RSD-Governancemodel
Informatiebeveiliging & Privacyorganisatie

vastgesteld in de MT-vergadering van 18 maart 2025

Bijgaand het document 'RSD-Governancemodel Informatiebeveiliging & Privacyorganisatie'. Dit document beschrijft de inrichting van de taakvelden informatiebeveiliging en privacy in de organisatie (de IB&P-organisatie) en maakt hiermee helder welke rollen, taken en verantwoordelijkheden de betrokken functionarissen hebben. Dit document is een levend document en wordt zo nodig aanpast in geval van nieuwe ontwikkelingen of nieuwe zienswijzen op een juiste inrichting. Het governancemodel heeft als doel een organisatie te creëren waarin beveiliging van informatie wordt gewaarborgd, aan de relevante wet- en regelgeving wordt voldaan, de continuïteit van de bedrijfsvoering is gewaarborgd en de reputatie van de RDWI als betrouwbare partner wordt beschermd.

Bijlage: Tabel 'Overzicht functies in de IB&P-organisatie' (*nog te realiseren*)

Documentbeheer

Versie	Datum	Wijziging / Actie
1.0	24/11/2020	Vastgesteld MT met voorbehoud aanpassing ISO P&O
1.1	02/12/2020	Akkoord P&O met voorgestelde aanpassing; ter informatie naar MT van 12/01/21
2.0	25/03/2025	Wijziging naam Revisie en aanvulling

Rollen, taken en verantwoordelijkheden binnen de IB&P-organisatie[1],

(mede) ontleend aan

- de organisatie IB&P, zoals laatstelijk vastgesteld door het MT op 6 december 2022
- de handreiking positionering en taken van de FG (IBD), en
- de handreiking functieprofielen informatiebeveiliging V1.0 (IBD)

Verantwoordelijkheidsniveaus

Binnen de RSD worden de volgende vier verantwoordelijkheidsniveaus met betrekking tot informatiebeveiliging en privacy onderscheiden.

Dagelijks bestuur

Het dagelijks bestuur, als eigenaar van de verwerkingen en (informatie)systemen van de RSD, draagt de bestuurlijke verantwoordelijkheid voor een passend niveau van privacy. Zij stelt – onder andere middels het privacybeleid - de kaders ten aanzien van privacy op basis van relevante wet- en regelgeving en normenkaders. Zij is verantwoordelijk voor een duidelijk te volgen privacybeleid en stimuleert de directeur en de unitmanagers dit beleid na te leven.

Directeur

Gemandateerde verantwoordelijkheid voor privacy ligt bij de directeur. Deze vormt samen met de unitmanagers het managementteam en stelt het gewenste niveau van privacy vast. De directeur is verantwoordelijk voor een correcte omgang met en juiste beveiliging van persoonsgegevens, bedrijfsprocessen en in- en externe informatiesystemen. De directeur wijst voor ieder (informatie)systeem een proceseigenaar aan. De ambtelijke eindverantwoordelijkheid ligt bij de directeur.

Unitmanagers

De unitmanagers vormen samen met de directeur het managementteam. De unitmanagers zijn verantwoordelijk voor de persoonsgegevens en integrale beveiliging van de processen en systemen die draaien onder hun verantwoordelijkheid. De unitmanagers zijn verantwoordelijk voor een juiste en veilige omgang met persoonsgegevens en de implementatie en het uitdragen van de maatregelen die voortvloeien uit het privacybeleid.

Medewerkers

Iedere medewerker is verantwoordelijk voor een juiste omgang met en beveiliging van persoonsgegevens die worden verwerkt binnen de eigen functie en taken. Medewerkers zijn zich bewust van de eisen ten aanzien van de omgang met persoonsgegevens en de vertrouwelijkheid, integriteit en beschikbaarheid van de informatieprocessen binnen de eigen functie en taken. Door de unitmanager worden ze geïnformeerd over procedures en werkwijzen en passen de regels en uitgangspunten hieruit toe in de uitvoering van de werkzaamheden.

Rollen, taken en verantwoordelijkheden uitgewerkt

Om informatiebeveiliging en privacy goed in te bedden binnen de organisatie is het informatiebeveiliging en privacy (IB&P)-team samengesteld. Het IB&P-team bestaat uit diverse rollen uit het IB&P-werkveld die in gezamenlijkheid zorgen voor een juiste positionering van het onderwerp binnen de organisatie. Het IB&P-team helpt bij het passend beheersen van informatiebeveiligings- en privacyrisico's, het ontwikkelen van

[1] Schematisch overzicht van de taken in bijgevoegde tabel (*nog niet gerealiseerd*)

informatiebeveiligings- en privacybeleid en procedures en fungeert als een intern aanspreekpunt voor informatiebeveiligings- en privacy-gerelateerde kwesties. Het IB&P-team bestaat uit de volgende rollen/functies:

Privacy Officer (PO)
De PO is verantwoordelijk voor het vormgeven en bewaken van het privacybeleid en draagt zorg voor het waarborgen van de privacy binnen de organisatie.

De PO:
- is eerste aanspreekpunt voor privacy-gerelateerde onderwerpen binnen de organisatie;
- formuleert, beheert, evalueert en monitort het privacybeleid en bijbehorende procedures;
- stelt de jaarlijkse privacyagenda op en informeert het managementteam hierover;
- adviseert het managementteam, en de ambtelijke organisatie, over privacybeleid en hiermee samenhangende reglementen en/of instructies en de positionering van privacy in werkprocessen;
- adviseert en ondersteunt bij het sluiten van verwerkersovereenkomsten;
- adviseert over technische, juridische en organisatorische maatregelen onder andere n.a.v. datalekken en risicoanalyses, zoals autorisatie, authenticatie en overeenkomsten;
- ondersteunt bij de afhandeling van datalekken, rechtenverzoeken van burgers, de implementatie en de uitvoering van het privacybeleid;
- is verantwoordelijk voor een tijdige melding van datalekken bij de autoriteit persoonsgegevens en overlegt hierover met de functionaris gegevensbescherming;
- ondersteunt bij de uitvoering van DPIA's;
- beheert, en draagt zorg voor de juistheid van, de privacyregisters, zoals onder meer het verwerkingsregister, het datalekregister en het risicoregister;
- draagt zorg voor het jaarlijks invullen van het AVG-borgingsinstrument;
- inventariseert en analyseert meldingen van inbreuken in verband met persoonsgegevens (datalekken) en rapporteert hier jaarlijks over aan het managementteam;
- organiseert bewustwordings- en trainingsactiviteiten en betrekt het IB&P-team hierbij;
- betrekt en informeert de functionaris gegevensbescherming bij diens activiteiten.

De Chief Information Security Officer (CISO)
De CISO treedt op als strategisch adviseur voor het bestuur en het managementteam en adviseert over het strategisch IB-beleid en geeft gevraagd en ongevraagd zwaarwegend advies. De CISO stuurt de informatiebeveiliging overeenkomstig de behoeften en de risicobereidheid van de organisatie en legt (tenminste) halfjaarlijks verantwoording hierover af aan het bestuur en het managementteam.

De CISO:
- rapporteert periodiek over de status van informatiebeveiliging, IB-incidenten en de afhandeling daarvan aan het bestuur en het managementteam.

Coördineren
De CISO:
- onderhoudt een overlegstructuur met het bestuur en het managementteam;
- 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, het managementteam, medewerkers en betrekt het IB&P-team hierbij;
- coördineert de uitvoering van organisatiebrede jaarplannen / meerjarenplan IB;
- initieert en / of coördineert IB-assessments, -tests, reviews en -audits.

Planvorming en beleid
De CISO:
- monitort en evalueert het strategisch en aanvullend IB-beleid;
- draagt zorg voor het opstellen, bijstellen, vernieuwen en herzien van strategische jaarplannen / meerjarenplan IB;
- monitort en evalueert de uitvoering van jaarplannen / meerjarenplan IB;
- vertaalt het Dreigingsbeeld informatiebeveiliging Nederlandse gemeenten van de IBD naar jaarplannen / meerjarenplan IB;
- monitort externe ontwikkelingen zoals Europese en nationale wet- en regelgeving.

Adviseren
De CISO:
- adviseert (gevraagd en ongevraagd) over en ontwikkelt het strategisch IB-beleid op bestuurlijk niveau;
- adviseert (gevraagd en ongevraagd) het bestuur en het managementteam 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 en het managementteam bij relevante (nieuwe) ontwikkelingen;
- adviseert (gevraagd en ongevraagd) het bestuur en het managementteam zodat de juiste acties worden genomen ten aanzien van de informatiebeveiliging;
- adviseert (gevraagd en ongevraagd) het bestuur en het managementteam 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:
- draagt zorg voor het monitoren en evalueren van het strategisch en aanvullend IB-beleid;
- draagt zorg voor organisatiebrede richtlijnen, standaarden en methoden voor informatiebeveiliging;
- monitort, evalueert en borgt het naleven van richtlijnen, standaarden en methoden voor informatiebeveiliging;
- monitort, evalueert en borgt de kwaliteit van IB-assessments;
- monitort, evalueert en borgt het IB-bewustzijn binnen de organisatie.
- monitort de relevante risico's voor de organisatie;
- werkt nauw samen met de information security officer(s) (ISO), functionaris gegevensbescherming (FG) en privacy officer(s) (PO);
- werkt nauw samen met businesscontrollers, risicomanagers, (interne) auditor en de unitmanager Financien, Informatiemanagement en Facilitair (FIF);
- 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 voor het bestuur en het managementteam;
- ondersteunt het bestuur en het managementteam bij het opstellen, bijstellen, vernieuwen en herzien van het strategisch IB-beleid;
- ondersteunt het dagelijks bestuur bij de IB-verantwoording aan het algemeen bestuur;
- ondersteunt de IB-organisatie bij de uitvoering van haar taken;
- neemt deel aan regionale CISO-koepels;
- wisselt extern kennis en ervaring uit met vakgenoten van andere gemeenten en met de informatiebeveiligingsdienst (IBD).

Information Security Officer (ISO)
De ISO geeft op tactisch / operationeel niveau invulling aan de IB-functie voor de hele organisatie. De ISO:
- fungeert als eerste aanspreekpunt binnen de organisatie voor informatiebeveiligingsvraagstukken *(nog te realiseren)*;
- ontvangt ten aanzien van zijn taken richtinggevend advies van de CISO *(nog te realiseren)*;
- ondersteunt de CISO en de organisatie bij het implementeren van maatregelingen op het gebied van informatiebeveiliging;
- ondersteunt bij het opstellen van IB-processen en -procedures;
- houdt het IB-incidentenregister up to date en signaleert en rapporteert aan de CISO/PO in geval er sprake is van een beveiligingsincident *(nog te realiseren)*;
- rapporteert periodiek aan de CISO en het managementteam over de status van informatiebeveiliging, bewustwording, IB-incidenten en de afhandeling daarvan;
- schrijft, in samenwerking met de CISO, jaarlijks het informatiebeveiligingsplan (de realisatie van het informatiebeveiligingsbeleid), en zorgt voor een juiste implementatie en naleving hiervan *(nog te realiseren)*;
- adviseert het managementteam bij de uitwerking van het IB-beleid in jaarplannen;
- houdt toezicht op de naleving van vastgestelde maatregelen en procedures op het gebied van informatiebeveiliging en rapporteert hierover aan de CISO *(nog te realiseren);*
- initieert de jaarlijkse check op het informatiebeveiligingsbeleid en de driejaarlijkse revisie hiervan *(nog te realiseren);*
- adviseert en ondersteunt bij het sluiten van verwerkersovereenkomsten;
- is poortwachter als het gaat om het signaleren van wijzigingen in processen die van invloed kunnen zijn op informatiebeveiliging *(nog te realiseren)*.

Security Officer Suwinet (SO)[2]
De SO:
- is verantwoordelijk voor het toezicht op de naleving van de maatregelen en procedures die voortkomen uit het beveiligingsplan Suwinet;
- bevordert de informatiebeveiliging en communicatie naar de medewerkers betreffende dit onderwerp;
- voert periodieke controles uit op een rechtmatig gebruik van Suwinet-gerelateerde applicaties en vraagt indien nodig een specifieke rapportage op en rapporteert hierover rechtstreeks aan het MT;

Met opmerkingen [AT1]: Ook nog te realiseren, bewustwording is bij de PO op dit moment belegd

[2] Verplichte aanstelling vanuit suwinet-wetgeving

- beoordeelt toegangsaanvragen voor Suwinet-gerelateerde applicaties en bepaalt daarbij ook de rol die de medewerker binnen deze applicaties;
- bespreekt persoonlijk met de nieuwe medewerkers het gebruik van Suwinet-gerelateerde applicaties en brengt hen op de hoogte van de beveiligingsprocedures. Onderdeel daarvan is het laten ondertekenen van de zorgvuldigheidsverklaring door de medewerker. De SO zorgt voor archivering van die ondertekende zorgvuldigheidsverklaring.

Informatie en communicatietechnologie (ICT) regisseur
De ICT regisseur is het centraal aanspreekpunt op het gebied van informatiebeveiliging en fungeert als schakel tussen de Regionale ICT Dienst (RID) en de organisatie. De ICT regisseur:

- adviseert op het gebied van informatiebeveiliging en controleert of/en in hoeverre beveiligingsmaatregelen worden nageleefd;
- voert regie uit op de bestaande dienstverlening door de RID aan de RSD, door tijdig te rapporteren, te analyseren en verbeteringen voor te stellen;
- bewaakt de met de RID afgesloten SLA o.a. wat betreft doorlooptijden, kosten, overige services en afspraken;
- ondersteunt de proceseigenaar bij het opstellen van autorisatiematrixen;
- draagt zorg voor controles op de rechtmatige toegang tot bedrijfsapplicaties;
- heeft een signaalfunctie in het geval van informatiebeveiligingsincidenten en is betrokken bij de opvolging hiervan;
- voert regie op in- en externe audits op het gebied van informatiebeveiliging;
- formuleert, beheert, evalueert en monitort het Suwinet-beveiligingsplan en onderneemt actie voor de jaarlijkse evaluatie en opvolging.

De Functionaris Gegevensbescherming (FG)
De FG is de onafhankelijke privacy adviseur en toezichthouder op de naleving van de privacywetten en -regelgeving binnen de organisatie. De kerntaken van de FG zijn vierledig: adviseren, toezien op naleving, samenwerking met en optreden als contactpunt van de AP, optreden als contactpunt voor betrokkenen

De FG:

- ziet toe op naleving van de AVG, Wpg en andere EU wet- en regelgeving, nationale bepalingen en het door de organisatie gevoerde privacybeleid inzake gegevensbescherming. Dit toezicht ziet toe of er voldaan is aan de verplichtingen omtrent het toewijzen van verantwoordelijkheden, het bewustmaken en opleiden van het bij de verwerking betrokken personeel en het uitvoeren van audits;
- informeert en adviseert (gevraagd en ongevraagd) over de verplichtingen uit hoofde van de AVG, Wpg en andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen;
- wordt door de PO geïnformeerd over eventuele datalekken en ondersteunt in het besluit of een datalek wordt gemeld bij de AP en/of betrokkene(n);
- geeft advies over de noodzaak en de wijze van uitvoeren van DPIA's of enige andere privacy-gerelateerde risicoanalyse;
- geeft advies naar aanleiding van uitgevoerde DPIA's of enige andere privacy risicoanalyse;
- 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.
- geeft bestuur en management gevraagd en ongevraagd advies over het afhandelen van klachten, uitoefenen van rechten, en adresseren van knelpunten die de burger signaleert;

- treedt op als contactpunt binnen de organisatie voor de Autoriteit Persoonsgegevens;
- rapporteert jaarlijks aan het hoogste leidinggevende niveau, diens bevindingen over AVG/Wpg-naleving en voor het overige indien de FG dit noodzakelijk acht. Daarbij kan de FG advies geven over te nemen maatregelen om juiste verwerking van persoonsgegevens te waarborgen;
- stelt een werkplan op waarin, op hoofdlijnen, het toezicht in het komende jaar uiteengezet wordt. Dit werkplan laat onverlet dat het bestuursorgaan altijd zelf verantwoordelijk is en blijft voor de manier waarop de AVG wordt nageleefd.
- wordt betrokken bij het opstellen van de privacy-jaaragenda.

Het reglement 'Functionaris voor de gegevensbescherming RDWI' is onverkort van toepassing op het handelen van de FG.

Voorgestelde overlegstructuren
IB&P-overleg
Voorzitter: ICT-regisseur
Deelnemers: PO, CISO (op uitnodiging), ISO, SO, ICT-regisseur, FG

Doel: directe sturing van de IB&P-organisatie, controle op actiepunten, toezicht op naleving.
Frequentie: Wekelijks

IB&P-overleg breed (olv coördinator FIF)
Deelnemers: Coördinator FIF, UM FIF, PO, CISO, ISO, SO, I-adviseur, ICT-regisseur, FG en coördinatoren.

Doel: Het beleggen van IB&P-bewustzijn organisatie breed en het zijn van informatieknooppunt: Wat speelt er? Waar loopt men tegenaan? Waar zitten risico's? Zijn deze bekend? Is er behoefte aan kennisoverdracht? Deelname bewustwordingsprogramma?

Frequentie: eenmaal per kwartaal