Informatiebeveiligingsbeleid Gemeente Schagen

Versie 1.0

17 januari 2018

Auteur

Inlichtingen bij

I Voorwoord

I.I Totstandkoming

In dit document is het informatiebeveiligingsbeleid beschreven van de gemeente Schagen.

Het informatiebeveiligingsbeleid 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. Tijdens het buitengewone VNG ledencongres op 29 november 2013, is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Hierin is opgenomen dat de Nederlandse gemeenten de Baseline Informatiebeveiliging Gemeenten (BIG) als uitgangspunt nemen om de informatiebeveiliging binnen de gemeentelijke organisaties te waarborgen.

Het beleid is zodanig opgezet dat het een visie geeft in hoe de gestelde inzichten en doelstellingen bereikt gaan worden en geeft een samenhangende reeks stappen aan voor de continuïteit van informatieveiligheid.

De basis van dit informatiebeveiligingsbeleid wordt gevormd door Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG - VNG/IBD).

I.II Leeswijzer en ambitieniveau

Dit document bevat strategische beleidsuitgangspunten op het gebied van informatieveiligheid en de organisatie van informatieveiligheid waarbij de rollen en verantwoordelijkheden aangaande informatieveiligheid en het verantwoordingsmechanisme staan beschreven. Dit document dient als kapstok voor de verdere inbedding van het informatiebeveiligingsbeleid, de standaarden, de procedures en de processen.

In een separaat document "Uitvoeringsplan informatiebeveiliging", wordt volgens de Baseline Informatiebeveiliging Gemeenten (BIG) het inhoudelijke normenkader beschreven. Hierin worden alle normen en maatregelen vanuit de BIG verder uitgewerkt, die leidend zullen zijn voor alle organisatieonderdelen van de gemeente Schagen. Met instemming van voorliggende document wordt direct ingestemd met de verdere uitwerking, die beschreven zal worden in het "Uitvoeringsplan informatiebeveiliging".

Met dit document wordt daarnaast bepaald dat de gemeente bij voorkomende keuzes en vraagstukken ten aanzien van de veiligheid van informatieprocessen de beleidsregels in dit document als uitgangspunt hanteert.

II. Waarom informatieveiligheid?

II.I Inleiding

Visie:
Informatieveiligheid bestaat deels uit harde technische acties, maar voor het merendeel uit zachte maatregelen gericht op gedrag en cultuur. De gemeente Schagen gaat uit van vertrouwen in haar medewerkers die zelfstandig en innovatief werken. Alle informatie in de organisatie is open voor iedereen, tenzij het persoonsgebonden informatie bevat. Daarmee wordt deze persoonsgebonden informatie op een veilige manier uitgewisseld. De balans tussen beveiliging en vrijheid is hiermee goed afgedekt. Hierin worden de keuzes vanuit het belang van onze inwoners gemaakt. Dit betekent dat:
De gemeente persoonsgebonden informatie beveiligt en beschermt en zorgt dat medewerkers deze informatie op een veilige manier kan uitwisselen.
De gemeente actief communiceert over informatieveiligheid om de medewerkers bewust te maken van hun verantwoordelijkheden.
De gemeente niet altijd kan voldoen aan de privacywetgeving als dit niet strookt met het inwonersbelang.

De gemeente Schagen 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 gemeente moeten kunnen beschikken over betrouwbare informatie om de klanten optimaal te kunnen helpen en adviseren. 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 is 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 gemeente Schagen richt 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 gemeente Schagen alert is 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 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 Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de Basisregistratie Personen (BRP) en Waardedocumenten (WD) of Basisregistratie Adressen en Gebouwen (BAG) separaat beleid ontwikkeld en geïmplementeerd wordt, is de keuze gemaakt dit gemeentebrede informatiebeveiligingsbeleid op te stellen voor alle organisatie onderdelen.

In het gemeentebrede informatiebeveiligingsbeleid wordt op strategisch niveau beschreven welke uitgangspunten gelden ten aanzien van de informatieveiligheid van de gemeente Schagen. Dit document zal samen met het "Uitvoeringsplan informatiebeveiliging", 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.II 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 VNG/IBD van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) 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.

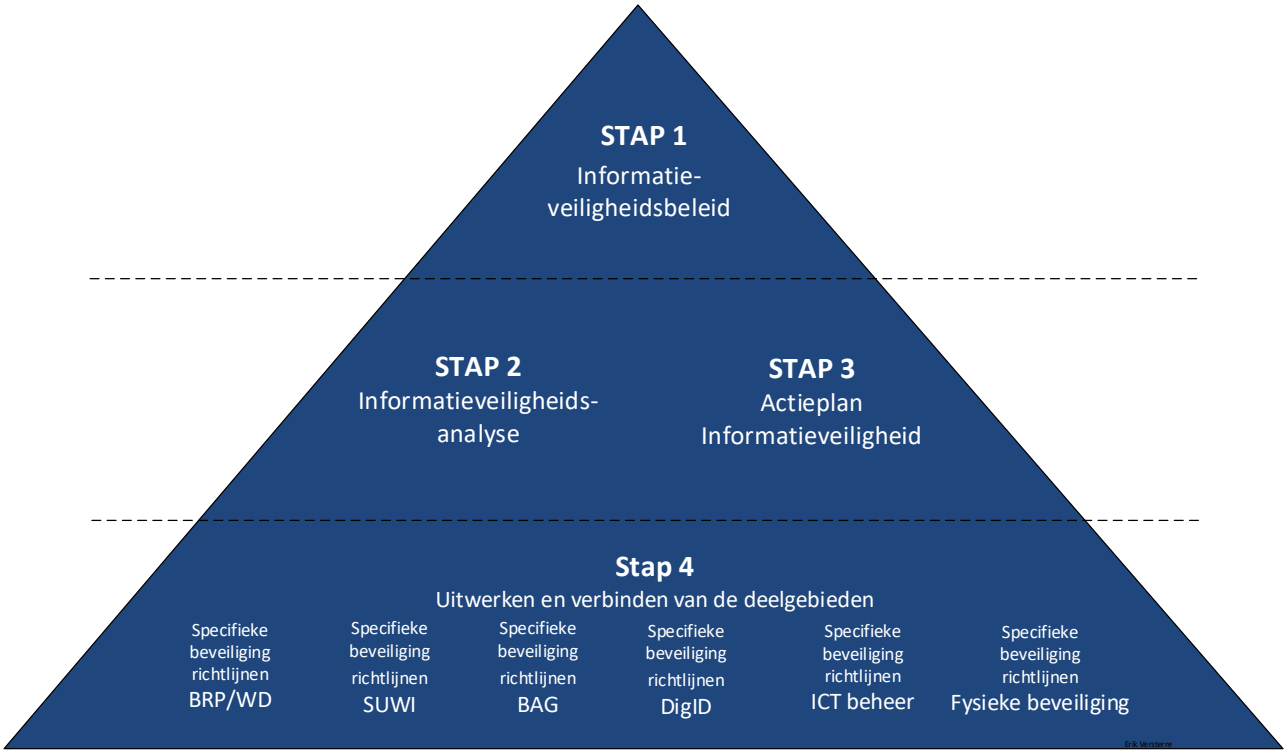
Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000 standaarden, de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/IBD) en aanvullende richtlijnen en eisen van het Nationaal Cyber Security Centrum (NCSC). Daarnaast is rekening gehouden met de wettelijke kaders die 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) en 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 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 informatiebeveiligingsbeleid aan. 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.

Het tactische niveau van de piramide is gericht op het tactische implementatietraject. De implementatiefase begint met het uitvoeren van een risico-inventarisatie en -evaluatie (RI&E). Tijdens deze RI&E worden de uitgangspunten uit het gemeentebrede informatiebeveiligingsbeleid getoetst aan de praktijksituatie. Hierin 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, cultuuraspecten en daarnaast op de sociale en fysieke inrichting van de gemeentelijke organisatie. Na de risico-inventarisatie vindt risicoweging en prioritering plaats, dit wordt gedaan aan de hand van een GAP-analyse. Tijdens deze stap worden risico's geconstateerd, 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 de BRP, de 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.III Toelichting op ISO 27001 en ISO 27002 (code voor informatieveiligheid)

Het gemeentebrede informatiebeveiligingsbeleid 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. De tweede standaard (27002) bevat een zeer uitgebreide verzameling van zogenaamde 'best practices' voor een praktische en concrete aanpak van informatieveiligheid binnen de organisatie. De Baseline Informatiebeveiliging Nederlandse Gemeenten 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.IV Verantwoordelijkheid en bevoegdheid informatiebeveiligingsbeleid

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 gemeentesecretaris
De vaststelling en implementatie van de informatieveiligheidsstructuur[2] en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de gemeente Schagen. Voor het nemen van operationele maatregelen is het afdelingshoofd KCC gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij cluster overstijgende (informatie)systemen.

[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.

Het afdelingshoofd KCC is verantwoordelijk voor de informatiesystemen van de gemeente. Deze systemen dienen te worden geclassificeerd en te worden ingericht 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.V 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.

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 (de mogelijkheid te kunnen achterhalen welke handelingen met de gemeentelijke informatiesystemen zijn uitgevoerd).

II.VI 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.
- Wet bescherming persoonsgegevens (Wbp).
- Algemene verordening gegevensbescherming (AVG)
- Archiefwet / Archiefregeling.
- Databankenwet.
- Wet elektronisch bestuurlijk verkeer;
- Wet elektronische handtekeningen;
- Wet algemene bepalingen Burgerservicenummer.
- Paspoortwet.
- Meldplicht datalekken.
- Wet basisregistratie personen (Wet BRP).
- Wet openbaarheid bestuur (Wob).
- Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI).
- Wet Basisregistratie Adressen en Gebouwen (BAG).
- Wet Kenbaarheid Publiekrechtelijke Beperkingen (WKPB).
- 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.

1. Informatiebeveiligingsbeleid

Visie:
Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de gemeente en de basis voor het beschermen van rechten van burgers en bedrijven. Dit vereist een integrale aanpak, goed opdrachtgeverschap en risicobewustzijn. Ieder organisatieonderdeel is hierbij bij betrokken. De komende jaren zet de gemeente Schagen in op het verhogen van informatieveiligheid en verdere professionalisering van de informatiebeveiligingsfunctie in de organisatie.

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 Beleidsuitgangspunten informatiebeveiliging gemeente Schagen

Het gehele gemeentelijk management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen).
De gemeente is zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van de regels volgens het principe van **Verplichtende Zelfregulering.** Hierbij geldt:

- Er is wetgeving waar altijd aan voldaan moet worden, zoals niet uitputtend: BRP, SUWI, BAG en PUIM, maar ook de archiefwet.
- Er is een gemeenschappelijk normenkader als basis: de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
- De gemeente stelt dit normenkader vast, waarbij er ruimte is voor afweging en prioritering op basis van het 'pas toe of leg uit' principe.
- Het systeem van verplichtende zelfregulering wordt geborgd door het onderdeel te maken van een interne cyclus, door transparantie en door toezicht.

1.2 Scope van het informatiebeveiligingsbeleid

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 gebruikte apparatuur. Organisatorisch zijn de uitgangspunten uit dit beleid van toepassing op zowel de ambtelijke organisatie als op (de leden van) het college en de gemeenteraad. Daarnaast bevat dit document de uitgangspunten voor handelen ten aanzien van informatieprocessen met keten- en uitvoeringspartners. Alle strategische beleidsuitgangspunten met betrekking tot informatieveiligheid en de organisatie van informatieveiligheid zijn in dit gemeentebreed document samengebracht.

1.3 Informatieveiligheidsanalyse

Op basis van dit beleidsdocument, welke door het college van B en W wordt vastgesteld, wordt door het managementteam het "Uitvoeringsplan informatiebeveiligingsbeleid", de "Informatieveiligheidsanalyse" en het "Actieplan informatieveiligheid" vastgesteld waarin wordt aangegeven op welke wijze het beleid uitgevoerd wordt.

De kernelementen in het uitvoeringsplan informatiebeveiliging zijn de uitwerkingen van de volgende onderwerpen:

- Beveiligingsaspecten ten aanzien van personeel.
- Fysieke beveiliging.
- Beheer van communicatie- en bedieningsprocessen.
- Logische toegangsbeveiliging.
- Verwerving, ontwikkeling en onderhoud van systemen.
- Beveiligingsincidenten.
- Continuïteitsbeheer.
- Naleving.

De kernelementen in de informatieveiligheidsanalyse zijn:

- Beschrijving van het huidige niveau van informatieveiligheid en de mate waarin aan de beveiligingseisen en -prioriteiten uit het strategische beleidsdocument en aan alle onderdelen van de informatieveiligheidsanalyse 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 dan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden daarvoor aanvullende maatregelen getroffen. Bij minder risicovolle verwerkingen kan een lager beveiligingsniveau worden overwogen.

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

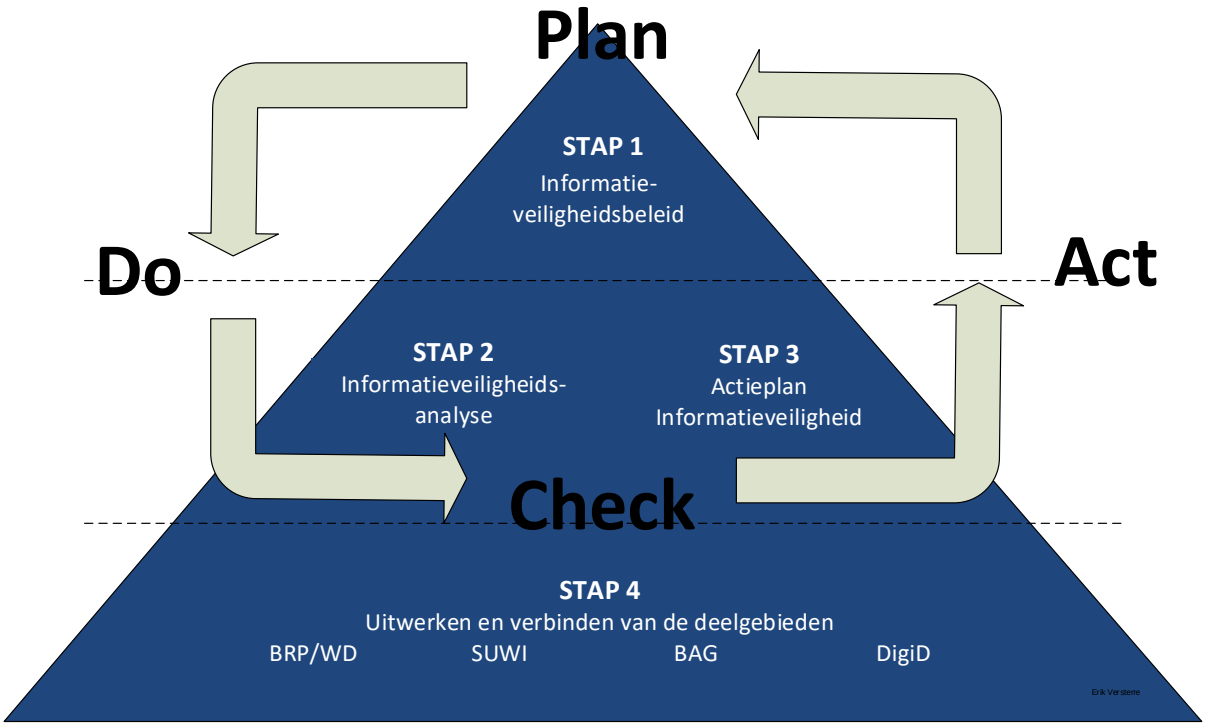
1.5 Borging van het informatiebeveiligingsbeleid

Om borging van het informatiebeveiligingsbeleid 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. **Informatiebeveiligingsbeleid:** bevat het informatiebeveiligingsbeleid en de visie op informatieveiligheid. Bijstelling van het informatiebeveiligingsbeleid vindt plaats rond een cyclus van 4 jaar. Indien zich grote wijzigingen voordoen vindt actualisatie eerder plaats;
2. **Informatieveiligheidsanalyse:** bevat de risicoanalyse (de toets aan de praktijk) op basis van informatiebeveiligingsbeleid en de normen die hierin zijn vermeld of de normen waar in het beleid naar wordt gerefereerd. Bijstelling van de informatieveiligheidsanalyse vindt plaats na 1 tot 2 jaar;
3. **Actieplan Informatieveiligheid:** bevat de concrete geprioriteerde acties volgend uit de informatieveiligheidsanalyse. De governance komt bij elkaar om de implementatie van het

actieplan informatieveiligheid te monitoren, dit vindt conform de bespreking in het informatieveiligheidsoverleg (zie paragraaf 2.2) vier maal per jaar plaats.

In de jaarrekening wordt gerapporteerd over het doorlopen van de beschreven cyclus met betrekking tot informatieveiligheid.



Figuur 2: De informatieveiligheidspiramide met PDCA cirkel

2. Organisatie van de informatieveiligheid

Doelstelling:
Het beheren van de informatiebeveiliging (IB) binnen de organisatie. Er is een beheerkader vastgesteld om de implementatie van informatiebeveiliging in de organisatie te initiëren en te beheersen.
Goedkeuring door het managementteam van het informatiebeveiligingsbeleid, de toewijzing van de rollen en de coördinatie en beoordeling van de implementatie van het beleid binnen de organisatie.

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 gemeente Schagen

Binnen de gemeente Schagen worden de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatieveiligheid onderscheiden:

2.1.1 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau
Het college van B en W van de gemeente Schagen draagt, ieder voor zich, als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatieveiligheid. Het college van B en W stelt de kaders ten aanzien van informatieveiligheid op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders.

2.1.2 Gemandateerde verantwoordelijkheden en taken op organisatieniveau
De gemandateerde verantwoordelijkheid voor informatieveiligheid ligt bij het afdelingshoofd KCC. Deze stelt in overleg met het managementteam en de CISO het gewenste niveau van informatieveiligheid vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. Het afdelingshoofd KCC 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.

Het afdelingshoofd KCC heeft in ieder geval de volgende verantwoordelijkheden:

- Het stellen van operationele kaders en het geven van sturing ten aanzien van de veiligheid van informatie.
- 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 inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatieveiligheid.

2.1.3 Verantwoordelijkheden en taken op afdelingsniveau
De afdelingshoofden zijn verantwoordelijk voor de (informatie)veiligheid van de informatieprocessen en -systemen binnen hun afdeling.

De *afdelingshoofden* hebben in ieder geval de volgende verantwoordelijkheden:

- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op de afdeling van toepassing zijn.
- Op basis van een expliciete risicoafweging 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, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn).

2.1.4 Chief Information Security Officer (CISO)

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het informatiebeveiligingsbeleid, 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:

- Rapporteert rechtstreeks aan de het afdelingshoofd KCC.
- Formuleert het informatiebeveiligingsbeleid.
- Stelt de informatieveiligheidsanalyse op 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 het afdelingshoofd KCC en het Management Team 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 informatiebeveiligingsbeleid en de informatieveiligheidsanalyse.
- 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 jaarrekening.

2.1.5 De coördinator ENSIA

Deze rol werkt de coördinator ENSIA (Eenduidige Normatiek Single Information Audit) mee aan het begeleiden, bewaken en waar nodig bijsturen van het ENSIA- verantwoordingsproces. De kerntaken zijn het creëren van bewustzijn over informatieveiligheid voor de hele gemeente en het organiseren van samenwerking.

De coördinator ENSIA heeft in ieder geval de volgende verantwoordelijkheden:

- Begeleidt, bewaakt en stuurt waar nodig bij in het ENSIA- verantwoordingsproces.
- Zorgt voor brede betrokkenheid en draagvlak in de organisatie.
- Zet de zelfevaluatie vragenlijst uit bij de verantwoordelijke personen; Bedrijfsvoering, Burgerzaken, Sociaal Domein, DigiD, BAG-beheer en BGT-beheer.
- Zorgt ervoor dat de bijbehorende documenten om de zelfevaluatie af te ronden, tijdig en compleet worden opgesteld, ingevoerd en geüpload.
- Zorgt dat zowel horizontaal als verticaal verantwoording op basis van de zelfevaluatie wordt afgelegd.
- Draagt zorg voor projectbemensing.
- Coördineert en bewaakt de uitvoering en voortgang.
- Verleent opdracht aan de auditor voor een Assurance-rapportage.
- Organiseert communicatie en voorlichting.
- Contactpersoon voor vertegenwoordigers van ICT, P&O (Bedrijfsvoering), Burgerzaken (BRP/PUN), Sociale Domein (SUWI), DigiD, BAG- en BGT-beheer.

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

De controller informatiebeveiliging 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 controller informatiebeveiliging is hiervoor verantwoordelijk, maar organiseert dit proces waar mogelijk met de inzet van beveiligingsbeheerders. Het principe hierbij is dat de toetsing binnen een bepaald domein plaatsvindt door een beveiligingsbeheerder van een ander domein en visa versa.
- 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 informatiebeveiligingsbeleid en de informatieveiligheidsanalyse.
- Toetsen/bewaken van het niveau van informatieveiligheid.
- Toetsing van evaluatieproces 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 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: DigiD, BRP, Waardedocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations en Autorisatiebevoegde Rijbewijzen), SUWI (officieel Security Officer SUWI), BAG (BAG beheerder). Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering: Facilitaire Zaken, ICT (Automatisering), DIV (Archivering) en P&O.

Specifieke verplichte beveiligingsbeheerdersrollen:
- 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.

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 informatiebeveiligingsbeleid, inclusief de maatregelen die op de audit en zelfevaluatie onderdelen gelden. Hieronder vallen:
- De voorbereiding en coördinatie van audits en (zelf)evaluaties.
- De preventie en detectie van beveiligingsincidenten en het geven van een adequate respons.
- Coördineren en toepassen van specifieke wet- en regelgeving.
- rapporteren aan de CISO en de controller informatiebeveiliging.

2.1.8 Security Officer SUWI
De Security Officer SUWI (de beveiligingsbeheerder SUWI) 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 en ziet er daarnaast op toe dat de maatregelen worden nageleefd. Ook adviseert de Security Officer medewerkers en management, doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet en evalueert de uitkomsten van verbetermaatregelen. De Security Officer verzorgt minimaal tweemaal per jaar een rapportage met betrekking tot de beveiligingsstatus van Suwinet aan het hoogste management en/of college. De Security Officer SUWI vraagt daarnaast meerdere keren per jaar een rapportage op bij het BKWI over het gebruik van Suwinet door de gemeente.

2.1.9 Privacybeheerder
Deze rol is gericht op de uitvoering en de naleving van de Wet bescherming van persoonsgegevens (Wbp), vanaf 25 mei 2018 van de 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 de privacywetgeving en adviseert het Management Team 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.
- De privacybeheerder heeft verder als taak:
    1. de uitleg van de privacyvoorschriften in de Wet bescherming persoonsgegevens (Wbp), vanaf 25 mei 2018 van de AVG, en daarnaast in de sectorale wetgeving;
    2. coördineren van de privacywerkzaamheden;
    3. coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de gemeente;
    4. verzorgen van meldingen en intrekkingen van meldingen bij de Autoriteit Persoonsgegevens (AP) tot de inwerkingtreding van de AVG;
    5. te fungeren als aanspreekpunt voor de AP tot de inwerkingtreding van de AVG;
    6. coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
    7. rapporteren aan het managementteam;
    8. richt procedures in voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
    9. beheer en onderhoud van de standaarddocumenten voor verwerkersovereenkomsten, convenanten en reglementen;
    10. advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van verwerkersovereenkomsten en convenanten en de vaststelling van reglementen;

2.1.10 Functionaris gegevensbescherming [3]
Op 25 mei 2018 treedt de algemene verordening gegevensbescherming (AVG) in werking. Voor overheidsinstanties zoals de gemeente Schagen zal het aanwijzen van een functionaris gegevensbescherming (FG) dan verplicht zijn (artikel 37 lid 1 AVG). Momenteel is er een privacybeheerder BRP, maar nog geen FG en ook geen gemeentebrede privacybeheerder binnen de gemeente Schagen. De FG zal een centraal punt zijn binnen de gemeente wat betreft de gegevensbescherming binnen de organisatie.

[3] Overgenomen uit 'Persoonsinformatie en privacy. Op weg naar een adequaat uitvoeringsniveau WBP door gemeente Rozendaal', M.W. (Marion) Anten & W. (Willem) de Vries, BMC Advies, 2017.

Het takenpakket van de FG zal uit de volgende punten bestaan (art. 39 lid 1 AVG):

- Informeren en adviseren van de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken over hun verplichtingen die voortvloeien uit de AVG en andere wetten 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 en toezien op de uitvoering daarvan.
- Samenwerken met en als contactpunt optreden voor de AP.

2.1.11 De afdeling Informatievoorziening en Automatisering
Het team I&A beheer waarvan de systeembeheerder deel uit maakt, beheert de werkplekken, serverplatformen, lokale netwerken, Wi-Fi 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 beveiligings-maatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de verantwoordelijken voor (informatie)systemen afgelegd.

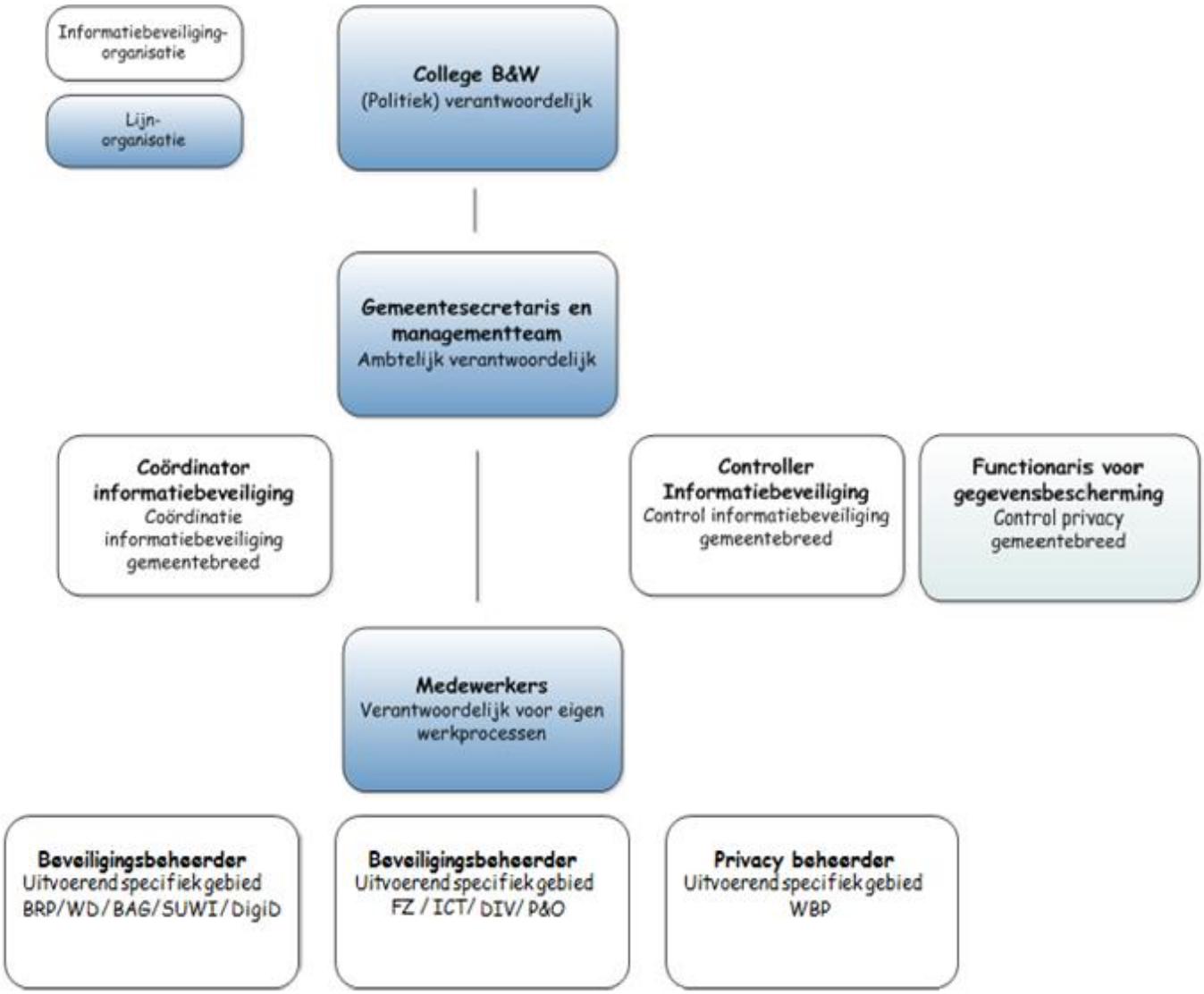
2.1.12 De beveiligingsbeheerder FZ
De beveiligingsbeheerder FZ is verantwoordelijk voor de fysieke veiligheid in en rond het gebouw, fysieke toegangsbeveiliging, de kantoorinrichting (archiefkasten, kluizen enzovoort) en contacten en contracten met externe partijen die voorzien in fysieke veiligheid, zoals alarmopvolging, bewaking en beveiliging.

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

2.1.14 De gegevensbeheerder
De gegevensbeheerder is verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatie-voorziening en voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

2.1.15 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 bijlage 2 staan de namen vermeld van de toegewezen rollen in de beveiligingsorganisatie.



Figuur 3: Functies en rollen in informatieveiligheidsorganisatie

2.2 Overleg en afstemmingsorganen

De CISO is voorzitter van het Informatiebeveiligingsoverleg (IBO) dat minimaal tweemaal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De CISO.
- De coördinator ENSIA.
- De controller Informatiebeveiliging.
- De beveiligingsbeheerders t.a.v.: BRP/Waardedocumenten, BAG, SUWI en DigiD.
- De beveiligingsbeheerders t.a.v.: FZ, ICT, DIV en P&O.
- De privacybeheerder en/of functionaris gegevensbescherming.
- Agendaleden: MT lid of specialist.

Onderwerpen:

- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het actieplan Informatieveiligheid.

- Beveiligingsincidenten.
- Planning en voorbereiding van Audits, controles en zelfevaluaties.
- Evaluatie en actualisatie informatiebeveiligingsbeleid 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 ICT crisisbeheersing

Voor interne crisisbeheersing dient een crisisteam informatieveiligheid geïnstalleerd te zijn. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit team bestaat in ieder geval uit:

- Afdelingshoofd KCC (voorzitter).
- CISO.
- De beveiligingsbeheerder ICT.
- De verantwoordelijke beveiligingsbeheerder (afhankelijk van het incident of de calamiteit).
- Relevante experts (indien nodig).
- Een lid van de afdeling communicatie.

De bovenstaande personen zullen eerst zelf bepalen wat de impact is van het incident of de calamiteit. Op basis van de mogelijke politieke gevolgen van het incident licht het afdelingshoofd KCC de verantwoordelijke portefeuillehouder in.

2.4 Rapporteren beveiligingsincidenten

De CISO wordt door de medewerkers 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 informatiebeveiligingsbeleid niet wordt nageleefd.

Afspraken moeten worden gemaakt over:

- doel van de registratie;
- inhoud van de registratie;
- mate van detaillering;
- wijze van handelen;
- wijze van rapporteren.

De CISO rapporteert aan de het afdelingshoofd KCC.

2.5 Verantwoordelijkheden afdeling overstijgende (informatie)systemen

De afdelingsoverstijgende (informatie)systemen binnen de gemeente worden onder de verantwoordelijkheid van ICT 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 het management het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt 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 schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het afdelingsoverstijgend (informatie)systeem gebruik maakt (de gebruikende partij).

Minimaal worden in deze afspraken vastgelegd:

- Voorwaarden voor het toegestane gebruik van het afdelingsoverstijgend (informatie)systeem.
- De verantwoordelijkheden van de gebruikende partij binnen zijn organisatieonderdeel voor de gegevens uit het afdelingsoverstijgend (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 de afspraken en oplossing 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 informatiebeveiligingsbeleid voldoet.

2.6 Contracten met derden

2.6.1 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 de website(s) wordt tussen de afdelingen van de gemeente Schagen 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.

2.6.2 Inhuren van derden
Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van de verantwoordelijk leidinggevende van de gemeente Schagen. Deze leidinggevende dient te waarborgen dat activiteiten binnen het kader van het informatiebeveiligingsbeleid worden uitgevoerd.

2.6.3 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.
- Voorafgaand aan het afsluiten van een contract voor uitbesteding en externe inhuur is bepaald wat de duur is van het contract.
- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een verwerkersovereenkomst (conform AVG artikel 28) 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.

2.6.4 Overeenkomsten met een derde partij en met betrekking tot ICT voorzieningen
Bij het aangaan van overeenkomsten met derde partijen gelden de volgende beveiligingseisen:

- De maatregelen behorend bij 2.7.3 zijn voorafgaand aan het ingaan van het contract gedefinieerd en geïmplementeerd.
- Uitbesteding (ontwikkelen en aanpassen) van software is geregeld volgens formele contracten waarin o.a. intellectueel eigendom, kwaliteitsaspecten, beveiligingsaspecten, aansprakelijkheid, escrow en reviews geregeld worden.
- In contracten met externe partijen is vastgelegd hoe men om dient te gaan met wijzigingen en hoe ervoor gezorgd wordt dat de beveiliging niet wordt aangetast door de wijzigingen.
- In contracten met externe partijen is vastgelegd hoe wordt omgegaan met geheimhouding en de geheimhoudingsverklaring.
- Er is een plan voor beëindiging van de ingehuurde diensten waarin aandacht wordt besteed aan beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid.
- In contracten met externe partijen is vastgelegd hoe escalaties en aansprakelijkheid geregeld zijn.
- Als er gebruikt gemaakt wordt van onderaannemers dan gelden daar dezelfde beveiligingseisen voor als voor de contractant. De hoofdaannemer is verantwoordelijk voor de borging bij de onderaannemer van de gemaakte afspraken.
- De producten, diensten en daarbij geldende randvoorwaarden, rapporten en registraties die door een derde partij worden geleverd, worden beoordeeld op het nakomen van de afspraken in de overeenkomst. Verbeteracties worden geïnitieerd wanneer onder het afgesproken niveau wordt gepresteerd.

2.6.4.1 Bewerkers van persoonsgegevens
De Algemene Verordening Gegevensbescherming (AVG) stelt regels voor het opslaan, verzamelen, vernietigen, verstrekken en combineren (kort gezegd: het verwerken) van persoonsgegevens. Wanneer een partij het verwerken van persoonsgegevens bij een andere partij uitbesteedt noemt men deze andere partij ‘een bewerker’. De gemeente Schagen legt in een register vast welke derden persoonsgegevens bewerken. Ook wordt vastgelegd of een verwerkersovereenkomst nodig is in de relatie tot die andere partij. In een verwerkersovereenkomst leggen de partijen onder andere vast voor welke doeleinden de gegevens verwerkt mogen worden, welke vormen van toezicht de eigenaar van de gegevens mag uitoefenen en hoe het zit met de onderlinge aansprakelijkheid. Het gemeentebestuur van de gemeente Schagen blijft ieder voor zich de verantwoordelijke voor de verwerking van persoonsgegevens.

3. Classificatie en beheer van informatie en bedrijfsmiddelen

Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie. Voor alle bedrijfsmiddelen is de eigenaar vastgelegd alsook de verantwoordelijke voor het handhaven van de beheersmaatregelen. de classificatie om bij verwerking de noodzaak en bescherming te kunnen aangeven. De adequate niveaus van bescherming van informatie zijn gedefinieerd en de noodzaak voor aparte verwerkingsmaatregelen is gecommuniceerd.

Doelstelling:
Het bepalen, handhaven en waarborgen van het juiste beveiligingsniveau voor informatie, (informatie) systemen en bedrijfsmiddelen.

Resultaat:
Een goed overzicht van alle ICT-componenten en andere relevante bedrijfsmiddelen en een toegewezen eigenaarschap. Een informatieclassificatiesysteem waarmee de behoefte, de prioriteit en de mate van beveiliging kan worden bepaald.

3.1 Inventarisatie van informatie en (informatie) bedrijfsmiddelen

Om een passend beveiligingsniveau te kunnen bieden, moeten de informatie en de bedrijfsmiddelen worden geïnventariseerd en de waarde en het belang ervan worden vastgelegd.

Informatievoorziening en Automatisering houdt een registratie bij van alle bedrijfsmiddelen die verband houden met (informatie) systemen (configuratiemanagement):

- Informatie (bijvoorbeeld databases, gegevensbestanden, documentatie en procedurebeschrijvingen).
- Programmatuur (bijvoorbeeld systeemprogrammatuur en standaardsoftware inclusief versiebeheer).
- Fysieke bedrijfsmiddelen (bijvoorbeeld apparatuur, schijven, accommodatie en netwerkinfrastructuur en actieve componenten).
- Diensten (bijvoorbeeld communicatiediensten, PKI diensten, energievoorziening ten behoeve van de informatievoorziening).

In de registratie is opgenomen waar de gegevens(bestanden) zijn opgeslagen, op welke computers de programmatuur draait, van welke componenten daarbij gebruik wordt gemaakt en wie de procesverant-woordelijken en beheerders zijn.

De afdeling Bedrijfsvoering houdt een registratie bij van alle fysieke voorzieningen die verband houden met (informatie) veiligheid van ruimten, gebouw(en) en de directe omgeving van de gemeentekantoren.

3.2 Eigendom van informatie en bedrijfsmiddelen

Alle informatie en bedrijfsmiddelen die verband houden met ICT-voorzieningen behoren een eigenaar te hebben in de vorm van een aangewezen deel van de organisatie. Voor elk bedrijfsproces, applicatie, gegevensverzameling en ICT-faciliteit is een verantwoordelijk leidinggevende benoemd.

3.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Er zijn regels vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met ICT voorzieningen en informatieprocessen. Hieronder volgen de geldende uitgangspunten:

- Apparatuur en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.
- De verantwoordelijkheid voor specifieke beheersmaatregelen mag door de eigenaar worden gemandateerd, maar de eigenaar blijft verantwoordelijk voor een goede bescherming van de bedrijfsmiddelen.
- Medewerkers dienen bij het gebruik van ICT-middelen, social media en gemeentelijke informatie de nodige zorgvuldigheid te betrachten en de integriteit en goede naam van de gemeente te waarborgen.
- Medewerkers gebruiken gemeentelijke informatie uitsluitend voor het uitvoeren van de aan hen opgedragen taken en het doel waarvoor de informatie is verstrekt.
- Privégebruik van gemeentelijke informatie en bestanden is niet toegestaan.
- Voor het werken op afstand en het gebruik van privémiddelen worden nadere regels opgesteld. Echter, de medewerker is gehouden aan regels zoals:
    - illegale software, of niet goedgekeurde software mag niet worden gebruikt voor de uitvoering van het werk;
    - er bestaat geen plicht de eigen computer te beveiligen, maar de gemeentelijke informatie daarop wel;
    - het verbod op ongewenst gebruik in de (fysieke) kantooromgeving geldt ook als dat via de eigen computer plaatsvindt.
- De medewerker neemt passende technische en organisatorische maatregelen om gemeentelijke informatie te beveiligen tegen verlies of tegen enige vorm van onrechtmatig gebruik. De medewerker houdt hierbij in ieder geval rekening met:
    - de beveiligingsclassificatie van de informatie;
    - de door de gemeente gestelde beveiligingsvoorschriften (o.a. dit informatiebeveiligingsbeleid)
    - aan de werkplek verbonden risico's;
    - het risico door het benaderen van gemeentelijke informatie met andere dan door de gemeente verstrekte of goedgekeurde ICT-apparatuur.

3.4 Classificatie van informatie en bedrijfsmiddelen

Om te kunnen bepalen welke beveiligingsmaatregelen moeten worden getroffen ten aanzien van informatieprocessen en informatiesystemen worden beveiligingsclassificaties gebruikt. De gemeentelijke informatiesystemen worden geclassificeerd op de drie kwaliteitsaspecten van informatie: beschikbaarheid, integriteit (juistheid, volledigheid) en vertrouwelijkheid (BIV). Onderstaande tabel geeft de classificatie niveaus weer. Na deze classificatie is onder meer duidelijk welke specifieke gemeentelijke informatie als vertrouwelijk wordt geclassificeerd. Na dit inzicht is duidelijk welke maatregelen per informatiesysteem nodig zijn.

Daar waar de maatregelen op de punten beschikbaarheid (niveau 'noodzakelijk'), integriteit (niveau 'hoog') en vertrouwelijkheid (niveau 'vertrouwelijk'), zoals gehanteerd in dit gemeentebreed informatiebeveiligingsbeleid (conform de BIG) als voldoende kunnen worden aangemerkt, is het niet noodzakelijk om aanvullende maatregelen te treffen. Door het implementeren van alle maatregelen, zoals beschreven in dit gemeentebreed informatiebeleid wordt het vereiste beveiligingsniveau voldoende afgedekt.

Classificatietabel			
Niveau	**Vertrouwelijkheid**	**Integriteit**	**Beschikbaarheid**
Geen / 0	**Openbaar** informatie mag door iedereen worden ingezien *(bv: algemene informatie op de externe website van de gemeente*	**Niet zeker** informatie mag worden veranderd *(bv: templates en sjablonen)*	**Niet nodig** gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn *(bv: ondersteunende tools als routeplanner)*
Laag / I	**Bedrijfsvertrouwelijk** informatie is toegankelijk voor alle medewerkers van de organisatie *(bv: informatie op het intranet)*	**Beschermd** het bedrijfsproces staat enkele (integriteits-) fouten toe *(bv: rapportages)*	**Noodzakelijk** informatie mag incidenteel niet beschikbaar zijn *(bv: administratieve gegevens)*
Midden / II	**Vertrouwelijk** informatie is alleen toegankelijk voor een beperkte groep gebruikers *(bv: persoonsgegevens, financiële gegevens*	**Hoog** het bedrijfsproces staat zeer weinig fouten toe *(bv: bedrijfsvoeringinformatie en primaire procesinformatie zoals vergunningen)*	**Belangrijk** informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk *(bv: voorwaardelijke primaire proces informatie)*
Hoog / III	**Geheim** informatie is alleen toegankelijk voor direct geadresseerde(n) *(bv: zorggegevens en strafrechtelijke informatie)*	**Absoluut** het bedrijfsproces staat geen fouten toe *(bv: specifieke gemeentelijke informatie op de website o.a. waaraan rechten zijn te ontlenen)*	**Essentieel** informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten *(bv: basisregistraties BRP en SUWI)*

Bijlage 1: begrippenlijst

Acceptatieprocedure
Procedure om vast te stellen of een nieuw (informatie)systeem voldoet aan de gestelde eisen van applicatiebeheer, onderhoud en exploitatie van de geautomatiseerde gedeeltes (software) van een informatiesysteem.

Application controls
Geprogrammeerde maatregelen binnen een applicatie ter waarborging van de vertrouwelijkheid, juistheid en volledigheid van de data. We kunnen hierbij denken aan het afschermen van menukeuzes, waardoor informatie niet oproepbaar is of het controleren van input op juistheid (postcode check) of volledigheid.

Audit (informatiebeveiliging)
Het door een onafhankelijke deskundige kritisch beoordelen van de opzet, het bestaan en de werking van de (beveiligings-) voorzieningen en de organisatie voor informatietechnologie op betrouwbaarheid, doeltreffendheid en doelmatigheid.

Authenticatie
Verificatie van de geclaimde identiteit, bijvoorbeeld door gebruik van wachtwoord, token, biometrie of een combinatie hiervan.

Autorisatie / autoriseren
Toekenning / toekennen van rechten (aan personen, processen en/of systemen).

Back-up
Reservekopie van een computerbestand of programmatuur.

Bedrijfskritisch
Van essentieel belang voor de continuïteit van de bedrijfsprocessen.

Beschikbaarheid
Zie continuïteit.

Beveiligingsincident
Voorval dat de betrouwbaarheid, beschikbaarheid of vertrouwelijkheid van de informatievoorziening verstoort, en daarmee de informatiebeveiliging kan aantasten.

Calamiteit
Gebeurtenis die een zodanige verstoring van de geautomatiseerde gegevensverwerking tot gevolg heeft, dat aanzienlijke maatregelen moeten worden genomen om het oorspronkelijke werkingsniveau te herstellen.

Change management
Beheer en beheersing van alle wijzigingen van componenten van (informatie)systemen en de ICT-infrastructuur.

Chief Information Security Officer (CISO)
Medewerker die gemeentebreed adviseert over informatiebeveiligingsvraagstukken in brede zin en activiteiten op het gebied van informatiebeveiliging coördineert.

Classificatie
Indeling in risicoklassen voor de aspecten beschikbaarheid, betrouwbaarheid, vertrouwelijkheid en waar nodig ook de controleerbaarheid.

Clear desk (ook wel clean desk)
Een opgeruimde werkplek waar geen vertrouwelijke of privacygevoelige documenten of andere informatiebronnen rondslingeren.

Clear screen
Een uitgeschakelde computer of afgesloten beeldscherm dat alleen met een inlogprocedure weer actief gemaakt kan worden.

Configuratie management
Beheer en beheersing van de samenstelling en de status van de ICT-infrastructuur en de (informatie)systemen die er gebruik van maken.

Configuratieschema
Overzicht van de onderdelen waaruit een (informatie)systeem is opgebouwd.

Continuïteit (bedrijfs-)
De mate waarin bedrijfsprocessen ongestoord doorgang kunnen hebben.

Continuïteitsmanagement
Stelsel van samenhangende activiteiten, mensen en middelen met als doel de continuïteit van de (kritische) bedrijfsprocessen te waarborgen.

Controller Informatiebeveiliging
Medewerker die zich richt op de verbijzonderde interne controle op de naleving van het informatiebeveiligingsbeleid en de escalatie van beveiligingsincidenten.

Coördinator ENSIA
Medewerker verantwoordelijk voor het begeleiden, bewaken en waar nodig bijsturen van het ENSIA-verantwoordingsproces. De kerntaken zijn het creëren van bewustzijn over informatieveiligheid voor UW Samenwerking en het organiseren van samenwerking.

Database
Een bestand waarin gedigitaliseerde gegevens op een gestructureerde manier zijn opgeslagen en bevraagd kunnen worden.

Datakluis
Brand- en inbraakwerende ruimte voor de opslag van (elektronische) gegevensdragers.

Document Structuurplan (DSP)
De Archiefwet maakt het maken en onderhouden van een Documentair Structuur Plan (DSP) verplicht. Een DSP biedt een overzicht van alle aanwezige informatie- en archiefbestanden van een organisatie in relatie tot het werk dat in die organisatie gedaan wordt.

Eigenaar
De eigenaar van een proces of een systeem is vanuit het informatiebeveiligingsbeleid verantwoordelijk voor het stellen van eisen en de inrichting van de controle hierop, zodat voldaan wordt aan het informatiebeveiligingsbeleid en aan de wettelijke eisen.

ENSIA
De ‘Eenduidige Normatiek Single Information Audit’.

Escrow
Specifiek in de softwaresector wordt escrow aangewend ter vrijwaring van de belangen van de softwareklant indien die zich wil indekken tegen bepaalde risico's in hoofde van de softwareleverancier (het meest gevreesde daarbij wellicht het faillissement van de leverancier). De softwareleverancier zal de broncode van de software (en de bijhorende documentatie) in bewaring geven bij de escrowagent, en deze broncode regelmatig updaten indien nieuwe versies op de markt gebracht worden. Indien de leverancier dan failliet zou gaan, heeft de klant tenminste de broncode van haar applicatie en kan zij alsnog trachten haar applicatie werkende te houden.

Functiescheiding
Het scheiden van gerelateerde taken en bevoegdheden met als doel het voorkomen van fouten en fraude.

Functionaris voor gegevensbescherming
25 mei 2018 treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Gemeenten moeten verplicht een functionaris voor gegevensbescherming aanwijzen ingevolge artikel 37 AVG. De FG moet betrokken worden bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. De FG heeft een onafhankelijke toezichthoudende rol binnen de organisatie en rapporteert rechtstreeks aan het managementteam. Daarnaast fungeert de FG als aanspreekpunt voor de Autoriteit Persoonsgegevens (AP).

Fysieke beveiliging
Beveiliging die met behulp van fysieke (bouwkundige, technische en/of organisatorische) middelen gerealiseerd wordt.

Gateway
Verbinding tussen verschillende netwerken waarop wordt bijgehouden welke computers c.q. protocollen met elkaar verbonden mogen worden.

Gebruiker / gebruikende partij
Degene die geautoriseerd gebruik maakt van een (informatie)systeem.

Gegevens
Feiten en begrippen, weergegeven in een vorm die geschikt is voor het communiceren, interpreteren en verwerken tot informatie, hetzij door de mens, hetzij door automatische middelen, dan wel beide.

Gegevensdrager
Een fysiek object waarin/waarop informatie is vastgelegd, bijvoorbeeld een boek, harde schijf, DVD of USB-stick.

Gegevensverwerking
Handeling of geheel van handelingen met betrekking tot gegevens.

Informatie- en communicatietechnologie (ICT)
Het vakgebied dat zich bezighoudt met informatiesystemen, telecommunicatie en computers. Hieronder valt het ontwikkelen en beheren van systemen, netwerken, databanken en websites. Ook het onderhouden van computers en programmatuur en het schrijven van administratieve software valt hieronder. Vaak gebeurt dit in een bedrijfskundige context.

ICT-component
Onderdeel van de informatie- en communicatie-infrastructuur, zoals netwerk, bekabeling, servers, werkstations.

Identificatie
Bepaling van de identiteit van een persoon, bijvoorbeeld door een unieke gebruikersnaam of netwerkadres.

Incident
Onverwachte of ongewone gebeurtenis.

Incidentmanagement
Beheer en beheersing van de afhandeling van incidenten.

Informatie
Informatie bestaat uit gegevens verzameld en uitgewerkt om te dienen als communicatie tussen personen. Informatie behoeft echter niet te zijn vastgelegd. De vormen van informatie kunnen zijn, digitaal, papier, beeld, geluid. De informatie kan opgeslagen worden digitaal en dossiers (papier).

Informatiebeveiliging
Samenhangend stelsel van activiteiten, methoden en middelen ter waarborging van beschikbaarheid, betrouwbaarheid en vertrouwelijkheid.

Informatiebeveiligingsbeleid
Strategie van een organisatie met betrekking tot informatiebeveiliging.

Informatiebeveiligingsplan
Document waarin beschreven staat welke beveiligingsmaatregelen getroffen worden/zijn op basis van het informatiebeveiligingsbeleid.

Informatiesysteem
Een samenhangende, gegevensverwerkende functionaliteit voor de besturing of ondersteuning van één of meer bedrijfsprocessen.

Informatievoorziening
Het geheel aan processen, bestaande uit het verzamelen, het opslaan, het verwerken van gegevens en het beschikbaar stellen ervan.

Internet Protocol (IP)
Veel gebruikt protocol voor netwerkverkeer.

Information Technology Infrastructure Library (ITIL)
Een referentiekader voor het inrichten van de beheerprocessen binnen een ICT-organisatie. ITIL is geen methode of model, maar eerder een reeks van best practices (de beste praktijkoplossingen) en concepten.

Local Area Network (LAN)
Zie Lokaal netwerk.

Logische (toegangs)beveiliging
(Toegangs)beveiliging die met behulp van programmatuur gerealiseerd wordt.

Lokaal netwerk (LAN)
Fysiek afgegrensd, instellingsgebonden netwerk.

Maatwerkprogrammatuur
Op specifiek (deel)proces toegesneden programmatuur.

MARAP
Management Rapportage.

Medium (opslag-)
Fysieke gegevensdrager.

Netwerk
Een verzameling objecten voor communicatie tussen tenminste twee knooppunten van apparatuur en programmatuur, waarbij gebruik gemaakt wordt van voorgeschreven communicatieprotocollen.

Netwerkadres (IP Adres)
Unieke identificatie van een element in een netwerk.

Netwerkconfiguratie
Overzicht van de objecten waaruit het netwerk bestaat en de relaties tussen deze objecten.

Noodplan
Document waarin beschreven staat welke acties een organisatieonderdeel moet ondernemen in een noodsituatie.

Ontruimingsplan
Document waarin beschreven staat op welke wijze een gebouw ontruimd moet worden in een noodsituatie.

OTAP
Een methodiek die wordt gebruikt in de ICT. Dit geeft een pad aan dat wordt doorlopen tijdens onder andere softwareontwikkeling of het implementeren van nieuwe applicaties.

Personal Digital Assistant (PDA)
Kleine computer, formaat "binnenzak".

PKI (Public Key Infrastructure)
Een Public Key Infrastructure (PKI) is een systeem waarmee uitgiften en beheer van digitale certificaten kan worden gerealiseerd. Een onafhankelijke partij waarborgt de integriteit en authenticiteit van het certificaat. Hiermee wordt gegarandeerd dat de identiteit van de certificaatbezitter klopt ("je bent wie je zegt dat je bent") en dat gegevens veilig kunnen worden uitgewisseld.

Privacybeheerder
Medewerker die adviseert over privacybescherming en activiteiten ter bescherming van persoonsgegevens en privacy coördineert.

Proces
Een samenhangende serie activiteiten ten behoeve van een van tevoren bepaald doel.

Procesoverstijgend informatiesysteem (CIS)
Systeem dat door meer dan één afdeling wordt gebruikt en waarin gegevens van meerdere organisatieonderdelen worden vastgelegd.

Procesverantwoordelijkheid / procesverantwoordelijke
Verantwoordelijkheid / verantwoordelijke voor het geheel van activiteiten van een bepaald proces.

Programmatuur
Het geprogrammeerde deel van (informatie)systemen.

Recovery
Herstel van een computerbestand of programmatuur.

Risicoanalyse
Methode die informatie oplevert over de schadeverwachting van bepaalde gebeurtenissen.

Routering
Het bepalen van de weg die berichten volgen security scan gericht onderzoek naar de mate van implementatie van beveiligingsmaatregelen.

Service Level Agreement (SLA)
Schriftelijke overeenkomst tussen een aanbieder (service provider) en een afnemer (klant) van bepaalde diensten.

Smartphone
Programmeerbare telefoon die voor vele uiteenlopende doeleinden gebruikt kan worden, zoals internet.

SNMP
Simple Network Management Protocol: zie diagnoseprotocol.

Systeem
Een verzameling van één of meer samenhangende objecten met tezamen een gespecificeerde functionaliteit. Objecten kunnen zowel een fysiek (computersysteem) als logisch (besturingssysteem) zijn.

Systeemeigenaar
Verantwoordelijke voor een (informatie)systeem.

Systeemhulpmiddel
Hulpprogramma voor beheer en onderhoud van (informatie)systemen en ICT-infrastructuur.

Systeemklok
Interne klok in een computersysteem.

Systeemprivilege
Recht op het gebruik van of toegang tot (een onderdeel van) een (informatie)systeem.

Systeemprogrammatuur
Fundamentele, ondersteunende programmatuur die behoort tot de technische infrastructuur van een (informatie)systeem.

Technisch beheer
Opslag en onderhoud van digitale informatie door middel van technische maatregelen.

Telewerken
Thuis of op een andere locatie werken op het netwerk van de organisatie met behulp van een externe lijnverbinding.

Third Party Mededeling (TPM)
Verklaring van een onafhankelijke derde partij die door betrokken partijen vertrouwd wordt.

Utility
Zie Systeemhulpmiddel.

Voice over IP (VOIP)
Gebruik van dezelfde netwerkbekabeling voor zowel spraak- als datacommunicatie.

Webapplicatie
Toepassingsprogrammatuur die via een internetbrowser benaderd kan worden.

Wide Area Network (WAN)
Netwerk dat zich niet beperkt tot één fysieke locatie en waaraan meerdere lokale netwerken (LAN's) gekoppeld kunnen zijn.

Bijlage 2: rollen en namen informatiebeveiligingsorganisatie

Rol	Naam
CISO	
Coördinator ENSIA	
Controller Informatiebeveiliging	
Beveiligingsbeheerder BRP en WD	
Beveiligingsfunctionaris reis- en waardedocumenten	
Beveiligingsbeheerder DigiD	
Beveiligingsbeheerder BAG	
Beveiligingsbeheerder SUWI	
Beveiligingsbeheerder FZ	
Beveiligingsbeheerder ICT	
Beveiligingsbeheerder DIV	
Beveiligingsbeheerder P&O	
Privacybeheerder	
Functionaris Gegevensbescherming (FG)	