. Dit document (met onderliggend tactisch beleid) besteedt hier aandacht aan.

De veiligheid van informatie speelt binnen een groot aantal gebieden van de gemeente een rol. Om te voorkomen dat binnen elk van die gebieden (bijvoorbeeld rondom de SUWI, DigiD, BRP, WD of BAG) separaat beleid ontwikkeld en geïmplementeerd moet worden, is de keuze gemaakt dit organisatiebredebrede informatieveiligheidsbeleid op te stellen. In dit organisatiebrede informatieveiligheidsbeleid worden beleidsuitgangspunten vastgelegd ten aanzien van alle onderliggende informatiedomeinen. Hieronder vallen niet alleen de informatie-intensieve domeinen als sociaal domein, samenlevingszaken, publieksdiensten of financiën, maar eveneens domeinen als beheer en onderhoud, ruimtelijke ordening en facilitaire zaken.

In het organisatiebrede informatieveiligheidsbeleid wordt op strategisch en tactisch niveau beschreven welke uitgangspunten gelden ten aanzien van de informatieveiligheid van De Friese Waddeneilanden. Deze documenten zullen samen met de technische beveiligingsmaatregelen en de procedures een adequaat niveau van beveiliging voor de organisatie moeten opleveren waardoor de kwaliteitskenmerken van informatie, te weten: de beschikbaarheid, de integriteit, de vertrouwelijkheid en de controleerbaarheid van de informatie binnen alle domeinen van de organisatie zijn gewaarborgd.

II.2 De informatieveiligheidspiramide

Ook de centrale overheid heeft veel aandacht voor de veiligheid van informatie binnen de verschillende overheidslagen. Naast het ontwikkelen van nieuwe wet- en regelgeving op dit gebied uit zich deze aandacht ook in bewustwordingscampagnes en ondersteuning van gemeentelijke overheden bij hun inspanningen om de veiligheid van overheidsinformatie te verhogen. De ontwikkeling door KING/VNG van de Baseline Informatiebeveiliging Nederlandse Gemeenten vormt hiervan een voorbeeld. Deze veiligheidsrichtlijnen voor gemeentelijke informatieprocessen, die gebaseerd zijn op de internationale standaarden voor informatieveiligheid NEN/ISO 27001 en 27002, bieden een meetlat voor gemeenten om hun Informatieveiligheid op orde te brengen en te houden.

Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000 standaarden, de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/KING) en aanvullende richtlijnen en eisen van het Nationaal Cyber Security Centrum (NCSC). Daarnaast is rekening gehouden met de wettelijke kaders die aan informatieverwerking worden gesteld, zoals de Wet BasisRegistratie Personen (Wet BRP), Wet Bescherming Persoonsgegevens (WBP), Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), het DigiD beveiligingsassessment (DigiD audit), Wet Openbaarheid Bestuur (Wob).
Naast deze veelal op persoonsgegevens gebaseerde kaders komen er in hoog tempo (aanvullingen op) wettelijke kaders met betrekking tot overige authentieke registraties, zoals de Wet Basisregistratie Adressen en Gebouwen (BAG), Wet Kenbaarheid Publiekrechtelijke Beperkingen (Wkpb), de nieuwe Wet Ruimtelijke Ordening (Wro) en de Archiefwet. Deze stroomlijning van de informatievoorziening vereist in steeds ruimere mate aansluiting op zogenaamde landelijke voorzieningen. De toenemende complexiteit en intensiteit van de informatieprocessen bieden een helder motief voor overheden om hun aandacht nog meer te richten op de veiligheid voor overheidsinformatie.

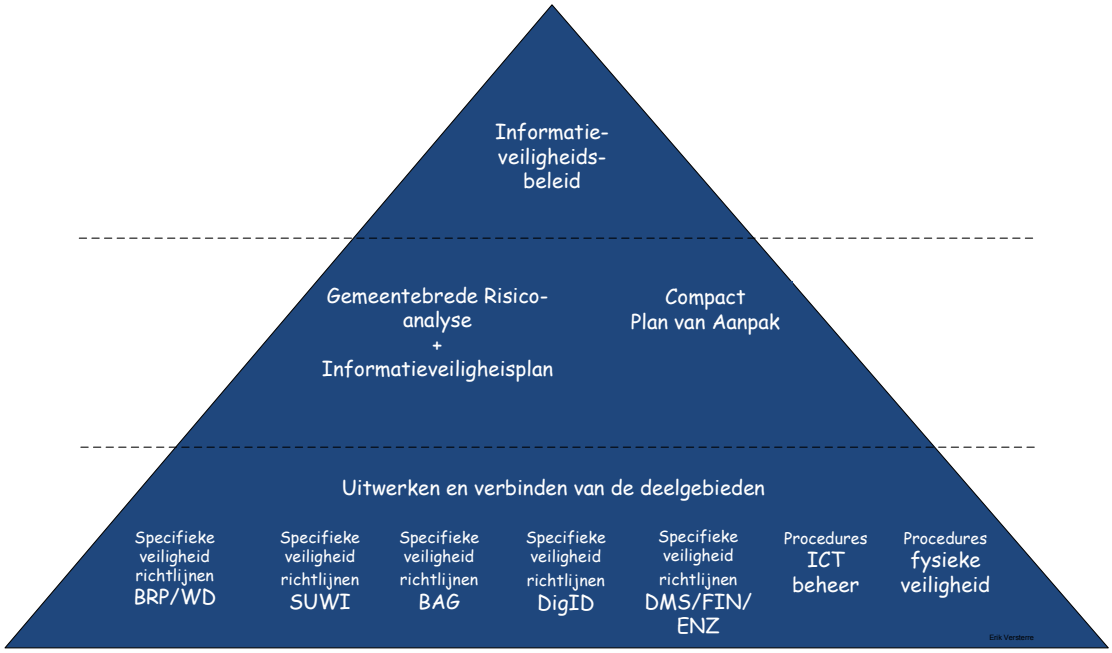
Teneinde de scope van dit document te verduidelijken, is in figuur 1 aangegeven welke niveaus van informatieveiligheid zijn te onderkennen.

Bovenaan de piramide treffen we het informatieveiligheidsbeleid aan. Dit is een organisatiebreed beleid dat, opgesplitst in een strategisch en tactisch gedeelte, 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. Het informatieveiligheidsbeleid is zodanig opgezet dat praktijksituaties eenvoudig kunnen worden opgezet of hieraan worden getoetst.

De tweede laag van de piramide is gericht op het implementatietraject. De implementatiefase begint met het uitvoeren van een risico-inventarisatie en evaluatie (RI&E). Tijdens deze RI&E worden de uitgangspunten in het informatieveiligheidsbeleid getoetst met de praktijksituatie. Hier worden niet alleen de ‘harde aspecten’ onderzocht, dat wil zeggen de techniek, de regels en de procedures, maar worden ook de ‘zachte aspecten’ meegenomen. Deze richten zich op het menselijk handelen en cultuuraspecten en daarnaast de sociale en fysieke inrichting van de organisatie. Na de risico-inventarisatie vindt risicoweging en prioritering plaats. Tijdens deze stap worden de geconstateerde risico’s gewogen en eventueel van maatregelen voorzien, zodat een compact overzicht ontstaat van risico’s en te treffen maatregelen.

Op het laagste niveau wordt een complete set aan maatregelen opgeleverd die gericht is op de specifieke eisen van een onderdeel. Een onderdeel kan een applicatie zijn zoals het BRP, het BAG of

het financiële systeem, maar kan ook gericht zijn op de ICT-beheerprocessen, de inrichting van de ICT-platformen of de juistheid van de crediteurenadministratie.



Figuur 1: De informatieveiligheidspiramide

II.3 Toelichting op ISO 27001 en ISO 27002

Het informatieveiligheidsbeleid is volledig gebaseerd op de internationale standaard voor informatieveiligheid NEN-ISO/IEC 27001 en 27002. De eerste standaard (27001) biedt een richtlijn voor de implementatie en planmatige borging van Informatieveiligheid binnen de organisatie. Dit komt overeen met het voorliggen strategische deel van het Informatieveiligheidsbeleid. De tweede standaard (27002) bevat een zeer uitgebreide verzameling van zogenaamde 'best practices' voor een praktische en concrete aanpak van informatieveiligheid binnen de organisatie. Het tactische gedeelte van het Informatieveiligheidsbeleid is vooral gebaseerd op deze standaard. De Baseline Informatiebeveiliging Nederlandse Gemeenten (2013) is afgeleid van deze beide internationale informatieveiligheidsnormen, waarbij in de Baseline Informatiebeveiliging Nederlandse Gemeenten de methodiek en de terminologie specifiek is aangepast voor de situatie in gemeenten.

II.4 Algemene oriëntatie en positionering

Informatieveiligheid maakt onlosmakelijk 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.

Raakvlakken:
- Algemeen beveiligingsbeleid (bijv. deuren, kluizen, toegangscontrole, alarmering);
- Personeelsbeleid (bijv. screening, opleiding en functietypering);
- Organisatiebeleid (bijv. functiescheiding);
- Informatiseringsbeleid (bijv. standaardisatie, Internet en Cloud functionaliteit);
- Privacybeleid (bijv. correct gebruik van persoonsgegevens);
- Juridisch beleid (bijv. afbreukrisico's bij privacyschendingen, clausulering in overeenkomsten met derden, Third Party Mededelingen);
- Dienstverleningsconcept (bijv. website, het Nieuwe Werken, DigiD).

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.

II.5 Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid

De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente[1], zo ook voor informatieveiligheid. De verantwoordelijkheid voor informatieveiligheid ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de algemeen directeur/gemeentesecretaris.

De vaststelling en implementatie van de informatieveiligheidsstructuur[2] en de organisatiebrede beleidsnormen vormen de verantwoordelijkheid van de colleges van burgemeester en wethouders van de gemeenten van De Friese Waddeneilanden. Voor het nemen van operationele maatregelen is de algemeen directeur/gemeentesecretaris gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij teamoverstijgende (informatie)systemen.

De teamleiders zijn verantwoordelijk voor de informatiesystemen waarvan zij eigenaar zijn. Zij dienen deze systemen te classificeren en in te richten zodat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

II.6 Wettelijke basis en controle beveiligingsnormen

De wettelijke basis van informatieveiligheid valt af te leiden uit Europese richtlijnen en landelijke wet- en regelgeving, waaronder (niet uitputtend):
- Grondwet;
- Auteurswet;
- Telecommunicatiewet;
- Ambtenarenwet;
- Wet computercriminaliteit;
- Wet Bescherming Persoonsgegevens (WBP);
- Archiefwet;
- Databankenwet;
- Wet Elektronisch Bestuurlijk Verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen burgerservicenummer;
- Paspoortwet;
- Wet BasisRegistratie Personen (BRP);
- Wet Openbaarheid Bestuur (Wob);
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI);

[1] In hoofdstuk 2 worden de verantwoordelijkheden en bevoegdheden ten aanzien van informatieveiligheid uitgebreider beschreven.

[2] Onder het begrip informatieveiligheidsstructuur wordt in dit verband de complete beheercyclus van het informatieveiligheidsproces verstaan (beleidsvorming, implementatie, verantwoording, controle en bijstelling). Informatieveiligheid wordt gedefinieerd als een verzamelbegrip voor de kwaliteitsaspecten beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid.

- Wet Basisregistratie Adressen en Gebouwen (BAG);
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB);
- Nieuwe Wet Ruimtelijke Ordeningen (nWRO).

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

1. Informatieveiligheidsbeleid

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

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

1.1 Beleidsdocument voor informatieveiligheid

Het College van B&W behoort een organisatiebreed beleidsdocument voor informatieveiligheid goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers, alsmede hiernaar te handelen. Met goedkeuring van voorliggende Strategische Informatieveiligheidsbeleid wordt direct ingestemd met de verdere uitwerking hiervan als beschreven het Tactische Informatieveiligheidsbeleid.

1.2 Scope van het informatieveiligheidsbeleid

De scope van dit beleid omvat alle gemeentelijke informatieprocessen, hieronder vallen zowel de ambtelijke als bestuurlijke informatieprocessen. Het beleid heeft niet alleen betrekking op de verwerking, uitwisseling en opslag van digitale informatie, maar ook informatie in fysieke c.q analoge vorm, ongeacht de locatie, het tijdstip en de gebruikte apparatuur. Daarnaast bevat dit beleid de uitgangspunten voor handelen ten aanzien van informatieprocessen met keten- en uitvoeringspartners.

1.3 Informatieveiligheidsplan

Op basis van dit strategische en het onderliggende tactische beleidsdocument wordt door het managementteam het informatieveiligheidsplan met plan van aanpak vastgesteld. Hierin wordt aangegeven op welke wijze het beleid uitgevoerd zal worden.
De kernelementen in het informatieveiligheidsplan zijn:

- Beschrijving van het huidige niveau van informatieveiligheid en de mate waarin aan de beveiligingseisen en -prioriteiten uit het beleid en aan alle onderdelen van het informatieveiligheidsplan wordt voldaan. Recente ontwikkelingen worden ook beschreven, zoals het in productie nemen van een nieuw informatiesysteem of technische infrastructuur die gevolgen kunnen hebben voor het beveiligingsniveau;
- Voor het bepalen van afhankelijkheden en risico's is een analyse verricht ten aanzien van de bedrijfsprocessen ten opzichte van de ICT-omgeving. Naar aanleiding van deze analyse zijn minimaal de volgende aandachtspunten voor het plan onderkend:
    - Risico's die onvoldoende af te dekken zijn door maatregelen;
    - Risico's die zijn gerelateerd aan de kritische bedrijfsprocessen en/of (informatie)systemen;
    - Een overzicht van verbeterpunten, aangevuld met een kostenaanduiding voor uitvoering en de wijze en termijn waarop zij uitgevoerd zullen worden;

- Een overzicht van de aanwezige (informatie)systemen waarbij is aangegeven welke systemen bedrijfskritisch zijn. Dit overzicht kan als bijlage aan het uitvoeringsplan worden toegevoegd.

1.4 Aanvullende maatregelen

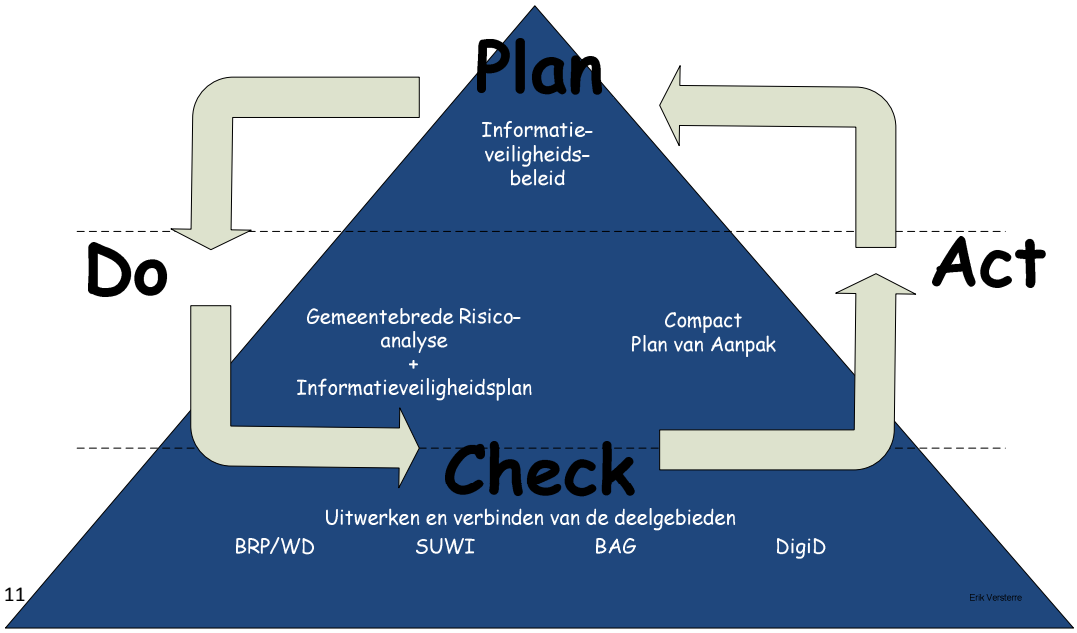
Afwijkend beveiligingsniveau
Als uit de risicoanalyse blijkt dat voor bepaalde gegevensverwerkingen een hoger beveiligingsniveau is vereist, moet een daarvoor verantwoordelijk persoon aanvullende maatregelen treffen. Bij minder risicovolle verwerkingen kan een lager beveiligingsniveau worden overwogen (zie hoofdstuk 1 in het Tactische Informatieveiligheidsbeleid).

Persoonsgegevens
Bij de verwerking van persoonsgegevens zijn aanvullende maatregelen vereist, afhankelijk van de klassenindeling van de Wet Bescherming Persoonsgegevens (WBP).

1.5 Borging van het informatieveiligheidsbeleid

Om 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 (zie figuur 2):

1. **Informatieveiligheidsbeleid:** bevat het zowel het Strategische als het Tactische informatieveiligheidsbeleid en de visie op informatieveiligheid. Bijstelling van beide delen van het informatieveiligheidsbeleid vindt plaats om de 4 tot 6 jaar en dient goedgekeurd te worden door de colleges van B&W van De Friese Waddeneilanden;
2. **Informatieveiligheidsplan:** bevat de risicoanalyse (de toets aan de praktijk) op basis van informatieveiligheidsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van het informatieveiligheidsplan vindt plaats na 1 tot 2 jaar en zal door de verschillende managementteams beoordeeld en goedgekeurd worden;
3. **Plan van Aanpak:** bevat de concrete acties volgend uit de risicoanalyse. Bijstelling (hieronder valt ook de voortgang op de realisatie van de afgesproken acties en maatregelen) van het plan van aanpak vindt (conform de bespreking in het informatieveiligheidsoverleg, zie hoofdstuk 2) twee maal per jaar plaats.



Figuur 2: 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.

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

2.1 Verantwoordelijkheidsniveaus binnen De Friese Waddeneilanden

Binnen De Friese Waddeneilanden worden de volgende verantwoordelijkheid- en takenniveaus met betrekking tot informatieveiligheid onderscheiden:

2.1.1 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau

De Colleges van B&W van de verschillende gemeenten van De Friese Waddeneilanden dragen als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatieveiligheid. Het college stelt de kaders ten aanzien van informatieveiligheid op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging gemandateerd aan de algemeen directeur/gemeentesecretaris.

2.1.2 Gemandateerde verantwoordelijkheden en taken op organisatieniveau

De gemandateerde verantwoordelijkheid voor informatieveiligheid ligt bij de algemeen directeur/gemeentesecretaris. Deze stelt met het managementteam het gewenste niveau van informatieveiligheid vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De algemeen directeur/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 aan. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd bij leidinggevenden op organisatieniveau.

2.1.3 Verantwoordelijkheden en taken op teamniveau

De teamleiders zijn verantwoordelijk voor de (informatie) veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun team.

2.1.4 De coördinator informatieveiligheid / Chief Information Security Officer (CISO)

Deze rol is op Waddeneilandenniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages.

2.1.5 De controller informatieveiligheid

Deze rol is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid, de realisatie van voorgenomen beveiligingsmaatregelen en de escalatie van beveiligingsincidenten.
De rol van controller informatiebeveiliging heeft op twee specifieke deelgebieden een voorgeschreven officiële benaming. Dit betreft het gebied van reisdocumenten en van 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.

2.1.6 Gemeente Leeuwarden (ICT)

De gemeente Leeuwarden, waarvan systeembeheer deel uit maakt, beheert de werkplekken, serverplatformen, lokale netwerken, WiFi verbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij mede verantwoordelijk voor alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de procesverantwoordelijken voor (informatie)systemen afgelegd.

2.1.7 Het team Facilitaire Zaken

Het team Facilitaire Zaken is verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting (archiefkasten, kluizen enzovoort).

2.1.8 Het team P&O

Het team P&O is verantwoordelijk voor de advisering inzake de personele en de organieke aspecten binnen de organisatie en speelt hiermee een belangrijke advies rol op het gebied van organisatie en informatieprocessen.

2.1.9 De beveiligingsbeheerder

Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. 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: BRP, Reisdocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations) , Rijbewijzen (Autorisatiebevoegde Rijbewijzen), BAG, SUWI (officieel Security officer SUWI) en DigiD.

Autorisatiebevoegde Reisdocumenten/Aanvraagstations

Verantwoordelijk voor het beheer van de autorisaties 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
De Security Officer beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd. De Security Officer bevordert en adviseert over de beveiliging van Suwinet, verzorgt minimaal twee maal per jaar rapportages over de status, controleert dat, met betrekking tot de beveiliging van Suwinet, de maatregelen worden nageleefd, evalueert de uitkomsten en adviseert en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet. De Security Officer heeft formeel wat betreft rapportages een bijzondere rol. Deze rapporteert namelijk rechtstreeks aan de bestuurlijk verantwoordelijke.
De security officer SUWI vraagt daarnaast meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van SUWInet door de gemeente en rapporteert zijn bevindingen richting het college.

2.1.10 Privacybeheerder
Deze rol is gericht op de uitvoering en de naleving van de Wet Bescherming van Persoonsgegevens (WBP). Daarnaast adviseert de medewerker over privacybescherming en over activiteiten ter bescherming van persoonsgegevens.

2.1.11 Functionaris voor de gegevensbescherming
Momenteel mogen organisaties zelf bepalen of ze een Functionaris voor de Gegevensbescherming benoemen: benoeming van een FG is nu niet verplicht. Dit wordt anders zodra de Europese Privacy Verordening in werking treedt. Deze rol wordt functionaris voor de gegevensbescherming (FG) of Data Protection Officer (DPO) genoemd. De functionaris gegevensbescherming is de interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. Deze toezichthouder wordt officieel functionaris voor de gegevensbescherming (FG) genoemd. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Wet bescherming persoonsgegevens (Wbp). De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. Bij organisaties met een FG stelt het College bescherming persoonsgegevens (CBP) zich terughoudend op als toezichthouder.

2.1.12 Functioneel applicatiebeheerder
Verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatie-systemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening.

2.1.13 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 en de beschikbaarheid van de informatieprocessen waarbij zij zijn betrokken.

2.1.14 Gegevensbeheerder
Verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

2.2 Toewijzing verantwoordelijkheden voor informatieveiligheid

De *algemeen directeur/gemeentesecretaris* en *het MT* hebben in ieder geval de volgende verantwoordelijkheden:

- Het stellen van kaders en het geven van sturing ten aanzien van de veiligheid van informatie;
- Het sturen op concern risico's;
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen beveiligingsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze beveiligingsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en systemen;
- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatieveiligheid;
- Het aanwijzen van een coördinator informatieveiligheid / CISO en een controller informatieveiligheid.

De teamleiders/coördinatoren hebben in ieder geval de volgende verantwoordelijkheden*:*

- Het uit (laten) voeren van maatregelen uit het informatieveiligheidsplan die op het team van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de teaminformatiesystemen;
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het rapporteren, via de coördinator informatieveiligheid / CISO*,* over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C managementrapportages.

De *coördinator informatieveiligheid / CISO* heeft in ieder geval de volgende verantwoordelijkheden:

- Coördineert het formuleren van informatieveiligheidsbeleid;
- Stelt het informatieveiligheidsplan op en zorgt voor de actualisatie van dat plan;
- Coördineert de uitvoering van informatieveiligheidsmaatregelen uit het informatieveiligheidsplan;
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de directie en de teamleiders/coördinatoren met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen;
- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en het informatieveiligheidsplan;
- 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;
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages. Hierbij bundelt de coördinator informatieveiligheid / CISO de deelbijdragen van o.a. de beveiligingsbeheerders.

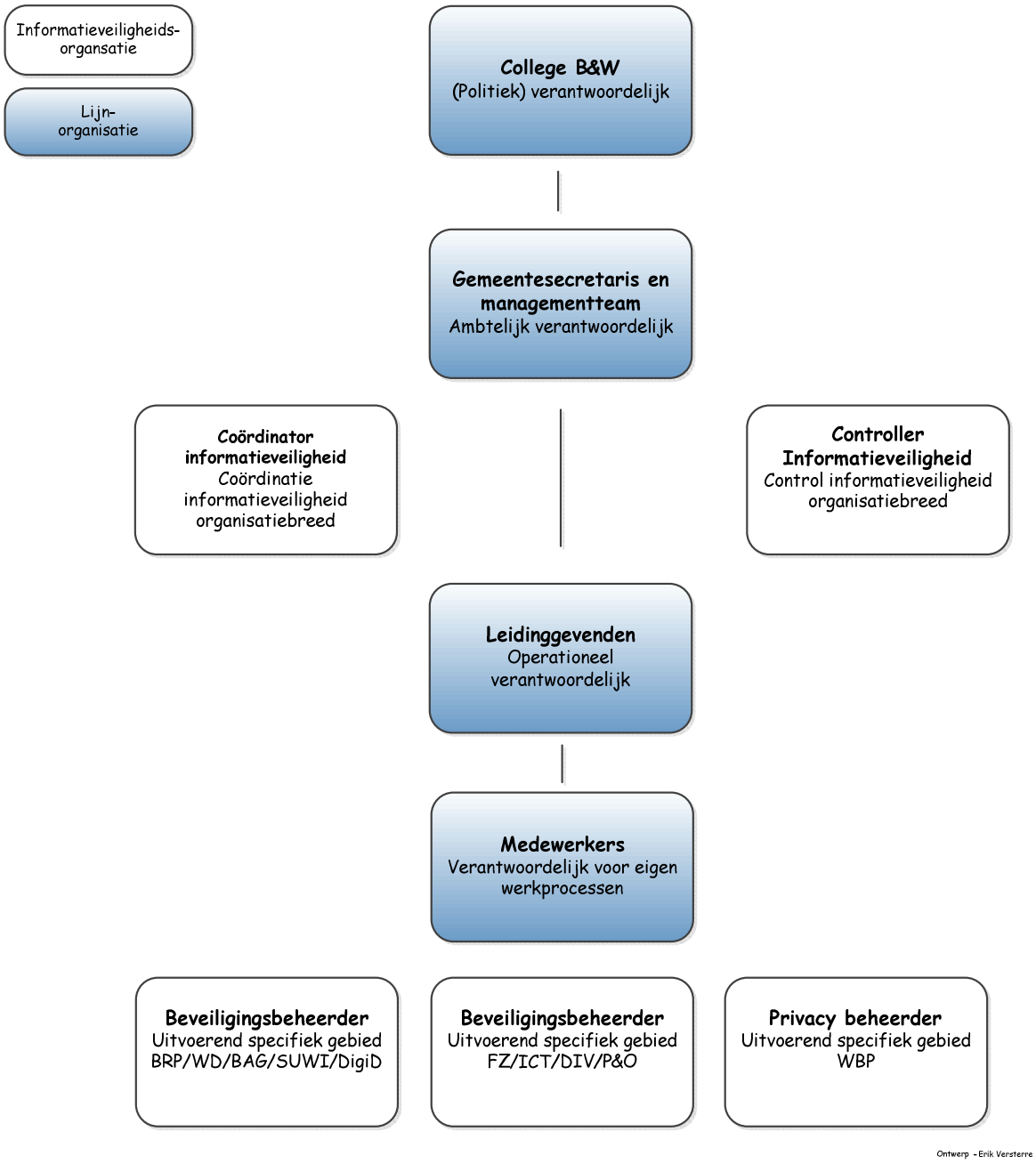
De *controller informatieveiligheid* heeft in ieder geval de volgende verantwoordelijkheden:

- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid;
- De controle op de voortgang van het uitvoeren van de maatregelen uit het informatieveiligheidsplan;
- De controle op de periodieke actualisatie van informatieveiligheidsbeleid en op het Informatieveiligheidsplan;
- Toetsen/bewaken van het niveau van informatieveiligheid;
- Toetsing van evaluatieproces van beveiligingsincidenten.

De *beveiligingsbeheerder* is -voor het toegewezen deelgebied- verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid en het onderliggende informatieveiligheidsplan. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons. De medewerker coördineert de toepassing van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan de coördinator informatieveiligheid / CISO en de controller informatieveiligheid.

De *privacybeheerder* heeft in ieder geval de volgende verantwoordelijkheden:
- Toezicht op de naleving van de Wet Bescherming van Persoonsgegevens (WBP) en de Wet Basisregistratie Personen (Wet BRP);
- Organisatiebreed adviseren over privacybescherming en over activiteiten ter bescherming van persoonsgegevens;
- Aanwijzingen geven aan gebruikers van systemen met betrekking tot persoonsregistraties;
- Ongevraagd advies uit te brengen over alle procedures en producten die betrekking hebben op de registratie van personen;
- Contactpersoon van de gemeente voor het College Bescherming Persoonsgegevens (CBP).

In bijlage 1 staan de namen vermeld van de toegewezen rollen in de beveiligingsorganisatie per gemeente.



Figuur 3: Functies en rollen in informatieveiligheidsorganisatie

2.3 Overleg en afstemmingsorganen

De coördinator informatieveiligheid is voorzitter van het overleg informatieveiligheid dat 2 tot 4 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De coördinator informatieveiligheid
- De controller Informatieveiligheid;
- Beveiligingsbeheerders t.a.v: BRP/Waardedocumenten, BAG, SUWI en DigiD;
- Beveiligingsbeheerders t.a.v: FZ, ICT, DIV en P&O
- Privacy beheerder;
- Agendaleden: MT lid of specialist.

Onderwerpen:

- Voortgang uitvoering maatregelen informatieveiligheidsplan c.q. Plan van Aanpak;
- Beveiligingsincidenten;
- Planning en voorbereiding van Audits en controles;
- Evaluatie en actualisatie informatieveiligheid en het informatieveiligheidsplan.

2.4 ICT crisisbeheersing

Voor interne crisisbeheersing dient een kernteam informatieveiligheid geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit team bestaat uit de coördinator informatieveiligheid / CISO, de manager IT (Leeuwarden), de beveiligingsbeheerder ICT (Leeuwarden), een lid van het MT, relevante experts en een lid van team communicatie.

2.5 Rapporteren beveiligingsincidenten

De coördinator informatieveiligheid / CISO wordt door de procesverantwoordelijken geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatieveiligheidsbeleid niet wordt nageleefd.

Er wordt minimaal eenmaal per jaar gerapporteerd aan de directie door de coördinator Informatieveiligheid / CISO.

2.6 Verantwoordelijkheden teamoverstijgende (informatie)systemen

Teamoverstijgende (informatie)systemen binnen de gemeentelijke organisaties worden onder de verantwoordelijkheid van de gemeente Leeuwarden gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder teamoverstijgend (informatie)systeem heeft de directie het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem.
De gemandateerd eigenaar van een teamoverstijgend (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 schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het teamoverstijgend (informatie)systeem gebruik maakt (de gebruikende partij).

2.7 Contracten met derden

2.7.1 Service level agreement (niveau van dienstverlening)

Bij structurele / langdurige ondersteuning en of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van websites wordt tussen een organisatie of een team daarvan en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van informatieveiligheid en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatieveiligheid. In het uitbestedingscontract wordt verwezen naar de SLA.

2.7.2 Inhuur derden

Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van het verantwoordelijk teamleider. Deze manager dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.

2.7.3 Toegang

Bij toegang van derden tot de gemeentelijke ICT voorzieningen gelden in principe de onderstaande uitgangspunten:

- Informatieveiligheid is (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een bewerkersovereenkomst (conform WBP artikel 14) afgesloten.
- Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd.
- Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld.
- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd

2.7.4 Grote projecten

Voor grote ICT-projecten gelden specifieke, op centraal niveau vastgestelde, richtlijnen, met name ten aanzien van Europese aanbesteding, screening van bedrijven en juridische aspecten.

BIJLAGE 1 Rollen en namen informatieveiligheidsorganisatie

Generieke rollen

Rol	Naam
Coördinator Informatieveiligheid	Peter Bruin
Controller Informatieveiligheid	Hielco Koeze
Beveiligingsbeheerder DigiD	Joop Beijaard
Beveiligingsbeheerder ICT	Peter Bruin (SSL gemeente Leeuwarden)

Specifieke rollen

Ameland

Rol	Naam
Beveiligingsbeheerder BRP en WD	Pedro Kooiker
Beveiligingsbeheerder BAG	Ronald Leijstra
Beveiligingsbeheerder SUWI	Jeroen Wijnberg
Beveiligingsbeheerder FZ	
Beveiligingsbeheerder DIV	Koos Molenaar
Beveiligingsbeheerder P&O	Jan Jaap Werkman
Privacy beheerder	

Schiermonnikoog

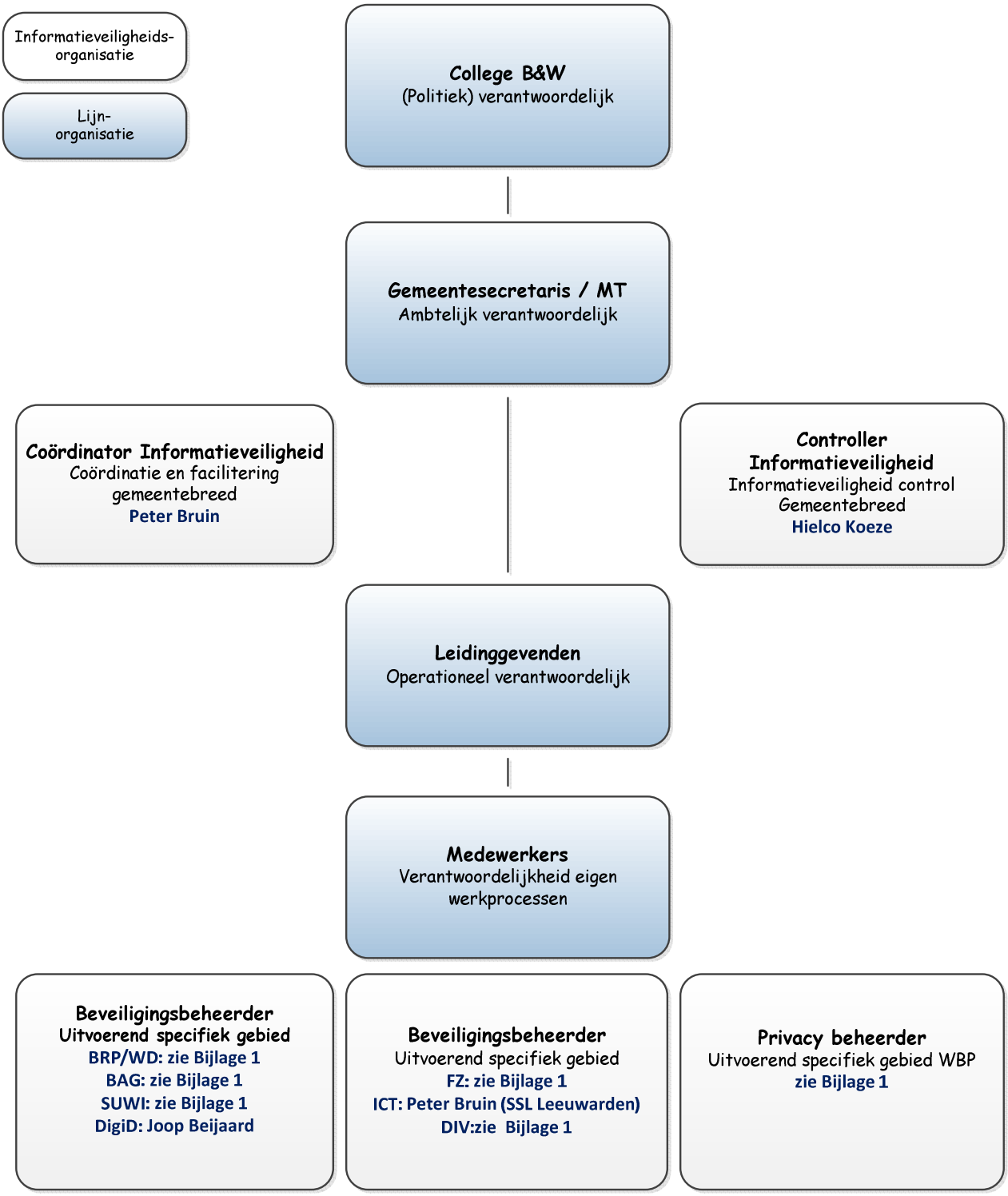
Rol	Naam
Beveiligingsbeheerder BRP en WD	Marty Cotie
Beveiligingsbeheerder BAG	Piet Huisman
Beveiligingsbeheerder SUWI	Gemeente Dantumadiel
Beveiligingsbeheerder FZ	Piet Huisman
Beveiligingsbeheerder DIV	Annie Kootstra
Beveiligingsbeheerder P&O	Grytske Klazema
Privacy beheerder	

Terschelling

Rol	Naam
Beveiligingsbeheerder BRP en WD	Tanja Fischer
Beveiligingsbeheerder BAG	Jauk Hek
Beveiligingsbeheerder SUWI	Dienst SoZaWe
Beveiligingsbeheerder FZ	Remko Pals
Beveiligingsbeheerder DIV	Arend Roos
Beveiligingsbeheerder P&O	Mandy Rieks
Privacy beheerder	Edward Petersen

Vlieland

Rol	Naam
Beveiligingsbeheerder BRP en WD	Jan Smit
Beveiligingsbeheerder BAG	Marja Veerdig
Beveiligingsbeheerder SUWI	Dienst SoZaWe
Beveiligingsbeheerder FZ	André de Bie
Beveiligingsbeheerder DIV	Carin Winkelman
Beveiligingsbeheerder P&O	Uitbesteed aan gemeente Leeuwarden
Privacy beheerder	Lobke Buren


Informatieveiligheids-organisatie
Lijn-organisatie
College B&W
(Politiek) verantwoordelijk
Gemeentesecretaris / MT
Ambtelijk verantwoordelijk
Coördinator Informatieveiligheid
Coördinatie en facilitering gemeentebreed
Peter Bruin
Controller Informatieveiligheid
Informatieveiligheid control Gemeentebreed
Hielco Koeze
Leidinggevenden
Operationeel verantwoordelijk
Medewerkers
Verantwoordelijkheid eigen werkprocessen
Beveiligingsbeheerder
Uitvoerend specifiek gebied
BRP/WD: zie Bijlage 1
BAG: zie Bijlage 1
SUWI: zie Bijlage 1
DigiD: Joop Beijaard
Beveiligingsbeheerder
Uitvoerend specifiek gebied
FZ: zie Bijlage 1
ICT: Peter Bruin (SSL Leeuwarden)
DIV:zie Bijlage 1
Privacy beheerder
Uitvoerend specifiek gebied WBP
zie Bijlage 1

BIJLAGE 2 Conversietabel functies en teams

In zowel het Strategische als het Tactische gedeelte van het Informatieveiligheidsbeleid worden functies en teams genoemd. Daar deze documenten gelden voor de vier gemeenten van De Waddeneilanden zit er verschil in de benamingen van deze afdelingen. In onderstaande tabel staat per benaming wat er per gemeente gelezen dient te worden.

Algemeen	**Ameland**	**Schiermonnikoog**	**Terschelling**	**Vlieland**
Managementteam	Directieteam	Managementteam	Directie	Teamleidersoverleg
Teamleider(s)	Coördinatoren	Teamleider(s)	Teamleider(s)	Teamleider(s)
Facilitaire Zaken	Gebouwbeheerder	Gebouwbeheerder	Gebouwbeheerder	Team Uitvoering & Ondersteuning
P&O	Team P&O	P&O-functionaris	Staf HRM	Team Beleid
Communicatie	Staf	Communicatie	Staf Communicatie	Team Beleid