Strategisch Informatiebeveiligingsbeleid Drechtsteden 2025 - 2029

Drechtsteden

INFORMATIEVEILIGHEIDSBEWUSTZIJN IS DE BELANGRIJKSTE BEVEILIGINGSMAATREGEL

COLOFON

NAAM DOCUMENT

Strategisch Informatiebeveiligingsbeleid Drechtsteden 2025-2029. Dit wordt verder in het document afgekort tot het IB-beleid 25–29.

AUTEUR

Richard Gillesen, Strategisch Beleidsadviseur Informatiebeveiliging

VERSIE

Strategisch IB Beleid Drechtsteden d.d. 1-11-2024 definitieve versie voor instemming in het SAB

VERSIEBEHEER

Het beheer van dit document berust bij de Chief Information Security Officer (CISO) en de Strategisch Beleidsadviseur Informatiebeveiliging (SBI) en dient jaarlijks te worden geëvalueerd.

DOEL EN SCOPE STRATEGISCH INFORMATIEBEVEILIGINGSBELEID DRECHTSTEDEN

Met de afzonderlijke vaststelling van dit Strategisch Informatiebeveiligingsbeleid Drechtsteden stelt het samenwerkingsverband van in totaal 7 gemeenten (Alblasserdam, Dordrecht, Hardinxveld-Giessendam, Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht en Zwijndrecht) en 3 gemeenschappelijke regelingen (Dienst Gezondheid & Jeugd, GR Sociaal, onderdeel Sociale Dienst Drechtsteden en de omgevingsdienst Zuid-Holland Zuid) een richtinggevend strategisch informatiebeveiligingskader vast voor de informatiebeveiliging binnen het samenwerkingsverband Drechtsteden en daar waar dat past tevens voor de eigen organisatie[1].

Het Strategisch Informatiebeveiligingsbeleid Drechtsteden is van toepassing op de 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.

DOELGROEP

Het Strategisch Informatiebeveiligingsbeleid Drechtsteden is openbaar en is beschikbaar voor het (politieke) bestuur, proceseigenaren (lijnmanagement), beheerders, externe partijen, ketenpartners, alle medewerkers, burgers, gasten, bezoekers en externe relaties en andere belanghebbende(n).

VASTSTELLING EN INWERKINGTREDING

Het Strategisch Informatiebeveiligingsbeleid Drechtsteden 2025 -2029 treedt in werking na vaststelling door de afzonderlijke colleges van Burgemeester en Wethouders van het samenwerkingsverband Drechtsteden dat bestaat uit de gemeenten, Alblasserdam, Dordrecht, Hardinxveld-Giessendam, Hendrik-Ido-Ambacht, Papendrecht, Sliedrecht, Zwijndrecht en het afzonderlijke dagelijks bestuur van de gemeenschappelijke regelingen, Dienst Gezondheid & Jeugd, GR Sociaal, onderdeel Sociale Dienst

[1] • GR Sociaal wil het IB Beleid tenminste één, maar mogelijk twee jaar hanteren. Dat geeft hen te tijd om een eigen IB Beleid te ontwikkelen.
• DG&J hanteert een eigen IB Beleid; het onderhavige IB Beleid wordt door DG&J als aansluitvoorwaarde gezien voor wat betreft de dienstverlening door Dordrecht (SGD). Immers, DG&J heeft met meer leveranciers en wet- en regelgeving te maken.
• OZHZ heroriënteert zich momenteel op het domein Informatiebeveiliging, waarop het eveneens met andere Omgevingsdiensten in de nabijheid samenwerkt. Ook hier heeft het IB Beleid de waarde van aansluitvoorwaarde.

Drechtsteden en de omgevingsdienst Zuid-Holland Zuid. Met de afzonderlijke vaststelling van het Strategisch Informatiebeveiligingsbeleid Drechtsteden 2025 -2029 komt het voorgaande Strategisch Informatiebeveiligingsbeleid Drechtsteden 2020-2024 te vervallen.

Inhoudsopgave

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”.

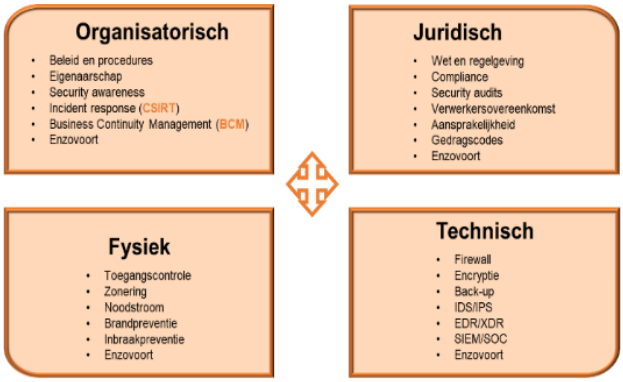
OPERATIONELE TECHNOLOGIE EN PROCES AUTOMATISERING

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[2]. Voor de bescherming van PA hanteert het samenwerkingsverband Drechtsteden de Cybersecurity Implementatie Richtlijn (CSIR)[3].

[2] https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf
[3] https://www.cert-wm.nl/csir

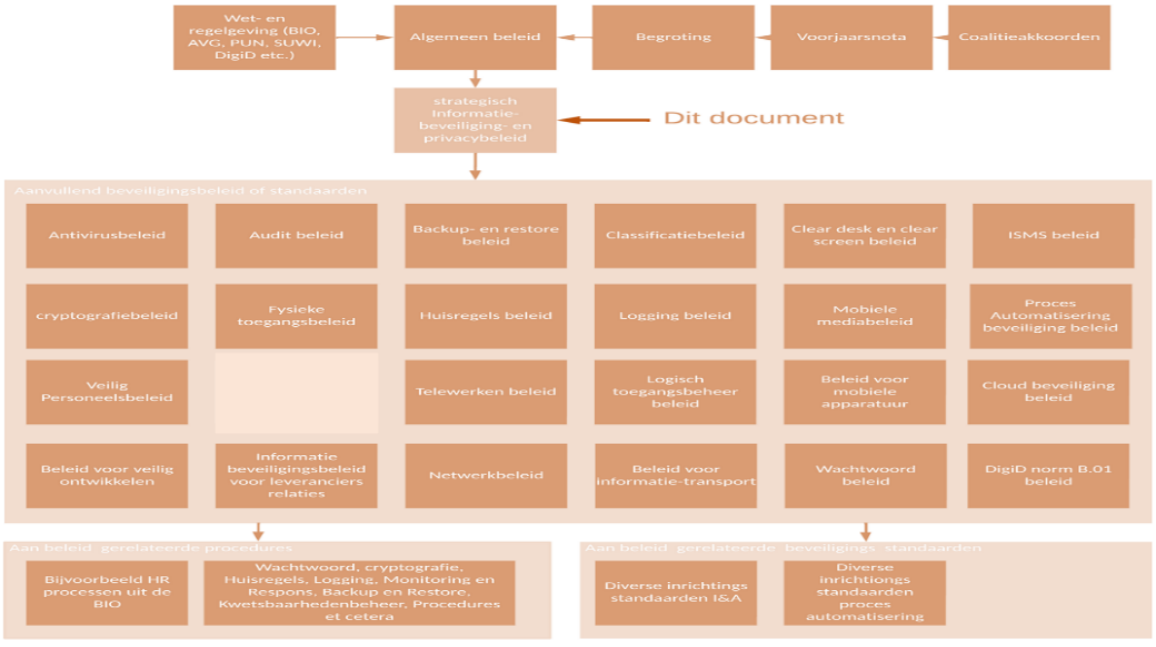
DOMEINEN WAAR INFORMATIEBEVEILIGINGSMAATREGELEN WORDEN GENOMEN

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[4] (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.

[4] NIS2-richtlijn - Digitale Overheid

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. 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.

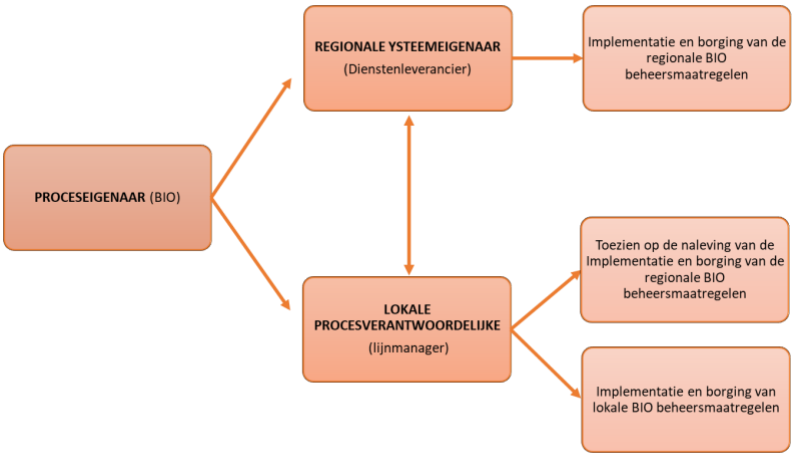
1.5. DE ROL VAN DE PROCESEIGENAAR BINNEN HET SAMENWERKINGSVERBAND DRECHTSTEDEN

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:
    a. Het toezicht houden op de naleving van de implementatie en borging van de regionale BIO beheersmaatregelen;
    b. 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[5] (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[6] en multi-factor[7] 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 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

[5] 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

[6] 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, gegevensclassificatie en afwijkingen.

[7] 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.

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[8] (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

[8] Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem.

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 [9] verplicht zijn.

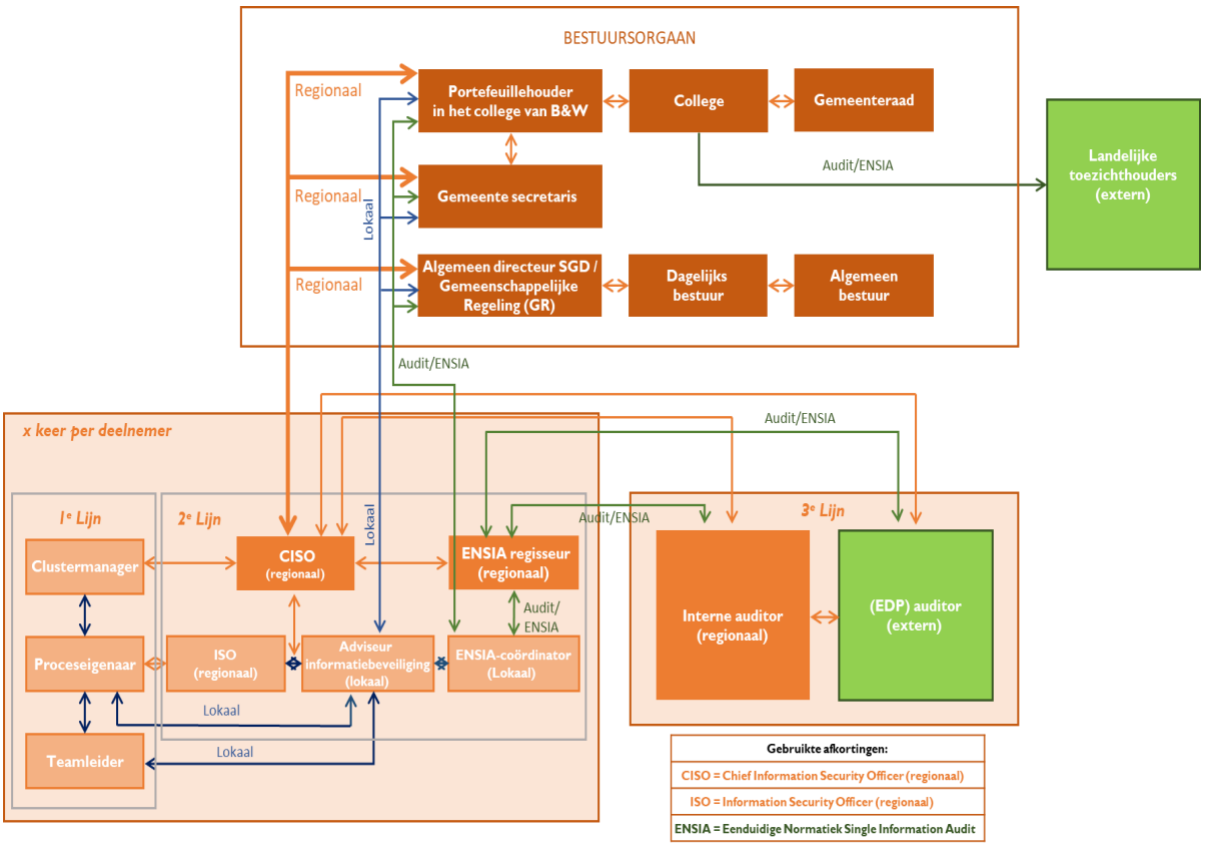
[9] Artikel 35 van de Algemene Verordening Gegevensbescherming (AVG)

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 [10]" (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

[10] Toelichting op het Three Lines Model

5. ENSIA

Een gemeente verantwoordt zich jaarlijks over haar informatieveiligheid middels de ENSIA-systematiek [11]. 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 collegeverklaring 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 proceseigenaren (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.

[11] 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.

6. BIJLAGE: DE 10 BESTUURLIJKE PRINCIPES, BEHORENDE BIJ DE BIO

De 10 bestuurlijke principes voor informatiebeveiliging

Behorende bij de Baseline Informatiebeveiliging Overheid (BIO)

COLOFON

COPYRIGHT

MET DANK AAN

De expertgroep, de reviewgemeenten en de Informatiebeveiligingsdienst voor Gemeenten die hebben bijgedragen aan het vervaardigen van dit product.

Versiebeheer

Het beheer van dit document berust bij de Vereniging van Nederlandse Gemeenten (VNG).

Opmaak

Chris Koning (VNG)

INFORMATIEBEVEILIGING EN DE GEMEENTELIJKE BESTUURDER

Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren. Binnen de eigen organisatie, maar ook daarbuiten: met inwoners, ondernemers, ketenpartners en medeoverheden. Door informatie te delen kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van inwoners verbeteren en meer mensen aan het werk krijgen. Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie adequaat organiseren. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid[1] hebben om de gegevens van hun inwoners onder alle omstandigheden te beschermen. De risico's rondom de vertrouwelijkheid, integriteit en beschikbaarheid van informatie(systemen) maken dat het onderwerp informatiebeveiliging niet mag ontbreken op de bestuurstafel.

MENS, PROCES EN TECHNIEK

Informatieveiligheid is veel meer dan ICT, het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met risico's omgaat. Is de medewerker zich bewust van die risico's? Zijn bestuurders zich bewust van de risico's van en voor de organisatie? Gemeentelijke bestuurders zijn verantwoordelijk voor de informatiebeveiliging binnen gemeentelijke organisatie. Beveiliging van gegevens en systemen is een zaak van organisatie, procedures, werkprocessen en in de laatste plaats techniek. Het gaat om de mens, de manier waarop deze werkt en het gereedschap waarmee het werk verricht wordt.

RISICOMANAGEMENT IS DE BASIS

De bestuurder is verantwoordelijk voor een veilige informatievoorziening. Het is daarom aan de bestuurder om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de bestuurder acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming. Risicomanagement staat daarmee aan de basis van informatiebeveiliging. Er dient een continu proces van identificatie en beoordeling van risico's plaats te vinden om te bepalen wat nodig is om informatie adequaat te beschermen. Hierbij moet worden opgemerkt dat het risico *nul* niet bestaat en dat het aan het bestuur is om te bepalen hoeveel of welk risico acceptabel is. En de risico's zijn talrijk: privacyschendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen, fysieke schade door storingen in systemen in de openbare ruimte.

NORMEN EN REGELS

De ontwikkelingen in de informatietechnologie gaan steeds sneller en de wetgeving rondom de bescherming van persoonsgegevens is aangescherpt. De internationale norm om informatie(systemen) adequaat te beveiligen is vastgelegd in de ISO27001/2. Voor de Nederlandse overheid is deze norm vertaald naar een zogenaamde *Baseline Informatiebeveiliging Overheid* (BIO) met daarin de regels waaraan alle overheidslagen dienen te voldoen. Door middel van een zelfevaluatie (ENSIA) verantwoorden gemeenten zich over deze norm.

BESTUURLIJKE AANVULLING OP DE NORMEN EN REGELS

In aanvulling op de baseline bevat dit document de bijbehorende principes voor bestuurders. Daarmee gaat dit document over waarden die u zichzelf als bestuurder oplegt. Deze waarden dienen verbonden te zijn aan de waarden van uw organisatie. Dit document is de bestuurlijke aanvulling op de baseline en helpt u om de juiste dingen te doen. De principes gaan daarom vooral over u en uw rol bij het borgen van informatiebeveiliging in uw organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement.

1 O.a. de Algemene wet gegevensbescherming, Wet BRP, PUN, DigiD, BAG, BGT en SUWI

DE 10 PRINCIPES VOOR INFORMATIEBEVEILIGING

Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1 BESTUURDERS BEVORDEREN EEN VEILIGE CULTUUR

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

Ik ben mij bewust van de voorbeeldfunctie van een bestuurder en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als bestuurder. Ik spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.

Toelichting

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

2 INFORMATIEBEVEILIGING IS VAN IEDEREEN

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

Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt als vanzelfsprekend en nuttig. Ik ben transparant naar de raad en zorg ervoor dat hij ook zijn rol kan pakken op dit onderwerp.

Toelichting

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

3 INFORMATIEBEVEILIGING IS RISICOMANAGEMENT

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

Ik zorg dat risicomanagement een onderdeel is van het bestuurlijk overleg en dialoog. Daarnaast zal ik het integreren in het risicobewustzijn van alle medewerkers en het onderdeel laten zijn van de samenwerking met partners en ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting

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

4 RISICOMANAGEMENT IS ONDERDEEL VAN DE BESLUITVORMING

Risicomanagement is onderdeel van alle besluiten en risicomanagement is chefsache.

Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen de medewerkers kunnen opereren.

Toelichting

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

5 INFORMATIEBEVEILIGING BEHOEFT OOK AANDACHT IN (KETEN)SAMENWERKING

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

Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van de gemeente en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld en dat de juiste maatregelen getroffen worden.

Toelichting

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

6 INFORMATIEBEVEILIGING IS EEN PROCES

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

Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.

Toelichting

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

7 INFORMATIEBEVEILIGING KOST GELD

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

Ik zorg ervoor dat er voldoende middelen beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatiedoelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn om deze maatregelen uit te voeren.

Toelichting

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

8 ONZEKERHEID DIENT TE WORDEN INGECALCULEERD

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

Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen. Ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan risicomanagement.

Toelichting

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

9 VERBETERING KOMT VOORT UIT LEREN EN ERVARING

Risicobeheer wordt voortdurend verbeterd door leren en ervaring.

Door mijn inzet zorg ik ervoor dat risicogestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.

Toelichting

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

10 HET BESTUUR CONTROLEERT EN EVALUEERT

Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.

Ik geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles de manier om te weten te komen of en hoe het beleid in de praktijk uitwerkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.

Toelichting

Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op bestuursniveau genomen worden, wanneer de situatie daar om vraagt.

Vereniging van Nederlandse Gemeenten

Nassaulaan 12
2514JS Den Haag
+31 70 373 8393
info@vng.nl

januari 2019

vng.nl