GEMEENTE ETTEN-LEUR

GEMEENTEBLAD

Officiële uitgave van de gemeente Etten-Leur

Nr. 505889

3 december 2024

Strategisch informatiebeveiligings- en privacybeleid 2024 t/m 2027

1. Inleiding

In 2018 werden zowel een strategisch informatiebeveilgingsbeleid als een strategisch privacybeleid vastgesteld. Deze stukken zijn inmiddels verouderd en aan vervanging toe.

Dit beleid beschrijft het strategisch informatiebeveiligings- en privacy beleid (IB&P beleid) voor de jaren 2024 - 2027 en vervangt alle voorgaande versies. Het beleid wordt minimaal iedere 3 jaar geheel herzien, maar wanneer nodig eerder aangepast.

Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerpspecifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau. De basis voor dit strategisch beleid zijn de Baseline Informatiebeveiliging Overheid (BIO)[1] en het model VNG Borgingsproduct AVG[2] &[3].

De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 bestuurlijke principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens.

1.1. Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen gemeentelijk Informatiebeveiligings- en privacyplan (vastgesteld door het managementteam) worden deze tactische en operationele aspecten van informatiebeveiliging en privacy verder uitgewerkt en geconcretiseerd.

Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2. Informatiebeveiliging

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van (persoons)gegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en heeft betrekking op verschillende groepen personen (bijvoorbeeld: het politieke bestuur, alle medewerkers, burgers, bezoekers en externe relaties).

1.3. Privacy & Gegevensbescherming (AVG)

De gemeente werkt met (persoons)gegevens van onder meer inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken.

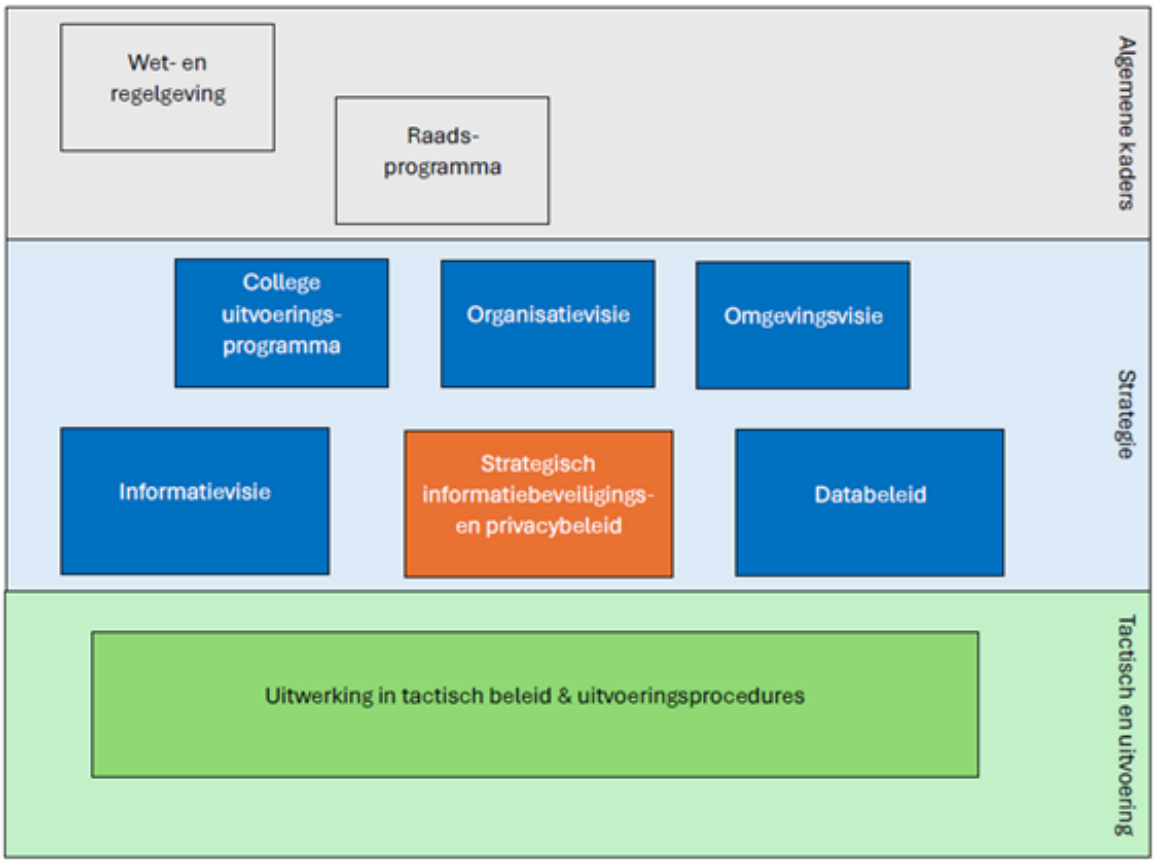
Bij de omgang met deze persoonsgegevens hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. Inwoners en andere betrokkenen moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

1) Baseline informatiebeveiliging overheid 1.04
2) VNG Borgingsprodukt AVG versie 2.0
3) VNG Borgingsprodukt AVG versie 3.0

1.4. Positie van dit beleid

Dit beleid beschrijft op strategisch niveau het informatiebeveiligings- en privacy beleid. Dit is uitgewerkt binnen diverse algemene kaders en andere (strategische) beleidsstukken c.q. uitgangspunten.

Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsdocumenten en dient daarmee als "kapstok" voor de verdere invulling en uitwerking van beleid op tactisch niveau voor informatiebeveiliging en privacy en implementatie op operationeel niveau.



2. Strategisch beleid

2.1. Doel

Doel van deze beleidsnota is het vastleggen van een solide basis voor informatiebeveiliging- en privacy binnen onze organisatie. Hiermee voorkomen we bijvoorbeeld datalekken, hacken, datagijzeling en andere beveiligingsincidenten en minimaliseren we de impact ervan indien zich een beveiligingsincident voordoet.

Dit beleid is het strategisch kader om de beschikbaarheid, integriteit en vertrouwelijkheid van de (persoons)gegevens en andere informatie(systemen) te waarborgen. Ten aanzien van verwerking van persoonsgegevens geldt specifiek nog dat deze moeten voldoen aan de beginselen uit de Algemene Verordening Gegevensbescherming (AVG).

De 6 AVG-beginselen zijn:
1. rechtmatigheid, behoorlijkheid en transparantie;
2. doelbinding;
3. dataminimalisatie;
4. juistheid;
5. opslagbeperking;
6. vertrouwelijkheid en integriteit.

Door te werken binnen dit strategisch kader kan de gemeente voldoen aan relevante wet- en regelgeving.

Dit beleid is de basis voor het tactische beleid en de operationele procedures om daarmee richting te geven voor de verdere invulling van informatiebeveiliging en privacy.

Dit vertaald zich in de volgende strategische doelen:
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het toepassen van dataminimalisatie.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

2.2. Scope informatiebeveiliging en privacy
De scope van deze beleidsnota omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens bij de gemeente, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Dit beleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals de AVG[4], UAVG[5], Wpg[6], BRP[7], PUN[8], DigiD[9] en diverse sectorale wetgeving. Voor bepaalde kerntaken gelden op grond van deze wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI en gemeentelijke basisregistraties) en DigiD met norm B.01 eisen. Deze worden in aanvullende beleidsdocumenten geformuleerd.

Alle informatie en informatiesystemen zijn van belang voor de gemeente, bepaalde informatie is van vitaal en kritiek belang. Het college van B en W is eindverantwoordelijke voor de informatiebeveiliging en privacy. Dit geldt voor alle gemeentelijke informatiesystemen en processen ongeacht waar deze worden gehost c.q. zijn belegd.

Alle Proces Automatiseringssystemen (PA) die binnen de gemeentelijke gebouwen en in de publieke ruimte van de gemeente worden gebruikt, die van de gemeente zijn, zoals gebouwbeheersingssystemen en bijvoorbeeld camera technologie of pompen en gemalen.

2.3. Ontwikkelingen
De ontwikkelingen genoemd zijn van belang voor de actualisering van het informatiebeveiligings- en privacybeleid. Nieuwe ontwikkelingen kunnen er uiteraard toe leiden dat dit beleid tussentijds geactualiseerd wordt. Dit wordt jaarlijks bekeken.

2.3.1. De BIO
De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat het managementteam (MT), de afzonderlijke MT-leden en teamleiders nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001. Daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.3.2. De AVG
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler werkende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Etten-Leur is zich hiervan bewust en wil daarom met dit beleid aangeven hoe zij in algemene zin invulling geeft aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de AVG.

4) Algemene verordening gegevensbescherming
5) Uitvoeringswet Algemene verordening gegevensbescherming
6) Wet Politiegegevens
7) Basisregistratie personen
8) Paspoortuitvoeringsregeling Nederland
9) Digitale Identiteit

2.3.3. De WPG

De gemeente heeft BOA's in dienst en zij verwerken gegevens die niet onder de AVG vallen maar onder de wet Politiegegevens (WPG). Hiervoor moet de gemeente beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht

2.3.4. De 10 principes voor informatiebeveiliging en privacy

De 10 principes voor informatiebeveiliging[10] zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. Deze principes zijn één-op-één toepasbaar op het thema Privacy.

Zij zijn als volgt:

1. Bestuurders bevorderen een veilige cultuur.
2. Informatiebeveiliging / Privacy is van iedereen.
3. Informatiebeveiliging / Privacy is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging / Privacy behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging / Privacy is een proces.
7. Informatiebeveiliging / Privacy kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging en privacy in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de persoonsgegevens en andere informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee zijn de onderwerpen informatiebeveiliging en privacy nadrukkelijk gewenst op de bestuurstafel.

2.3.5. Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.3.6. Informatie uit incidenten, inbreuken op de beveiliging en datalekken

De gemeente kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.4. Gebruikte standaarden voor informatiebeveiliging en privacy

2.4.1. Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2012. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2012 genomen. Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[11] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen.

Naar verwachting zal in 2024 of 2025 een vernieuwde versie van de BIO geïmplementeerd worden. Deze wordt aangepast naar de actuelere normen NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. Daarnaast zal hierin ook de EU-richtlijn "Netwerk- en Informatiesystemen 2" (NIS2) in worden door vertaalt.

De inhoud en structuur van deze beleidsnota zijn afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacyplan zal deze structuur volgen.

10) https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

11) *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*

Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Het beveiligingsbeleid van de gemeente is ook voor de bescherming van PA en dit beleid betreft dan ook afdelingen die zich met PA bezig houden.[12] Voor de bescherming van PA gebruikt de gemeente de Cybersecurity Implementatie Richtlijn (CSIR).[13]

2.4.2. Standaarden privacy

De basis voor de inrichting van het privacybeleid is het Borgingsproduct AVG (versies 2.0. en 3.0) van de Vereniging van Nederlandse Gemeenten (VNG). De kaders in dit borgingsproduct zijn op hun beurt gebaseerd op NEN-ISO/IEC 27701:2019.

NEN-ISO/IEC 27701 specificeert eisen en geeft richtlijnen voor het inrichten, implementeren, onderhouden en continu verbeteren van een managementsysteem voor privacy-informatie ('Privacy Information Management System', PIMS) in de vorm van een uitbreiding op ISO/IEC 27001 en ISO/IEC 27002 voor privacymanagement binnen de context van de organisatie.

Deze normen zijn ontwikkeld binnen de geldende wet- en regelgeving, zoals de AVG.

2.5. Ambitie en visie van de gemeente Etten-Leur op het gebied van informatiebeveiliging en privacy

Om de continuïteit in de dienstverlening en bedrijfsvoering te borgen is een solide inrichting van informatiebeveiliging nodig. Het college en het managementteam maken hierbij op basis van risicomanagement bewuste keuzes om informatieveiligheid te borgen en om kwetsbaarheden in de bedrijfsvoering te minimaliseren. Risico op dataverlies en -manipulatie van gegevens van inwoners en bedrijven worden hiermee verkleind. Veiligheids- en imagorisico's voor de organisatie - zoals afpersing, diefstal van persoon- en bedrijfsgegevens, uitval van ICT-diensten- worden hiermee verkleind.

Uiteraard moeten alle organisaties daarnaast te voldoen aan privacy wet- en regelgeving, zoals het onderhouden van een verwerkingsregister, het naleven van de meldplicht voor datalekken en het aanstellen van een Functionaris voor Gegevensbescherming (FG), etc. Niettemin wordt de mate van naleving van de AVG door organisaties ook bepaald door hun ambities op dit gebied.

Een degelijke inrichting van informatiebeveiliging en privacy aan de voorkant voorkomt herstelwerkzaamheden achteraf. Om deze inrichting te bereiken, is het noodzakelijk om op het gebied van de bescherming van onze (persoons)gegevens te professionaliseren.

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

13) https://www.cert-wm.nl/csir

Het huidige volwassenheidsniveau van informatiebeveiliging en privacy[14] van Etten-Leur ligt momenteel op niveau 2 en op enkele gebieden op niveau 3. Dit blijkt uit eerder uitgevoerde ENSIA- en DigiD-audits en diverse DPIA's.

De ambitie is om volwassenheidsniveau 4 in 2027 in stappen te bereiken. De wijze waarop zal nader worden uitgewerkt in uitvoeringsplannen.

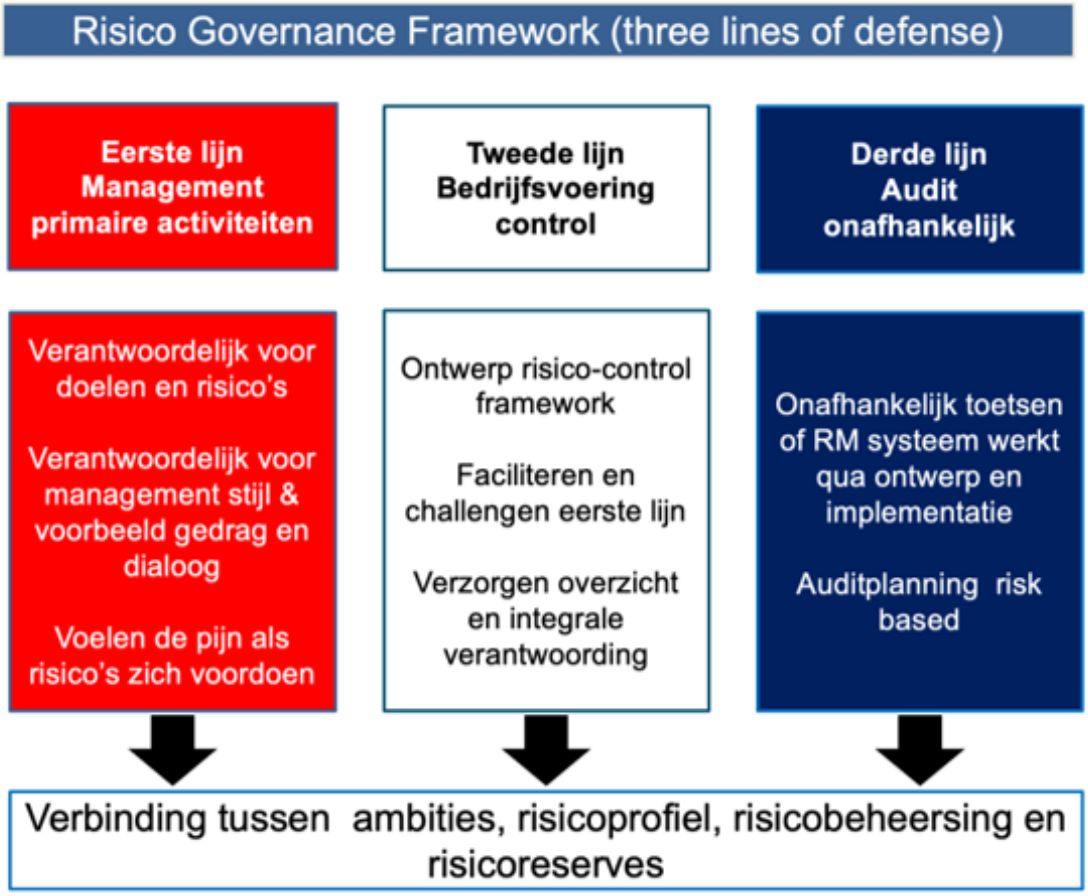
Op dit niveau heeft de gemeente de informatiebeveiliging en privacy op een professionele wijze geborgd binnen de organisatie en processen. Daarbij zijn de risico's geminimaliseerd tot een acceptabel niveau. Dit niveau is ook noodzakelijk om te kunnen voldoen aan (aankomende) wet- en regelgeving.

Volwassenheidsniveau 5 is het ultieme, maar vraagt een grote betrokkenheid van alle medewerkers voor informatieveiligheid. Dat is voorlopig niet reëel.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. Goede onderlinge samenwerking en afstemming, ieder vanuit zijn eigen verantwoordelijkheid, zijn bepalend voor het succes van informatiebeveiliging en privacy. De methodiek, die hier het beste bij aansluit, is het 'Three Lines Model' (eerder bekend als 'Three Lines of Defense').

14) *Gebaseerd op volwassenheidsmodel voor informatieveiligheid van NBA-LIO/NOREA*



In dit model is het lijnmanagement verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen. De tweede lijn (CISO, PO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier zit ook de ENSIA coördinator.

Ongeacht het voorgaande is en blijft ledere medewerker, zowel vast als tijdelijk, intern of extern, verplicht (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde:

- toegang;
- gebruik;
- verandering;
- openbaring;
- vernietiging;
- verlies; en/of,
- overdracht.

en bij vermeende inbreuken hiervan melding te maken.

3.1. Aansturing: managementteam
Het managementteam zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teamleider. Het managementteam zorgt dat de teamleiders zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. Het managementteam zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het managementteam stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het managementteam draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidson-

derwerpen en laat zich hierin bijstaan door de CISO en PO van de gemeente. Zij vormen het kloppend hart van dit beleid en coördineren en bewaken mede de uitvoering hiervan. Daarmee fungeren zij als aanjager voor het onderwerp informatiebeveiliging en privacy.

Het managementteam autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt in de gemeente gezien als een integraal onderdeel van risicomanagement.

3.2. Uitvoering: afdelingshoofden en teamleiders
Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Etten-Leur hebben een interne eigenaar die de primaire verantwoordelijkheid draagt voor de bescherming van de daarin aanwezige informatie. Om deze verantwoordelijkheid waar te maken moeten zij goed ondersteund worden vanuit de tweede lijn.

Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel (bijvoorbeeld aan een kwaliteitsmedewerker of vakspecialist binnen het eigen team). De bedoeling is dat alle processen, systemen, verwerkingen en (persoons)gegevens altijd een eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn.

Afdelingshoofden en teamleiders rapporteren aan het managementteam over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp informatiebeveiliging en privacy te bespreken in het MT-overleg.

Enkele belangrijke taken van de afdelingshoofden en teamleiders in het kader van informatiebeveiliging en privacybescherming zijn, in samenwerking met de CISO en PO:
- Het leveren van input voor wijzigingen op maatregelen en procedures.
- Het voldoen aan wet- en regelgeving die op hun processen van toepassing is en invulling geven aan de rollen die binnen die wet- en regelgeving bedacht is.
- Het binnen de eigen afdeling uitdragen van het IB&P beleid en de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
- Het vroegtijdig betrekken van CISO, PO en FG, bij nieuwe of gewijzigde processen.
- Het (laten) uitvoeren van risicoanalyses en (pre-)DPIA's voor de processen waar zij verantwoordelijk voor zijn.
- Het leveren van informatie voor de bijhouding van diverse voorgeschreven registers, zoals het verwerkingsregister, algoritmeregister, etc.
- Bespreking van beveiligingsincidenten en privacy inbreuken en de consequenties die dit moet hebben voor beleid en maatregelen.

3.3. Controle en verantwoording
Dit Strategisch IB&P Beleid is een verantwoordelijkheid van het bestuur van de gemeente Etten-Leur. Bestuur en management werken volgens de 10 principes voor informatiebeveiliging en privacy en de beginselen voor het verwerken van (persoons)gegevens. Zij geven sturing aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie.
Het managementteam is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan respectievelijke portefeuillehouders. Het managementteam rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.
De FG, CISO en PO hebben de bevoegdheid om gevraagd en ongevraagd te rapporteren over informatiebeveiliging en privacy aan bestuur en management.

3.4. ENSIA

De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA[15] -systematiek. Dat betekent dat hiervoor een 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 afdelingshoofden en teamleiders. Zij leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten.

De verantwoording over de informatiebeveiliging en privacybescherming komt in het jaarverslag tot uitdrukking in de collegeverklaring Informatiebeveiliging en privacy. Met deze verklaring geeft het college van B en W aan in hoeverre de gemeente voldoet aan de afspraken die gemaakt zijn voor de ENSIA-

15) *Eenduidige normatiek single information audit*

verantwoording Informatiebeveiliging en wettelijke eisen zoals uit de AVG. 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/WOZ[16] /BAG[17]/SUWI[18].

Middels deze verantwoording worden het bestuur van de gemeente en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel en laat zien dat de gemeente Etten-Leur informatiebeveiliging en privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

3.5. Verdere uitwerking IB&P governance
Voortbordurend op het gehanteerde "Three lines of defense"-model zal het managementteam de governance binnen deze kaders nader uitwerken. Deze zijn uitgewerkt in de bijlage bij dit beleid.

Praktische uitgangspunten hierbij zijn:

- Het college van B en W stelt als eindverantwoordelijke het strategisch IB&P beleid vast.
- Het managementteam stelt jaarlijks het IB&P plan vast.
- Het managementteam is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in een managementsysteem voor informatiebeveiliging en privacybescherming.
- Het managementteam is verantwoordelijk voor het vragen om informatie bij de afdelingshoofden en teamleiders en ziet erop toe dat deze adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.
- De CISO ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert hierover rechtstreeks aan het managementteam
- De PO ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de bescherming van persoonsgegevens en rapporteert hierover rechtstreeks aan het managementteam.
- De FG is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG en WPG voorschrijven.
- De CISO, FG en PO brengen jaarlijks gezamenlijk voorgaand jaarverslag uit, mitsdien hierover overeenstemming is, waarbij rekening wordt gehouden met de wettelijke onafhankelijkheid van de FG en CISO.
- Het managementteam, afdelingshoofden en teamleiders stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de functionaris gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.
- Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO, PO en/of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De afdelingshoofden en teamleiders zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging en privacy voor de bedrijfsmiddelen (processen, projecten, systemen, etc.) waarvoor zij verantwoordelijk zijn.
- Iedereen, intern en/of extern, die werkzaamheden verricht voor of namens de gemeente Etten-Leur is verantwoordelijk voldoende basiskennis, waaronder informatiebeveiliging en privacy, op te doen en deze bewust altijd toe te passen bij het uitvoeren van deze werkzaamheden. Hiervoor wordt in of naast het jaarplan informatiebeveiliging en privacy een bewustwordingsprogramma opgesteld en uitgevoerd.

3.6. Uitgangspunten en randvoorwaarden
Om dit beleid goed uit te kunnen voeren zijn een aantal uitgangspunten en randvoorwaarden van belang. Deze worden in deze paragraaf verder uitgewerkt.

16) *Wet onroerende zaken*
17) *Basisregistratie adressen en gebouwen*
18) *Wet structuur uitvoeringsorganisatie werk en inkomen*

3.6.1. Uitgangspunten

- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.

3.6.2. Randvoorwaarden

Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt een IB&P plan opgesteld, gebaseerd op:
    - Nieuwe en gewijzigde wet- en regelgeving;
    - Dit IB&P beleid;
    - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
    - Andere audit resultaten;
    - het dreigingsbeeld gemeenten van de IBD;
    - Uitkomsten risico-analyses en DPIA's;
    - De door de afdelingsmanagers ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).

- Om uitvoering te kunnen geven aan dit strategisch beleid en het IB&P plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

Bijlage: Uitwerking rollen en verantwoordelijkheden informatiebeveiliging en privacy

1. Inleiding

Deze bijlage vormt een nadere uitwerking van hoofdstuk 3 van het Strategisch Informatiebeveiligings- en privacybeleid 2024-2027.

Hierin worden de rollen en verantwoordelijkheden rondom informatiebeveiliging en privacy binnen onze organisatie nader toegelicht. Dit vormt een essentieel onderdeel van ons streven naar een veilig en betrouwbaar beheer van informatie.

1.1. Leeswijzer

In dit document worden de specifieke taken en verantwoordelijkheden van de verschillende functionarissen en teams binnen de organisatie uiteengezet. Het begint met een beschrijving van de bestuurlijke verantwoordelijkheid en de wijze waarop deze in de organisatie is verankerd.

Vervolgens worden de rollen van de sleutelfunctionarissen, zoals de Functionaris Gegevensbescherming (FG), de Privacy Officer, en de Chief Information Security Officer (CISO), gedetailleerd uitgewerkt.

Hiermee biedt deze bijlage houvast en duidelijkheid over wie verantwoordelijk is voor de verschillende aspecten van informatiebeveiliging en privacy.

2. Rollen en verantwoordelijkheden bestuur en organisatie

2.1. Bestuurlijke verantwoordelijkheid

Gemeenteraad, College, en Portefeuillehouder
Dragen bestuurlijke verantwoordelijkheid voor het formuleren en implementeren van beleid op het gebied van informatiebeveiliging en privacy. De gemeenteraad treedt op als toezichthouder.

2.2. Organisatie

Gemeentesecretaris
Is eindverantwoordelijk voor de borging van informatiebeveiliging en privacy binnen de organisatie.

Managementteam (MT)
Verantwoordelijk voor het integreren van informatiebeveiliging en privacy in strategische besluitvorming en processen binnen de organisatie.

Concerncontroller
Adviseert en ondersteunt op het gebied van informatiebeveiliging en privacy in relatie tot risicobeheer en rechtmatigheid.

Afdelingshoofd Bedrijfsvoering & Teamleider Informatie
Zijn verantwoordelijkheid voor het vormen en borgen van een organisatorisch breed geweten op het gebied van informatiebeveiliging en privacy op concernniveau.

Overige afdelingshoofden / teamleiders / proceseigenaren
Verantwoordelijk voor de correcte verwerking van informatie binnen hun processen, inclusief het nemen van maatregelen voor informatiebeveiliging en privacy.

Informatieadviseurs / businessanalist / data-analist
Geven advies over de toepassing van informatiebeveiligings- en privacybeleid binnen hun specifieke werkveld.

Functioneel beheerders
Verantwoordelijk voor het beheer van informatiesystemen en het implementeren van beveiligings- en privacy maatregelen. Inclusief de bewaking daarvan bij leveranciers. Hierbij hebben zij een signaalfunctie richting de proceseigenaren en het IB&P-team.

Juridische ondersteuners/concernjurist/inkoopadviseurs
Adviseren op juridisch c.q. inkooptechnisch gebied, met inachtneming van informatiebeveiliging en privacy wet- en regelgeving. Zo nodig betrekken zij het IB&P-team.

Contactpersonen IB&P / kwaliteitsmedewerkers
Treden vanuit deze rol binnen hun team of afdeling op als vooruitgeschoven ondersteunde post op het gebied informatiebeveiliging en privacy. Zij zijn goed bekend met de processen binnen hun werkveld en zorgen er voor dat het IB&P-team goed en tijdig wordt aangehaakt. Deze samenwerking verloopt uiteraard visa versa.

Projectleiders
Zorgen, samen met de opdrachtgever, voor de borging van informatiebeveiliging en privacy in de uitvoering van projecten.

Iedere medewerker / andere gebruikers van bedrijfsmiddelen
Verantwoordelijk voor het naleven van informatiebeveiligings- en privacyrichtlijnen in hun dagelijkse werkzaamheden en het signaleren van bijzonderheden op dit gebied.

2.3. Externe partners (Leveranciers, ICT WBW, Samenwerking op de "ï", De6 gemeenten, KAREL, etc.)
Geacht zich te houden aan de gestelde informatiebeveiligings- en privacyvereisten in hun dienstverlening aan de organisatie.

3. Taken sleutelfunctionarissen informatiebeveiliging en privacy

3.1. Functionaris gegevensbescherming

3.1.1. Positionering
De FG…
- Voert zijn taken onafhankelijk van het verantwoordelijke bestuursorgaan, management of medewerkers uit.
- Ontvangt t.a.v. zijn taken geen instructies van het verantwoordelijke bestuursorgaan, management of medewerkers.
- Wordt niet ontslagen of gestraft naar aanleiding van de uitvoering van zijn taken.
- Brengt rechtstreeks verslag uit aan de gemeentesecretaris en griffier (als hoogst leidinggevende van de ambtelijke organisatie van de respectievelijke bestuursorganen) en het verantwoordelijke bestuursorgaan.
- Heeft rechtstreeks toegang tot het verwerkingsverantwoordelijke bestuursorgaan en het management als hij dat nodig acht, bijvoorbeeld om door hem gesignaleerde risico's naar voren te brengen.
- Geeft zwaarwegende adviezen. Het verantwoordelijke bestuursorgaan, management en medewerkers kunnen daarvan afwijken, zij het gemotiveerd en gedocumenteerd.
- Heeft op zijn verzoek toegang tot alle informatie, systemen en processen en ruimtes wanneer hij dat noodzakelijk acht voor de uitvoering van zijn taken.
- Wordt naar behoren en tijdig betrokken bij aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- Wordt door de directie en de proceseigenaren ondersteund in de uitoefening van het toezicht.

3.1.2. Taken
Algemeen
De FG…
- Voert geen taken uit die kunnen conflicteren met zijn taken als FG, waaronder taken waarbij hij verantwoordelijk is voor verwerkingen t.b.v. de verwerkingsverantwoordelijke.
- Houdt bij de uitvoering van zijn taken naar behoren rekening met het aan verwerkingen verbonden risico, en met de aard, de omvang, de context en de verwerkingsdoeleinden.

Toezichthouden
De FG…
- Ziet toe op de toepassing en naleving van verplichtingen van de organisatie t.a.v. gegevensbescherming. Er wordt toezicht gehouden op: de verplichting om medewerkers bewust te maken en op te leiden, verantwoordelijkheden toe te wijzen, gegevensbescherming-effectbeoordelingen en audits uit te voeren, risicomaatregelen te implementeren en de afhandeling van verzoeken en klachten van betrokkenen.
- Ziet toe op de toepassing en naleving van verplichtingen van de organisatie t.a.v. gegevensbescherming bij samenwerkingen met anderen waarin de organisatie (gezamenlijk) verwerkingsverantwoordelijk blijft.
- Ziet toe op de toepassing en naleving van het gegevensbeschermingsbeleid van de organisatie.
- Treedt op als contactpunt voor en pleegt overleg met de Autoriteit Persoonsgegevens over aangelegenheden t.a.v. gegevensbescherming, en werkt in die hoedanigheid met haar samen ten behoeve van de versterking van haar systeemtoezicht.
- Treedt op als contactpunt voor burgers aangaande aangelegenheden t.a.v. gegevensbescherming, en ziet in die hoedanigheid toe op de afhandeling door de organisatie van klachten en andere knelpunten die de burger signaleert.

Informeren
De FG…

- Informeert het verantwoordelijke bestuursorgaan, management en medewerkers over hun verplichtingen t.a.v. gegevensbescherming.

Adviseren
De FG…
- Geeft het verantwoordelijke bestuursorgaan en management gevraagd en ongevraagd strategisch en tactisch advies over passende wijzen om hun verplichtingen t.a.v. gegevensbescherming in hun taakuitvoering, bedrijfsvoering en dienstverlening in te vullen en te integreren, waaronder over het te voeren beleid en prioritering van activiteiten.
- Geeft advies over de noodzaak en de wijze van uitvoeren van gegevens-beschermingseffectbeoordelingen of enige andere gegevensbeschermings-gerelateerde risicoanalyse.
- Geeft advies naar aanleiding van uitgevoerde gegevensbeschermings-effectbeoordelingen of enige andere gegevensbeschermingsgerelateerde risicoanalyse (zoals risicoanalyses t.a.v. de toepassing van algoritmen, geautomatiseerde besluitvorming of doorgifte naar landen buiten de Europese Economische Zone), waaronder over adequaatheid van gedefinieerde maatregelen.
- Geeft bestuur en management gevraagd en ongevraagd advies over het afhandelen van klachten, uitoefenen van rechten, en adresseren van knelpunten die de burger signaleert.

3.2. Privacyofficer .

3.3.1 Positionering
De privacy officer…
- Is gepositioneerd binnen de afdeling Concernondersteuning.
- Heeft een voldoende onafhankelijke positie.
- Ontvangt t.a.v. zijn taken richtinggevend advies van de functionaris gegevensbescherming.
- Rapporteert rechtstreeks aan het management
- Informeert en betrekt zo nodig de functionaris gegevensbescherming.

3.3.2. Taken
Rapporteren
De privacy officer…
- Legt verantwoording af in het kader van de planning en control cyclus.

Coördineren
De privacy officer…
- Coördineert de organisatiebrede privacyactiviteiten en -projecten.
- Coördineert de uitvoering van (meer)(jaren)plannen.
- Coördineert de afhandeling van datalekken.
- Coördineert de afhandeling van rechtenverzoeken.
- Coördineert de uitvoering van gegevensbeschermingseffectbeoordelingen.
- Onderhoudt een overlegstructuur met de verschillende organisatieonderdelen ter bevordering van kennis en kwaliteit ten aanzien van privacy.

Planvorming en beleid
De privacy officer…
- Formuleert, beheert, evalueert en monitort beleid en procedures.
- Stelt (meer)(jaren)plannen op, waaronder voor de bewustwording en opleiding van management en medewerkers en voor communicatie naar betrokkenen.
- Monitort en evalueert de uitvoering van (meer)(jaren)plannen.

Adviseren
De privacy officer…
- Adviseert bestuur en de ambtelijke organisatie over privacybeleid en -ontwikkelingen
- Geeft advies aan management, teamleiders en medewerkers over de toepassing van privacygerelateerde wet- en regelgeving en branchenormering.
- Geeft advies over (afdelings)specifieke privacygerelateerde reglementen, beleid en werkinstructies en over de positionering van privacy in werkprocessen.
- Adviseert en ondersteunt bij het sluiten van verwerkersovereenkomsten, regelingen, reglementen en convenanten

Uitvoeren
De privacy officer…
- Beheert privacyregisters, zoals verwerkingsregisters, datalekregisters, risico- en maatregelenregisters.
- Adviseert over en draagt zorg voor organisatiebrede richtlijnen, standaarden, methoden en technieken voor privacy.

- Participeert in projectgroepen.
- Inventariseert en analyseert meldingen van inbreuken in verband met persoonsgegevens (datalekken).
- Monitort de relevante risico's voor de gemeente.
- Organiseert bewustwordings- en trainingsactiviteiten.

Ondersteunen
De privacy officer…
- Ondersteunt de organisatie bij de uitvoering van haar taken op het gebied van privacy, waaronder:
  - de afhandeling van datalekken.
  - de afhandeling van rechtenverzoeken van burgers.
  - implementatie en de uitvoering van het privacybeleid.
  - de uitvoering van gegevensbeschermingseffectbeoordelingen.

- Is eerste aanspreekpunt voor privacygerelateerde onderwerpen binnen de organisatie.

3.4. Chief Information Security Officer (CISO).

3.4.1. Positionering
De CISO…
- Voert zijn taken onafhankelijk van het verantwoordelijke bestuursorgaan, management of medewerkers uit.
- Is gepositioneerd binnen de afdeling Concernondersteuning.
- Is strategisch IB-adviseur van het bestuur, de directie en het management en geeft gevraagd en ongevraagd zwaarwegend advies.

3.4.2. Taken
Rapporteren
De CISO…
- Rapporteert periodiek over de status van informatiebeveiliging, IB-incidenten en de afhandeling daarvan aan het bestuur en de directie.

Coördineren
De CISO…
- Onderhoudt een overlegstructuur met het bestuur, de directie en het management.
- Stemt de werkzaamheden af van personen, afdelingen en instanties die zijn betrokken bij de uitvoering van het strategisch IB-beleid.
- Coördineert de organisatiebrede (strategische) IB-activiteiten en -projecten.
- Coördineert de verhoging van bewustzijn op het gebied van IB bij het bestuur en organisatie.
- Coördineert de uitvoering van organisatiebrede jaarplannen / meerjarenplan IB.
- Initieert en / of coördineert IB-assessments, -tests, reviews en -audits.
- Coördineert de IB-calamiteitenorganisatie.

Planvorming en beleid
De CISO…
- Formuleert, beheert, evalueert en monitort beleid en procedures.
- Vertaalt het Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten van de IBD naar jaarplannen / meerjarenplan IB.

Adviseren
De CISO…
- Adviseert (gevraagd en ongevraagd) het bestuur, de directie en management bij de uitwerking van het strategisch IB-beleid in jaarplannen / meerjarenplan IB voor hun verantwoordelijkheidsgebieden, en bij de implementatie van deze plannen.
- Adviseert (gevraagd en ongevraagd) het bestuur, de directie en het management bij relevante (nieuwe) ontwikkelingen.
- Adviseert (gevraagd en ongevraagd) het bestuur, de directie en het management zodat de juiste acties worden genomen ten aanzien van de informatiebeveiliging.
- Adviseert (gevraagd en ongevraagd) het bestuur, de directie en het management bij de reactie op ernstige IB- en ICT-incidenten.
- Adviseert het crisisteam, bij een hack, cyberaanval, of een andere continuïteitsverstoring in de dienstverlening.
- Geeft zwaarwegend advies, waar alleen met gegronde motivatie van kan worden afgeweken, waarbij de consequenties van afwijking op het juiste niveau worden aanvaard.

Uitvoeren
De CISO…

- Adviseert over, draagt zorg voor en monitort organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging.
- Monitort, evalueert en borgt de kwaliteit van IB-assessments.
- Monitort de relevante risico's voor de gemeente.
- Organiseert bewustwordings- en trainingsactiviteiten.
- Onderhoudt contact met (overheids)instanties en toezichthouders ten aanzien van informatiebeveiligingsaangelegenheden.
- Onderhoudt contact met de informatiebeveiligingsdienst (IBD).

Ondersteunen
De CISO…
- Is eerste aanspreekpunt voor IB-gerelateerde onderwerpen binnen de organisatie.
- Ondersteunt de organisatie bij de uitvoering van haar taken op het gebied van informatiebeveiliging.