Strategisch gemeentebreed informatieveiligheidsbeleid

Versie : 1.0

Auteur : Olaf Holtrop, Duo+
John van der Sluis, senior adviseur Informatieveiligheid, BMC

Datum : 19 december 2017

I Voorwoord

I.I Totstandkoming

In dit document is het strategische informatieveiligheidsbeleid beschreven van de Duo gemeenten.

Het informatieveiligheidsbeleid 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 (BIG) door de Informatiebeveiligingsdienst (IBD) opgeleverd. Tijdens de Buitengewone Algemene Ledenvergadering (BALV) van de VNG op 29 november 2013, is de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangenomen. Hierin is opgenomen dat de Nederlandse gemeenten de BIG als uitgangspunt nemen om de informatiebeveiliging binnen de gemeentelijke overheid te organiseren en te waarborgen.

De BIG bestaat uit een Strategische en een Tactisch-operationele variant. Dit document bevat de visie van het besturen van de Duo gemeenten op informatiebeveiliging, geeft aan hoe de gestelde inzichten en doelstellingen bereikt gaan worden, inclusief een samenhangende reeks stappen die de continuïteit van informatieveiligheid borgen.

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, namelijk het "Tactisch gemeentebreed informatieveiligheidsbeleid", wordt aan de hand van de BIG het inhoudelijke normenkader uitgewerkt. Hierin worden alle normen en maatregelen vanuit de BIG verder uitgewerkt, die leidend zal zijn voor alle organisatieonderdelen van de Duo gemeenten. Met instemming van het voorliggende document wordt direct ingestemd met de verdere uitwerking, die beschreven zal worden in het "Tactisch gemeentebreed informatieveiligheidsbeleid".

In dit "Tactisch gemeentebreed informatieveiligheidsbeleid" worden de informatiebeveiligingsnormen beschreven. Elk hoofdstuk begint met de doelstelling en het beoogde resultaat en beschrijft vervolgens de basisnormen.
De indeling van het informatiebeveiligingsbeleid is gebaseerd op de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Als referentie zijn de hoofdstuknummers uit de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) achter ieder hoofdstuk vermeld.

- Waarom informatiebeveiliging?
- Informatiebeveiligingsbeleid en -plan (BIG hoofdstuk 5).
- Organisatie van de informatiebeveiliging (BIG hoofdstuk 6).
- Classificatie en beheer van informatie en bedrijfsmiddelen (BIG hoofdstuk 7).
- Beveiligingsaspecten ten aanzien van personeel (BIG hoofdstuk 8).
- Fysieke beveiliging (BIG hoofdstuk 9).
- Beheer van communicatie- en bedieningsprocessen (BIG hoofdstuk 10).
- Logische toegangsbeveiliging (BIG hoofdstuk 11).

- Verwerving, ontwikkeling en onderhoud van systemen (BIG hoofdstuk 12)
- Beveiligingsincidenten (BIG hoofdstuk 13).
- Continuïteitsbeheer (BIG hoofdstuk 14).
- Naleving (BIG hoofdstuk 15).

Bijlagen:

- Begrippenlijst.
- Inventarisatie van relevante wet en regelgeving.

Met dit strategisch informatieveiligheidsbeleid wordt daarnaast bepaald dat Duo+ 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:
Een betrouwbare informatievoorziening is noodzakelijk voor het goed functioneren van de Duo gemeenten en Duo+ 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 betrokken. De komende jaren zetten de Duo gemeenten en Duo+ in op het verhogen van informatieveiligheid en verdere professionalisering van de IB-functie in de organisatie.

De komende jaren zetten de Duo gemeenten, en de mede door de Duo gemeenten opgerichte Gemeenschappelijke Regeling Duo+, in op het verhogen van informatieveiligheid.
De Duo gemeenten zijn informatie-intensieve organisaties met een primaire focus op de dienstverlening. Deze organisatiekenmerken vragen om een betrouwbare en veilige informatievoorziening. De medewerkers 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 Duo gemeenten.

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

Daarnaast zijn de Duo gemeenten steeds afhankelijker van goed werkende informatievoorziening en -systemen. Dit betekent dat de Duo gemeenten alert zijn op mogelijke verstoringen van of bedreigingen gericht op informatiesystemen, mede omdat veel informatiesystemen niet primair 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 organisatie 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 informatieveiligheidsbeleid op te stellen voor alle organisatie onderdelen.

In het gemeentebrede informatieveiligheidsbeleid wordt op strategisch niveau beschreven welke uitgangspunten gelden ten aanzien van de informatieveiligheid. Dit document zal samen met het "Tactisch gemeentebreed informatieveiligheidsbeleid", de technische beveiligingsmaatregelen en de procedures een adequaat niveau van beveiliging voor de organisaties 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 Duo gemeenten zijn gewaarborgd.

II.II De informatieveiligheidspiramide

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 en samenwerkingsverbanden bij hun inspanningen om de veiligheid van overheidsinformatie te verhogen.

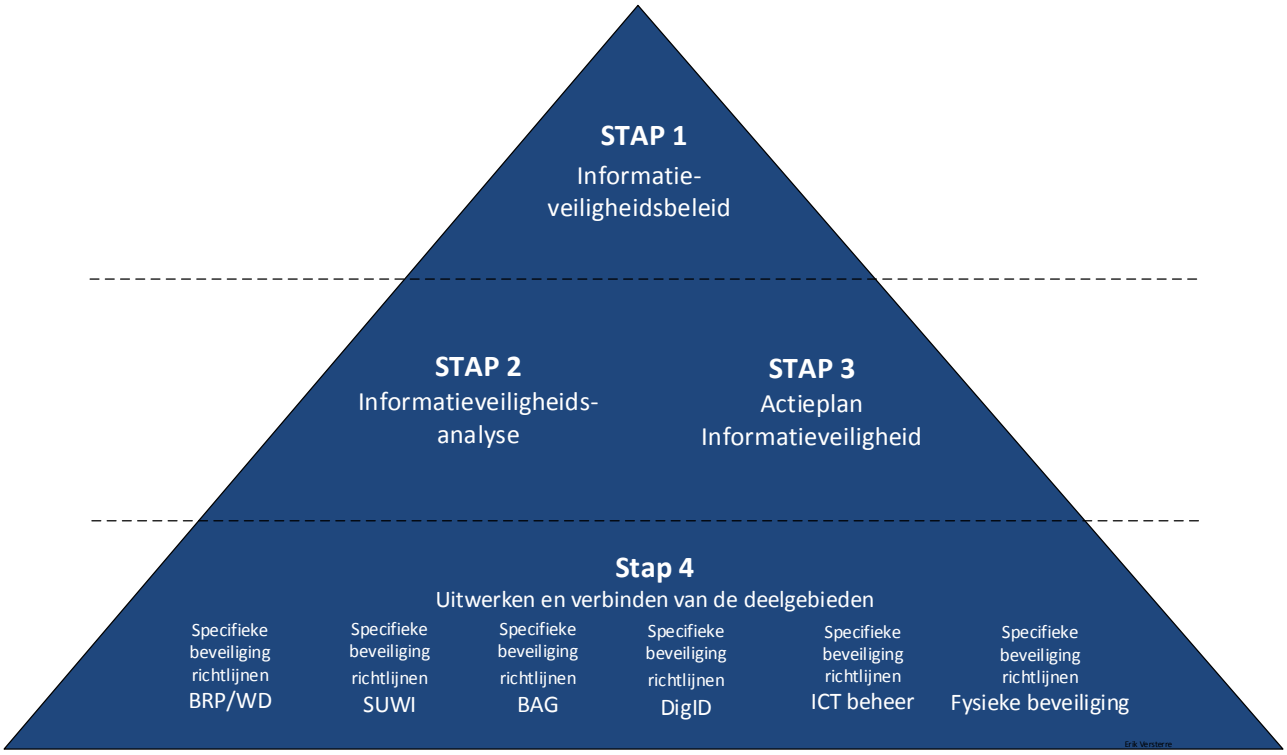
Dit document is gebaseerd op de richtlijnen uit de internationale NEN/ISO 27000 standaarden, de Baseline Informatiebeveiliging Nederlandse Gemeenten (VNG/IBD) en aanvullende richtlijnen en eisen van het Nationaal Cyber Security Centrum (NCSC). Daarnaast is rekening gehouden met de wettelijke kaders die 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 informatieveiligheidsbeleid 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 GAP-analyse. Tijdens deze GAP-analyse 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 GAP-analyse vindt als slot nog een risicoweging, prioritering en planning van te nemen maatregelen plaats. Tijdens deze stap worden risico's, die zijn 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 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. 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 informatieveiligheidsbeleid

De gemeenteraden van de drie deelnemende gemeenten binnen de Duo gemeenten dragen de specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente[1], zo ook voor informatieveiligheid. De eindverantwoordelijkheid voor informatieveiligheid ligt op bestuurlijk niveau bij de drie Colleges (accountable), de directeur Duo+ is voor de dagelijkse uitvoering verantwoordelijk (responsible). Indien het specifiek alleen een van de drie deelnemende gemeenten betreft, is de gemeentesecretaris

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

van de desbetreffende gemeente mede verantwoordelijk. De eindverantwoordelijkheid bestaat uit vaststelling en implementatie van de informatieveiligheidsstructuur[2] en de gemeentebrede beleidsnormen. Voor het nemen van operationele maatregelen op het gebied van informatieveiligheid is de directeur Duo+ gemandateerd. Dit betekent dat de directeur Duo+ toeziet op ontwikkeling en beheer van geschikt instrumentarium om informatieveiligheid te kunnen waarborgen. Dit geldt ook in geval van ketenafhankelijkheid en bij cluster overstijgende (informatie)systemen. Indien het specifiek alleen een van de drie deelnemende gemeenten betreft, is de gemeentesecretaris van de desbetreffende gemeente mede verantwoordelijk.

Voor de informatiesystemen zijn de leidinggevenden/proceseigenaren verantwoordelijk, zij dragen er zorg voor dat de informatiesystemen geclassificeerd en ingericht worden naar Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV), 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.

[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.

- 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).
- Basisregistratie Grootschalige Topografie (BGT).
- Generieke digitale infrastructuur (GDI).

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. 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

De colleges van burgemeester en wethouders van de Duo gemeenten behoren het gemeentebreed beleidsdocument voor informatieveiligheid goed te keuren, uit te geven en kenbaar te maken aan alle medewerkers (ook die van de bedrijfsvoeringsorganisatie Duo+), alsmede hiernaar te handelen.

De volgende aspecten zijn in dit beleidsdocument aanwezig:
- De doelstellingen van informatieveiligheid voor de Duo gemeenten.
- De beveiligingseisen en –prioriteiten.
- De organisatie van de informatieveiligheidsfunctie (zie hoofdstuk 2).
- Een omschrijving van de algemene en specifieke verantwoordelijkheden en bevoegdheden met betrekking tot informatieveiligheid voor leidinggevenden, medewerkers en ondersteunende informatiebeveiligingsrollen (zie hoofdstuk 2).
- De verwijzing naar relevante wet- en regelgeving en gemeentelijke regels en voorschriften op het gebied van privacybescherming, integriteit, archivering en fysieke beveiliging (zie II.II) en de wijze waarop naleving van deze wettelijke, reglementaire of contractuele verplichtingen wordt gewaarborgd (zie II.VI).
- De beschrijving van een periodiek evaluatieproces waarmee de inhoud en de effectiviteit van het vastgestelde beleid kunnen worden getoetst (zie 1.5).

1.2 Scope van het informatieveiligheidsbeleid

De scope van dit beleid omvat alle gemeentelijke informatieprocessen, hieronder vallen zowel de ambtelijke als bestuurlijke informatieprocessen. 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) de drie colleges en de drie gemeenteraden. 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 praktisch samengebracht.

1.3 Informatieveiligheidsanalyse

Op basis van dit strategische beleidsdocument, welke door de drie colleges van B en W wordt vastgesteld, werkt de directeur Duo+ het “Tactisch gemeentebreed informatieveiligheidsbeleid”, de “Informatieveiligheidsanalyse” en het “Actieplan informatieveiligheid” uit. Het Directieberaad Duo+ en Bestuur Duo+ zien

toe op haalbaarheid van de voorgestelde instrumenten, voor alle onderdelen van de Duo organisatie en coherentie met overige afspraken, welke intern en extern gericht kunnen zijn.

De kernelementen in het tactische gemeentebrede informatieveiligheidsbeleid 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 en de daarbij horende dataclassificatie blijkt dat voor bepaalde gegevensverwerkingen een hoger beveiligingsniveau is vereist dan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) worden daarvoor aanvullende maatregelen getroffen. In bepaalde gevallen zal hiervoor toestemming gevraagd worden aan de drie colleges van B en W. 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) en de Algemene verordening gegevensbescherming (AVG).

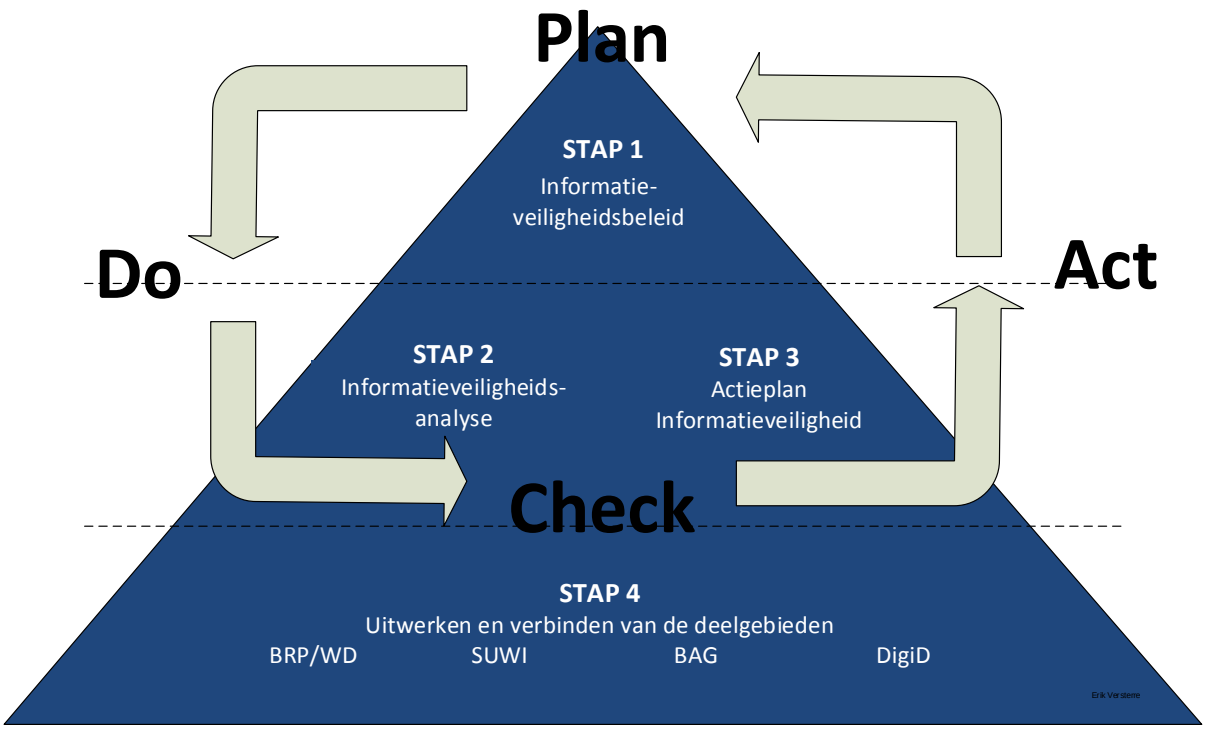
1.5 Borging van het informatieveiligheidsbeleid

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 (zowel strategisch als tactisch):** bevat het informatieveiligheidsbeleid en de visie op informatieveiligheid. Bijstelling van het informatieveiligheidsbeleid 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 informatieveiligheidsbeleid 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 (GAP). De Projectgroep Informatie Beveiliging (PIB) komt bij elkaar om de implementatie van het actieplan informatieveiligheid te monitoren, dit vindt conform 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 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 Duo gemeenten

Binnen de Duo gemeenten worden de volgende verantwoordelijkheids- en takenniveaus met betrekking tot informatieveiligheid onderscheiden:

2.1.1 Beleidsbepalende, regisserende en coördinerende verantwoordelijkheden op organisatieniveau

De drie gemeenteraden hebben de specifieke bevoegdheid om de werking van het beleid binnen de Duo organisatie te controleren, inclusief het informatiebeveiligingsbeleid. De verantwoordelijkheid voor informatiebeveiliging ligt op bestuurlijk niveau bij de drie colleges van B&W en op ambtelijk niveau bij de gemeentesecretarissen. Wanneer een taakgebied is overgedragen aan de bedrijfsvoeringsorganisatie Duo+, is dit belegd bij de directeur Duo+.

De directeur Duo+ is verantwoordelijk voor het inrichten van de beveiligingsorganisatie, met aan het hoofd de CISO. De CISO houdt onafhankelijk toezicht, rapporteert of de gewenste informatiebeveiligingsniveaus voor de Duo gemeenten worden gehaald. Dat leidt tot gevraagd en ongevraagd advies aan diverse gremia, waaronder de directeur Duo+ en indien het specifiek alleen een van de drie deelnemende gemeenten betreft, de gemeentesecretaris van de desbetreffende gemeente.

Beveiligingseisen worden per proces vastgesteld. De drie Colleges wijzen, volgend op beleidskeuzes, voor ieder bedrijfsproces een verantwoordelijke aan, waarmee zij ook de verantwoordelijke voor elk informatiesysteem impliciet aanwijst. Deze lijnverantwoordelijken krijgen via de beveiligingsorganisatie best practices en hulpmiddelen aangeboden om de beveiligingseisen samen te stellen die bij het proces horen waarvoor zij verantwoordelijk zijn.

De directeur Duo+ heeft in ieder geval de volgende verantwoordelijkheden. Dit in overleg met het Directieraad:

- 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 vastleggen van de verantwoordelijkheid voor informatieveiligheidscomponenten en –systemen.
- Het vastleggen van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatieveiligheid.

2.1.2 Verantwoordelijkheden en taken van leidinggevenden
De leidinggevenden zijn verantwoordelijk voor de (informatie)veiligheid van de informatieprocessen en -systemen binnen hun organisatie-onderdeel.

De leidinggevenden hebben in ieder geval de volgende verantwoordelijkheden*:*
- Het (laten) uitvoeren van maatregelen uit de informatieveiligheidsanalyse die op het organisatie-onderdeel van toepassing zijn.
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de informatiesystemen.
- 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 aanwijzen van beveiligingsbeheerders en andere medewerkers binnen de beveiligingsorganisatie, wanneer classificatie van de gegevensset of het informatiesysteem daartoe aanleiding geeft.

2.1.3 Chief Information Security Officer (CISO)
De CISO, ook wel de coördinator Informatiebeveiliging genoemd, is op organisatieniveau verantwoordelijk voor het actueel houden van het informatieveiligheidsbeleid, het coördineren van de uitvoering van het beleid, het adviseren bij projecten, het beheersen van risico's, evenals het opstellen van rapportages.

De *CISO* heeft in ieder geval de volgende verantwoordelijkheden:
- Rapporteert rechtstreeks aan de besturen van de Duo gemeenten en aan de directeur Duo+ indien van toepassing.
- Coördineert het formuleren van informatieveiligheidsbeleid.
- 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.
- De periodieke toetsing op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid. De *CISO* 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.
- Stelt een plan op voor overleg en rapportage met betrekking tot informatieveiligheid.
- Ondersteunt de managementteams en besturen van de Duo gemeenten met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen.
- Is aanspreekpunt voor medewerkers van de Duo gemeenten over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en de informatieveiligheidsanalyse.
- Bevordert het beveiligingsbewustzijn in de Duo gemeenten, zorgt voor brede betrokkenheid en draagvlak in de organisaties.
- 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 Duo gemeenten in de documentatie van de P&C-cyclus.

- De controle op de voortgang van het uitvoeren van de maatregelen uit de informatieveiligheidsanalyse en actieplan informatieveiligheid.
- De controle op de periodieke actualisatie van het informatieveiligheidsbeleid en de informatieveiligheidsanalyse.
- Toetsen/bewaken van het niveau van informatieveiligheid.
- Toetsing van evaluatieproces van beveiligingsincidenten.
- Samen met de ENSIA-coördinator bewaakt en stuurt hij waar nodig bij in het ENSIA- verantwoordingsproces dat aan de Duo gemeenten is opgelegd.
- Organiseert communicatie en voorlichting.

2.1.4 De coördinator ENSIA

De coördinator ENSIA (Eenduidige Normatiek Single Information Audit) werkt mee aan het begeleiden, bewaken en waar nodig bijsturen van het ENSIA- verantwoordingsproces. De kerntaken zijn het creëren van bewustzijn over informatieveiligheid voor de Duo organisatie 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 binnen de Duo gemeenten.
- 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.
- Organiseert communicatie en voorlichting.
- Contactpersoon voor de beveiligingsbeheerders van de Duo gemeenten.

2.1.5 De beveiligingsbeheerder

Deze rol is verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen en de informatiesystemen die toegang tot en beheer van deze gegevens regelen. Voorbeelden van de deelgebieden waarbij een beveiligingsbeheerder is aangewezen: 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.

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

2.1.5.1 De controller Informatiebeveiliging
Deze rol is op organisatieniveau verantwoordelijk voor het verbijzonderde toezicht op de naleving van de specifieke verplichte beveiligingsbeheerdersrollen:

- *Autorisatiebevoegde/beveiligingsfunctionaris Reisdocumenten/Aanvraagstations*
  Verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations) en toezicht op de naleving van de beveiligingsprocedures reisdocumenten.
- *Autorisatiebevoegde Rijbewijzen/beveiligingsfunctionaris rijbewijzen*
  Verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW en toezicht op de naleving van de beveiligingsprocedures rijbewijzen.

2.1.5.2 Privacybeheerder
Deze rol is gericht op de uitvoering en de naleving van de Wet bescherming van persoonsgegevens (Wbp) en interne afspraken over de classificatie van de (persoons-)gegevens. 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 de managementteams en leidinggevenden bij wijzigingen in proces uitvoering, bedrijfsvoering en de toepassing van een privacy impact assessment (PIA).
- 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:
  a) de uitleg van de privacyvoorschriften in de Wet bescherming persoonsgegevens (Wbp), vanaf 25 mei 2018 van de AVG, en daarnaast in de sectorale wetgeving;
  b) coördineren van de privacywerkzaamheden;
  c) coördineren, samenvoegen en openbaar maken van de overzichten van gegevensverwerkingen die worden aangeleverd door de organisatieonderdelen van de Duo gemeenten;
  d) beheer en onderhoud van de standaarddocumenten voor bewerkersovereenkomsten, convenanten en reglementen.

2.1.5.3 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 Duo gemeenten.

2.1.6 Functionaris gegevensbescherming [3]

Op 25 mei 2018 treedt de algemene verordening gegevensbescherming (AVG) in werking. Voor overheidsinstanties zoals de Duo gemeenten zal het aanwijzen van een functionaris gegevensbescherming (FG) dan verplicht zijn (artikel 37 lid 1 AVG). De FG zal een centraal punt zijn binnen de Duo gemeenten wat betreft de gegevensbescherming binnen de Duo gemeenten.

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

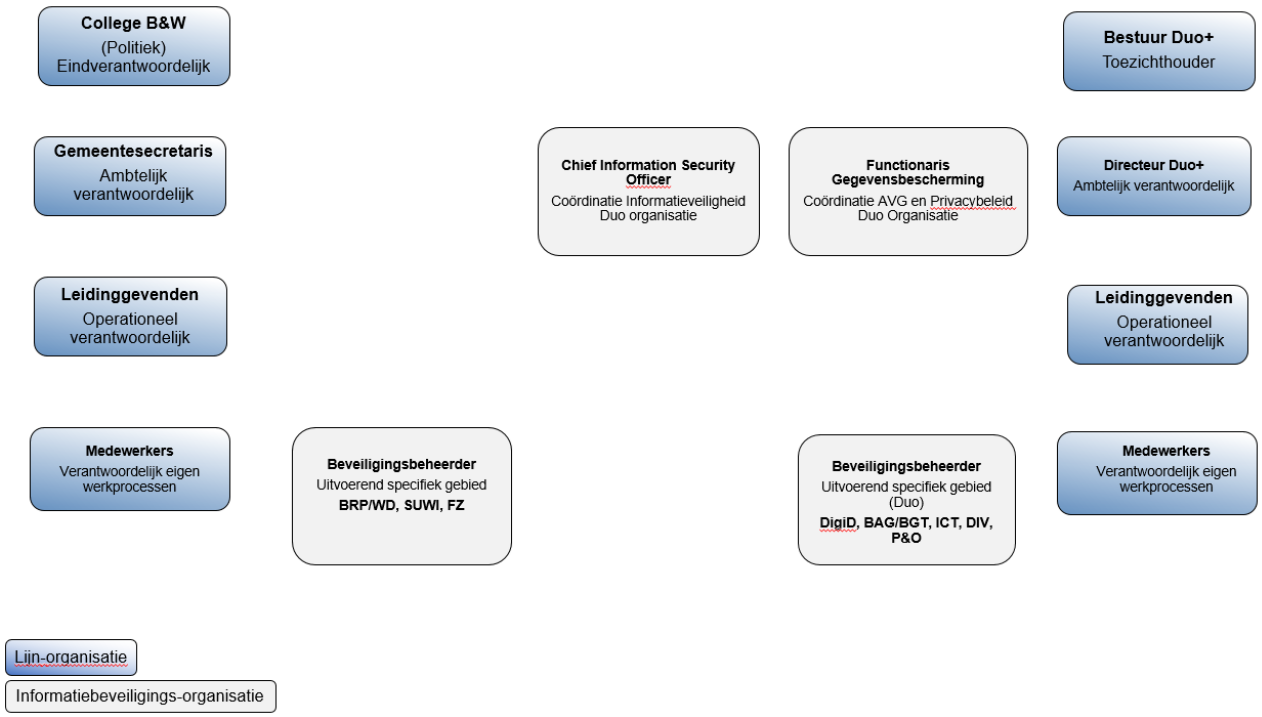
- Informeren en adviseren van de verwerkingsverantwoordelijke of de verwerker en de werknemers die verwerken over hun verplichtingen die voortvloeien uit de AVG en andere wetten met betrekking tot gegevensbescherming.
- Toezien op naleving van zowel de AVG en andere wetten met betrekking tot gegevensbescherming 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:
    - verzorgen van meldingen en intrekkingen van meldingen bij de Autoriteit Persoonsgegevens (AP) tot de inwerkingtreding van de AVG;
    - coördineren van verzoeken om inzage, correctie en verzet ten aanzien van persoonsgegevens en adviseren over de afhandeling;
    - rapporteren aan het managementteam van de desbetreffende gemeente;
    - inrichten procedures voor het afhandelen van datalekken waarbij persoonsgegevens betrokken zijn;
    - beheer en onderhoud van de standaarddocumenten voor bewerkersovereenkomsten, convenanten en reglementen;
    - advisering en ondersteuning bij het besluitvormingsproces en het afsluiten van bewerkersovereenkomsten en convenanten en de vaststelling van reglementen.
- Samenwerken met en als contactpunt optreden voor de AP.

2.1.7 De medewerkers

Alle medewerkers van de Duo gemeenten 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.

[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.

Figuur 3: Functies en rollen in informatieveiligheidsorganisatie



2.2 Overleg en afstemmingsorganen

De CISO is voorzitter van de Projectgroep Informatie Beveiliging (PIB) die minimaal viermaal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:

- De CISO.
- De coördinator ENSIA.
- De beveiligingsbeheerders.
- De privacybeheerder en/of functionaris gegevensbescherming.
- Agendaleden: MT lid of specialist.

Onderwerpen:

- Voortgang uitvoering maatregelen uit de informatieveiligheidsanalyse c.q. uit het actieplan Informatie-veiligheid.
- Beveiligingsincidenten.
- Planning en voorbereiding van controle, zelfevaluaties en audits.
- Evaluatie en actualisatie informatieveiligheidsbeleid en de informatieveiligheidsanalyse.

Daarnaast vindt indien nodig afstemming plaats tussen de CISO en de functioneel applicatie- en gegevens-beheerder(s) en de procesverantwoordelijke van (informatie)systemen.

2.3 Rapporteren beveiligingsincidenten

De CISO wordt door de medewerkers geïnformeerd over beveiligingsincidenten en legt deze vast ten be-hoeve 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.

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 viermaal per jaar aan de gemeentesecretarissen van de 3 deelnemende gemeenten alsook aan de directeur Duo+. Indien nodig treedt de procedure meldplicht datalekken in werking.

2.4 ICT crisisbeheersing (Business Continuity)

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:
- De gemeentesecretaris van de desbetreffende gemeente (voorzitter).
- De 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 de gemeentesecretaris van de desbetreffende gemeente de verantwoordelijke portefeuillehouder in.

2.5 Verantwoordelijkheden afdeling overstijgende (informatie)systemen

De afdelingsoverstijgende (informatie)systemen binnen de Duo gemeenten worden onder de verantwoordelijkheid van de bedrijfsvoeringsorganisatie Duo+ gefaciliteerd en onderhouden.

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 procesverantwoordelijke maakt schriftelijk afspraken met het gemeentelijke organisatieonderdeel, onderdeel van de bedrijfsvoeringsorganisatie Duo+ 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 informatieveiligheidsbeleid 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 het organisatieonderdeel van de gemeente 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 Duo gemeenten. Deze leidinggevende dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid 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 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.

2.6.4 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 Wet bescherming persoonsgegevens (Wbp) 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 Duo gemeenten leggen in een register vast van welke derden persoonsgegevens worden bewerkt. Ook wordt vastgelegd of een bewerkersovereenkomst nodig is in de relatie tot die andere partij. In een bewerkersovereenkomst 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. Op 25 mei 2018 treedt de algemene verordening gegevensbescherming (AVG) in werking. De FG zal een centraal punt zijn binnen de Duo gemeenten wat betreft de gegevensbescherming binnen de Duo organisatie.

3. Classificatie en beheer van informatie en bedrijfsmiddelen

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.

De Duo gemeenten houden 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 procesverantwoordelijken en beheerders zijn.

De Duo gemeenten houden 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. Dit kan een ook een medewerker buiten een van de drie gemeenten zijn, wanneer deze als lijnverantwoordelijke is aangewezen door het bevoegd bestuur.

3.3 Aanvaardbaar gebruik van bedrijfsmiddelen

Er zijn regels (o.a. op Intercomm alsook vastgelegd in CAR/UWO) 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 Duo gemeenten 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 het eigen device 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 Duo gemeenten gestelde beveiligingsvoorschriften (o.a. dit informatieveiligheidsbeleid)
    - aan de werkplek verbonden risico's;
    - het risico door het benaderen van gemeentelijke informatie met andere dan door de Duo gemeenten 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, financiele 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)*