Gemeente Hardinxveld-Giessendam

GEMEENTEBLAD

Officiële uitgave van de gemeente Hardinxveld-Giessendam

Nr. 533276

23 december 2024

Strategisch Informatiebeveiligingsbeleid Drechtsteden 2025-2029

Inleiding/Managementsamenvatting

Informatieveiligheid is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en onze dienstverlening, cyberdreigingen, digitale aanvallen, de decentralisatie van overheidstaken, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Informatieveiligheid raakt de gehele bedrijfsvoering en verdient samen met privacybescherming continu aandacht. Hoe gevoeliger/waardevoller de (persoons)gegevens zijn, hoe meer maatregelen er getroffen en in stand moeten worden gehouden om deze gegevens te beschermen tegen onrechtmatige toegang en/of misbruik en/of manipulatie.

Binnen het samenwerkingsverband Drechtsteden worden heel veel gegevens verzameld en gebruikt. Zowel vertrouwelijke als gevoelige (persoons)gegevens, waaronder Burger Service Nummers (BSN), financiële gegevens en bijzondere persoonsgegevens zoals medische- en strafrechtelijke gegevens. Deze gegevens worden binnen het samenwerkingsverband Drechtsteden gebruikt om wettelijke taken goed te kunnen uitvoeren. Denk hierbij onder andere aan taken in het sociaal domein, in het openbare orde en veiligheidsdomein of voor burgerzaken. Dit brengt zowel een wettelijke als morele verantwoordelijkheid met zich mee. Burgers, bedrijven en ketenpartners verwachten van het samenwerkingsverband Drechtsteden (bestaande uit de gemeenten Alblasserdam, Dordrecht, Hardinxveld-Giessendam, Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht en Zwijndrecht en de gemeenschappelijke regelingen, Dienst Gezondheid & Jeugd, GR Sociaal, onderdeel Sociale Dienst Drechtsteden en de omgevingsdienst Zuid-Holland Zuid) dat er zorgvuldig en veilig wordt omgegaan met deze (persoons)gegevens.

Doel van onze informatiebeveiliging

Het zorgdragen voor de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatievoorziening is essentieel om de continuïteit van onze dienstverlening aan burgers, bedrijven en samenwerkingspartners te kunnen bewerkstelligen.

Het IB-beleid 25-29 bevat de strategische beleidskaders voor informatiebeveiliging en vormt de kapstok voor (de uitwerking van) aanvullend onderliggend informatiebeveiligingsbeleid, tactische en operationele richtlijnen, processen, procedures en maatregelen. De daaruit voortkomende prioriteiten en werkzaamheden worden uitgewerkt in het jaarlijks op te stellen "Informatiebeveiligingsplan Drechtsteden 202X".

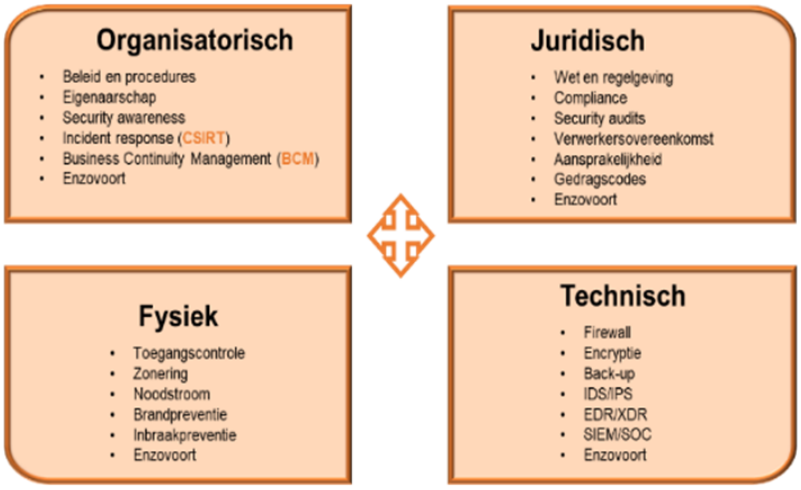
Operationele Technologie en Proces Automatisering

Binnen het samenwerkingsverband Drechtsteden wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten door middel van Proces Automatisering (PA). Dit wordt gedaan om objecten op afstand te kunnen monitoren, bewaken, beheren, aansturen en/of te bedienen. Voorbeelden van deze objecten zijn bruggen, sluizen, tunnels, verkeersmanagementsystemen zoals intelligente verkeersregelinstallaties en objecten voor stadszicht- en beheer zoals camera's en verdwijnpalen. Het IB-beleid 25-29 is ook van toepassing op de bescherming van PA[1]. Voor de bescherming van PA hanteert het samenwerkingsverband Drechtsteden de Cybersecurity Implementatie Richtlijn (CSIR)[2].

1) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf
2) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf7

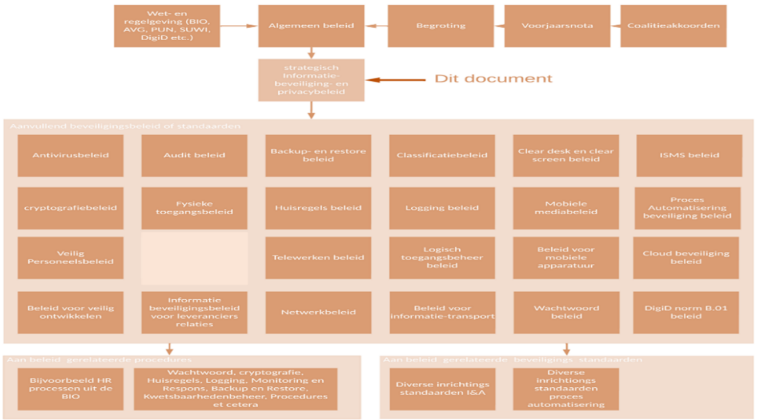
Domeinen waar informatiebeveiligingsmaatregelen worden genomen

Om zorg te kunnen dragen voor de beschikbaarheid, vertrouwelijkheid en integriteit van de informatievoorziening is het noodzakelijk om een samenhangend pakket van organisatorische-, juridische-, technische- en fysieke informatiebeveiligingsmaatregelen te treffen en te onderhouden. Informatieveiligheid reikt verder dan het implementeren van technische informatiebeveiligingsmaatregelen. Het is een groot misverstand om te denken dat informatiebeveiliging iets technisch is dat centraal geregeld kan of moet worden. Hieronder wordt schematisch weergegeven binnen welke domeinen maatregelen voor informatiebeveiliging worden getroffen en onderhouden. De beschreven maatregelen binnen deze domeinen zijn illustratief en niet limitatief.



Plaats van het Strategisch Informatiebeveiligingsbeleid Drechtsteden

Het IB-beleid 25-29 vormt de kapstok voor (de uitwerking van) aanvullend onderliggend informatiebeveiligingsbeleid, tactische en operationele richtlijnen, processen, procedures en maatregelen. Dit wordt hieronder schematisch weergegeven. De daaruit voortkomende prioriteiten en werkzaamheden worden uitgewerkt in het jaarlijks op te stellen "Informatiebeveiligingsplan Drechtsteden 202X". De inhoud en structuur van het IB-beleid 25-29 zijn gebaseerd op de Baseline Informatiebeveiliging Overheid (BIO). Ook het "Informatiebeveiligingsplan Drechtsteden 202x" zal worden gebaseerd op de BIO.



1. Het Strategisch Informatiebeveiligingsbeleid Drechtsteden

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De inhoud en structuur van het IB-beleid 25-29 zijn gebaseerd op de BIO. Het IB-beleid 25-29 bevat de strategische beleidskaders voor onze informatiebeveiliging en vormt de kapstok voor (de uitwerking van) aanvullend onderliggend informatiebeveiligingsbeleid, tactische en operationele richtlijnen, processen, procedures en maatregelen. De daaruit voortkomende prioriteiten en werkzaamheden worden uitgewerkt in het jaarlijks op te stellen "Informatiebeveiligingsplan Drechtsteden 202X".

1.1 Scope van Strategisch Informatiebeveiligingsbeleid Drechtsteden

Het IB-beleid 25-29 is van toepassing op de gehele bedrijfsvoering en geleverde dienstverlening door of vanuit het samenwerkingsverband Drechtsteden en alle uit te voeren processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen), inclusief gegevensverwerking die in de Cloud zijn of worden ondergebracht. Het beperkt zich niet alleen tot de ICT en is relevant voor het (politieke) bestuur, proceseigenaren (lijnmanagement), beheerders, externe partijen, ketenpartners, alle medewerkers, burgers, gasten, bezoekers en externe relaties en andere belanghebbende(n).

1.2 Visie op onze informatieveiligheid

Het primaire uitgangspunt voor onze informatieveiligheid is en blijft risicomanagement. Dat vereist een integrale aanpak, goed opdrachtgeverschap, onderlinge samenwerking en risicobewustzijn, waarbij ieder organisatieonderdeel is betrokken. De nadruk komt hierdoor te liggen op de governance rondom onze informatieveiligheid. Ook de BIO en de Network and Information Security directive[3] (NIS2-richtlijn) sluiten hierop aan door de verantwoordelijkheid voor informatiebeveiliging in de organisatie(s) nadrukkelijk neer te leggen bij het bestuur en de proceseigenaren. Deze verantwoordelijkheid brengt met zich mee dat de proceseigenaren de risico's op het niveau van de werkprocessen/informatiesystemen in beeld hebben met als doel het implementeren en onderhouden van passende organisatorische-, juridische-, technische- en fysieke informatiebeveiligingsmaatregelen. Overblijvende (rest)risico's worden op het juiste bestuurs- / managementniveau geaccepteerd.

Meer specifiek:

1. Relevante Europese, landelijke, sectorale wet- en regelgeving en specifieke normenkaders zijn, voor zover van toepassing op de deelnemer(s) aan het samenwerkingsverband Drechtsteden, altijd leidend. Denk bij wet- en regelgeving (niet limitatief) aan: de Baseline Informatiebeveiliging Overheid (BIO), de NEN7510, de Network and Information Security directive (NIS2-richtlijn), de Algemene Verordening Gegevensbescherming (AVG), de Wet Basisregistratie Personen (BRP), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de archiefwet, enzovoort;
2. We zijn een betrouwbare partij voor onze burgers, bedrijven en samenwerkingspartners en gaan zorgvuldig en veilig om met hun én onze gegevens. We vinden een optimum tussen investeringen in informatiebeveiligingsmaatregelen en het weerstandsvermogen, zonder de organisatie(s) te verlammen met het implementeren en borgen van maatregelen om alle risico's tot "naderend tot nul" te reduceren. Per slot van rekening, een 100% waterdichte informatiebeveiliging bestaat niet;
3. De te treffen en onderhouden organisatorische-, juridische-, technische- en fysieke informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen.

1.3. STRATEGISCHE DOELEN

De strategische doelen van het IB-beleid 25-29 zijn:

1. Het zorg dragen voor de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatievoorziening, omdat dat essentieel is voor de continuïteit van de dienstverlening van(uit) het samenwerkingsverband Drechtsteden;
2. Het beschermen van onze bedrijfsmiddelen en beheerde (persoons)gegevens tegen onrechtmatige toegang en/of misbruik en/of manipulatie;

3) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf

3. Het managen van de informatiebeveiliging(risico's), het minimaliseren van (cyber)risico's en het verhogen van de weerbaarheid daartegen;
4. Het adequaat reageren op cyberincidenten en het voorkomen of beperken van schade.

1.4. LEIDENDE PRINCIPES

De leidende principes van het IB-beleid 25-29 zijn:

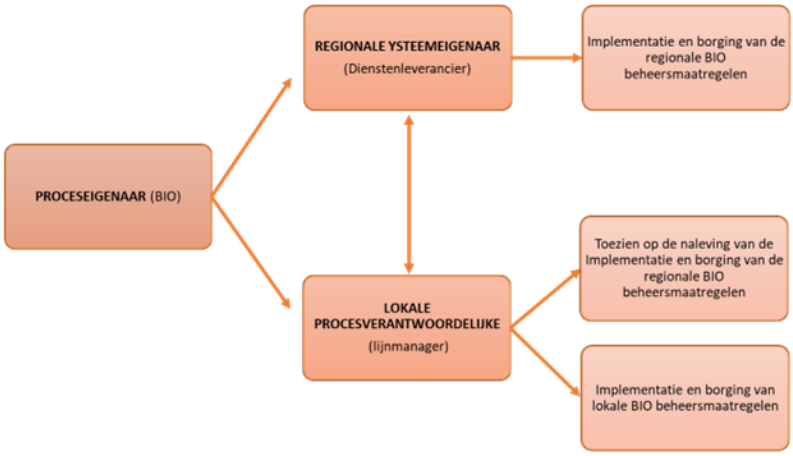
1. De implementatie van de BIO (maatregelen) vindt regionaal plaats en waar dat strikt noodzakelijk is vindt de implementatie van de BIO (maatregelen) lokaal plaats;
2. Op regionaalniveau vindt de vertaling van wet- en regelgeving op het gebied van informatiebeveiliging in beleid, normen en richtlijnen plaats. Het beleid, de normen en richtlijnen zijn voor alle deelnemers binnen het samenwerkingsverband Drechtsteden leidend;
3. Vanuit de BIO is aantoonbaarheid zeer belangrijk. De verantwoordelijkheid voor het integraal toetsen of aan de eisen is voldaan ligt vanuit de BIO altijd bij de gemeente(n);
4. Door periodieke controle, regionale brede planning en regionale coördinatie wordt de informatiebeveiliging van de informatievoorziening verankerd binnen het Drechtstedelijke samenwerkingsverband. Het IB-beleid 25-29 vormt samen met het jaarlijks op te stellen "Informatiebeveiligingsplan Drechtsteden 202X" het fundament onder het zorgdragen voor een betrouwbare informatievoorziening en informatiebeveiliging. Het plan wordt actueel gehouden op basis van het dreigingsbeeld informatiebeveiliging Nederlandse gemeenten 202X/202X, nieuwe ontwikkelingen, registraties in het incidentenregister, het risicoregister en risicoanalyses voor informatiebeveiliging en privacybescherming
5. Informatiebeveiliging is een continu verbeterproces. "Plan, do, check en act" vormen samen het managementsysteem van informatiebeveiliging. Een Information Security Management System (ISMS) is randvoorwaardelijk voor een adequate implementatie van de Baseline Informatiebeveiliging Overheid (BIO);
6. Voor gemeenten zijn de 10 bestuurlijke principes, behorende bij de Baseline Informatiebeveiliging Overheid leidend, zie hiervoor bijlage 1.

1.5. DE ROL VAN DE PROCESEIGENAAR BINNEN HET SAMENWERKINGSVERBAND DRECHTSTEDEN

Binnen de BIO is de proceseigenaar de lijnmanager die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem. In de BIO wordt de duiding van de rol van proceseigenaar beschreven vanuit het perspectief van een afzonderlijke gemeente en niet vanuit de context van een samenwerkingsverband zoals de Drechtsteden. Binnen het samenwerkingsverband Drechtsteden is een groot deel van de ICT systemen, de ICT infrastructuur evenals het beheer regionaal (dienstenleverancier) ondergebracht. Desondanks is er ook een set lokaal te implementeren BIO maatregelen aanwezig.
Op de volgende wijze geven we binnen het samenwerkingsverband Drechtsteden invulling aan de rol en verantwoordelijkheden van de proceseigenaar uit de BIO. De rol van proceseigenaar wordt onderverdeeld in een regionale systeemeigenaar (bij de dienstenleverancier) en een lokale procesverantwoordelijke (lijnmanager). Elk hebben ze hun eigen BIO aandachtsgebieden en verantwoordelijkheden:

1. De regionale systeemeigenaar is verantwoordelijk voor de implementatie en borging van de regionale BIO beheersmaatregelen;
2. De lokale procesverantwoordelijke (lijnmanager) is verantwoordelijk voor:
3. Het toezicht houden op de naleving van de implementatie en borging van de regionale BIO beheersmaatregelen;
4. De implementatie en borging van lokale BIO beheersmaatregelen.

Deze verdeling wordt hieronder schematisch weergegeven.



2. BELEIDSUITGANGSPUNTEN

Bij het treffen en onderhouden van maatregelen voor de borging van de informatieveiligheid gelden de volgende beleidsuitgangspunten waaraan (vooraf) wordt getoetst:

1. Relevante Europese, landelijke, sectorale wet- en regelgeving en specifieke normenkaders zijn, voor zover van toepassing op de deelnemer(s) aan het samenwerkingsverband Drechtsteden, altijd leidend. Denk bij wet- en regelgeving (niet limitatief) aan: de Baseline Informatiebeveiliging Overheid (BIO), de NEN7510, de Network and Information Security directive (NIS2-richtlijn), de Algemene Verordening Gegevensbescherming (AVG), de Wet Basisregistratie Personen (BRP), de Wet Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI), de archiefwet, enzovoort;
2. De Baseline Informatiebeveiliging Overheid (BIO) is het verplichte normenkader voor informatiebeveiliging. De te treffen en onderhouden informatiebeveiligingsmaatregelen worden hieraan (vooraf) getoetst. De kennisproducten van de informatiebeveiligingsdienst (IBD) worden bij de onderliggende uitwerkingen gehanteerd;
3. De te treffen en onderhouden informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen. Deze afweging(en) worden schriftelijk vastgelegd. Het uitvoeren van een dataclassificatie is altijd verplicht en vanaf het basisbeveiligingsniveau 2 (BBN2) wordt ook een risicoanalyse verplicht uitgevoerd. Daar waar het wettelijk verplicht is wordt ook een Data Protection Impact Assessment[4] (DPIA) uitgevoerd;
4. Eventuele (rest-)risico's, welke niet afgedekt (kunnen) worden met maatregelen of niet proportioneel zijn, worden door de Chief Information Security Officer voorzien van een advies en ter acceptatie voorgelegd aan het managementniveau dat past bij het risico;
5. Toegang vanuit een onvertrouwde zone naar een vertrouwde zone geschiedt altijd en alleen op basis van een zero trust[5] en multi-factor[6] authenticatie;
6. Er is ruimte voor afwijkingen en prioriteringen op basis van het "pas toe of leg uit" principe. Deze afwegingen worden door de proceseigenaar (lijnmanagement) schriftelijk vastgelegd, door de Chief Information Security Officer voorzien van een advies en vooraf ter goedkeuring en ter acceptatie voorgelegd aan het managementniveau dat past bij het risico;
7. Indien van toepassing wordt het IB-beleid 25-29 verder uitgewerkt c.q. verbijzonderd in onderliggend(e) tactisch beleid, informatiebeveiligingsplannen, richtlijnen, procedures, enzovoort. Deze

4) Een DPIA is een instrument om vooraf de privacy risico's van een gegevensverwerking in kaart te brengen en vervolgens maatregelen te kunnen nemen om de risico's te verkleinen.
5) Zero trust gaat uit van het principe never trust, always verify. Dit bestaat uit een sterke controle van de identiteit. Verifieer en autoriseer altijd op basis van alle beschikbare gegevenspunten, inclusief gebruikersidentiteit, locatie, apparaat status, service of workload, gegevens-classificatie en afwijkingen.
6) Een gebruikersaccount kent een gebruikersnaam en een wachtwoord, dit noemen we vaak: "iets wat je weet". Multi-factor authenticatie voegt daar een extra dimensie aan toe: "iets dat je weet" (je wachtwoord) en "iets dat je hebt" bijvoorbeeld een fysieke/soft token, key generator of vingerafdruk. In het eerste geval heeft men het dan over verschillende soorten tokens: USB-token, een key-/nummergenerator, een sms-code. In het tweede geval heeft men het dan over de biometrische kenmerken van een persoon, de meest gangbare zijn: een vingerafdruk, een irisscan of je stem.

uitwerkingen worden getoetst aan en gebaseerd op de beschikbare de kennisproducten van de informatiebeveiligingsdienst (IBD);
8. Daar waar wetgeving, regelgeving en/of specifieke normenkaders eisen stellen aan taken en verantwoordelijkheden van medewerkers inzake informatieveiligheid en het functiewaarderingsysteem daarin niet voorziet dan worden deze opgenomen in aanvullende individuele afspraken op functieniveau tussen de leidinggevende en de medewerker;
9. Iedere medewerker, zowel vast als tijdelijk, intern of extern, ketenpartner of betrokkene, is verplicht waar nodig gegevens, applicaties, devices en de infrastructuur te beschermen tegen ongeautoriseerde toegang (naleven informatiebeveiligingsbeleid), gebruik, verandering (manipulatie), openbaring, vernietiging, verlies of ongeautoriseerde overdracht. Bij (vermeende) inbreuken hierop dienen medewerkers dit direct na constatering zowel te melden aan het serviceloket en aan de proceseigenaar (lijnmanager);
10. We gaan uit van de eigen verantwoordelijkheid van medewerkers zowel vast als tijdelijk, intern of extern zoals vastgelegd in het personeelshandboek;
11. De gemeentesecretaris/algemeen directeur, de Chief Information Security Officer (CISO), de (regionale en lokale) Information Security Officer (ISO), en proceseigenaar[7] (lijnmanager) bevorderen de naleving van het IB-beleid 25-29, de algehele communicatie en bewustwording (awareness) rondom informatieveiligheid.

3. VERPLICHT UIT TE VOEREN STAPPEN

De te treffen en onderhouden informatiebeveiligingsmaatregelen zijn altijd op een risicoafweging gebaseerd en worden proportioneel getroffen. Om de informatiebeveiligingsrisico's in beeld te brengen en daarmee te komen om een tot een zorgvuldige afweging dienen de hieronder vermelde stappen altijd te worden uitgevoerd. Op basis van deze stappen wordt bepaald wat de te treffen en onderhouden informatiebeveiligingsmaatregelen zijn en wat de afwegingen daarbij zijn geweest. Dit wordt schriftelijke vastgelegd.

3.1. HET UITVOEREN VAN EEN DATACLASSIFICATIE EN HET BEPALEN VAN HET BBN

Het uitvoeren van een dataclassificatie is altijd verplicht. Het toekennen van classificatieniveaus aan data en/of informatiesystemen is van groot belang, omdat daarmee het (vereiste) beschermingsniveau wordt geïdentificeerd. Het vormt de basis voor het bepalen van het basisbeveiligingsniveau (BBN) dat van toepassing is. Het beschermingsniveau van gegevens (data) en/of informatiesystemen wordt uitgedrukt in classificatieniveaus voor beschikbaarheid, integriteit en vertrouwelijkheid. Mede aan de hand hiervan kan worden bepaald welke beveiligingseisen gelden en welke maatregelen moeten worden genomen. De eerste stap bij een dataclassificatie is nagaan welke wetgeving, regelgeving en/of specifieke normenkaders mogelijk eisen stellen aan gebruik, distributie en opslag van data. Daarnaast is het van belang om de verantwoordelijkheden t.a.v. de gegevens (data) en/of informatiesystemen goed in beeld te hebben. Bij het uitvoeren van een dataclassificatie wordt de handreiking dataclassificatie van de informatiebeveiligingsdienst (IBD) geraadpleegd en als leidraad gehanteerd. Nadat de data is geclassificeerd wordt het bijbehorende basisbeveiligingsniveau (BBN) bepaald.

3.2. VANAF BBN 2 IS HET UITVOEREN VAN EEN RISICOANALYSE VERPLICHT

De aanpak van onze informatieveiligheid is risico gebaseerd. Dat wil zeggen dat beveiligingsmaatregelen worden getroffen en onderhouden op basis van de resultaten uit de dataclassificatie en het bepalen van het bijbehorende basisbeveiligingsniveau. Vanaf het basisbeveiligingsniveau 2 (BBN2) dient een aanvullende risicoanalyse te worden uitgevoerd.

3.3. HET UITVOEREN VAN EEN DATA PROTECTION IMPACT ASSESSMENT KAN VERPLICHT ZIJN

Een Data Protection Impact Assessment (DPIA) is een instrument om vooraf de privacy risico's rondom de verwerking van persoonsgegevens in kaart te brengen en om op basis van de geïdentificeerde risico's de te treffen maatregelen te bepalen om deze risico's af te dekken/mitigeren. Het uitvoeren van een Data Protection Impact Assessment (DPIA) kan in sommige situaties bij wet[8] verplicht zijn.

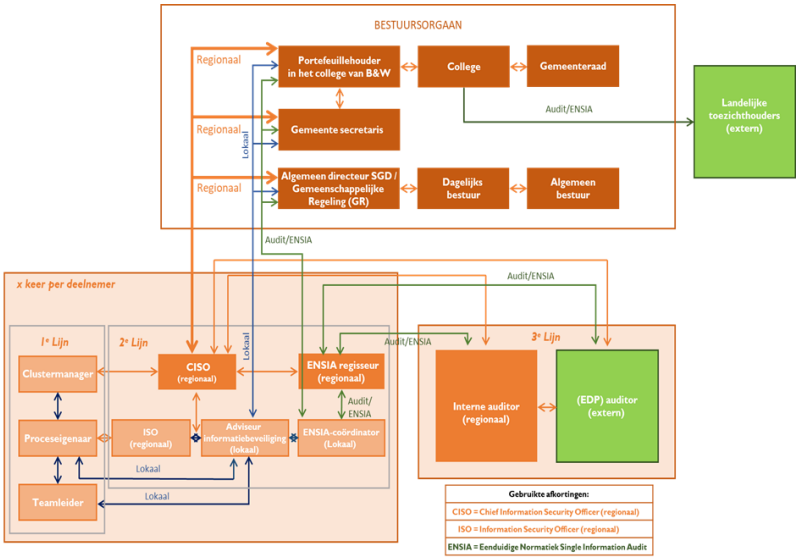
7) Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem.
8) Artikel 35 van de Algemene Verordening Gegevensbescherming (AVG)

4. ORGANISATIE, TAKEN & VERANTWOORDELIJKHEDEN

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot de informatiebeveiliging op welke plaats belegd zijn binnen het samenwerkingsverband Drechtsteden.

4.1. INRICHTING IB ORGANISATIE DRECHTSTEDEN CONFORM HET THREE LINES MODEL

De indeling van de informatiebeveiligingsorganisatie binnen het samenwerkingsverband Drechtsteden sluit aan op de uitwerking van het "Three Lines Model"[9] (eerder bekend als "Three Lines of Defense"). In dit model is het bestuursorgaan eindverantwoordelijk voor de integrale informatiebeveiliging, de inrichting en werking van de informatiebeveiligingsorganisatie en voor de implementatie van alle informatiebeveiligingskaders in de organisatie, dus ook voor een juiste toepassing van de BIO. De eerste lijn, het lijnmanagement (proceseigenaar), is verantwoordelijk voor het zorg dragen voor de informatiebeveiliging en privacybescherming binnen de eigen processen. De tweede lijn (CISO, regionale ISO, lokale adviseur informatiebeveiliging, regionale ENSIA regisseur en de lokale ENSIA coördinator) ondersteunt, adviseert, coördineert en bewaakt of het lijnmanagement (proceseigenaar) zijn/haar verantwoordelijkheden ook daadwerkelijk neemt. De derde lijn bestaat uit een interne auditor en een (externe) register EDP-auditor. De derde lijn geeft onafhankelijke en objectieve adviezen (interne auditor) en Assurance (register EDP-auditor) over de toereikendheid en effectiviteit van de informatiebeveiliging en het bijbehorende risicomanagement. De indeling van de informatiebeveiligingsorganisatie binnen het samenwerkingsverband Drechtsteden wordt hieronder schematisch weergegeven.



Schematische weergave IB organisatie Drechtsteden

5. ENSIA

Een gemeente verantwoordt zich jaarlijks over haar informatieveiligheid middels de ENSIA-systematiek[10]. De verantwoording over de informatieveiligheid komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging. Met deze verklaring geeft het college van Burgemeester en Wethouders aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-verantwoording (over de naleving van de BIO). Ook worden de eventuele verbetermaatregelen vermeld die de gemeente gaat treffen. De ingevulde zelfevaluatievragenlijst vormt de basis voor het opstellen van de collegever-

9) Toelichting op het Three Lines Model

10) Gemeenten verantwoorden zich over informatiebeveiliging en kwaliteit middels ENSIA. Dat staat voor Eenduidige Normatiek Single Information Audit. De focus van ENSIA ligt op verantwoording richting de gemeenteraad, het hoogste politieke orgaan van de gemeente. Parallel hieraan leggen gemeenten verantwoording af aan de rijksoverheid waar het gaat om het gebruik van landelijke voorzieningen.

klaring aan de raad. Via ENSIA verantwoordt de gemeente zich ook aan de stelselhouders voor DigiD/Suwinet etc.
Dat betekent dat jaarlijks door de gemeentesecretaris een gemeentelijke (lokale) ENSIA-coördinator wordt aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke proceseigenaren (lijnmanager). De proces-eigenaren (lijnmanagers) leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten tijdig aan. Binnen het samenwerkingsverband Drechtsteden wordt het proces regionaal gecoördineerd door een ENSIA regisseur.

BIJLAGE 1
De 10 bestuurlijke principes voor informatiebeveiliging, behorende bij de Baseline Informatiebeveiliging Overheid (BIO) (https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/01/De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf)