Informatiebeveiligingsbeleid gemeente Rijswijk

Datum	5 oktober 2026
Kenmerk (Corsanr)	26.145750
Opsteller	Peter van de Vaate
Versie	V 1.8

Revisie Historie

Versie	Revisie Beschrijving	Auteur	Datum
1.5	Door B&W vastgestelde versie	Peter van de Vaate	29 augustus 2023
1.6	Actualisering op basis van de Cyberbeveiligingswet en toepassing van de nieuwe versie van de BIO. Verwijzing naar de Wet Politiegegevens.	Peter van de Vaate	19 juni 2026
1.7	Tekstuele aanpassingen	Team uitvoering informatieveiligheid	3 juli 2026
1.8	Tekstuele aanpassingen na overleg wethouder	Piera Cherchi, Patricia Schoots, Peter van de Vaate	5 oktober 2026

Distributie

Naam	Versie
Gemeentelijk Managementteam	
Ciso Delft	

Referenties

Titel	Auteur
Baseline Informatiebeveiliging Overheid	
De 10 bestuurlijke principes voor informatiebeveiliging Behorende bij de Baseline Informatiebeveiliging Overheid (BIO)	Vereniging van Nederlandse Gemeenten (VNG)
Voorbeeld Strategisch Gemeentelijk Informatiebeveiligingsbeleid	Informatie beveiligingsdienst (IBD)

Besluit

Naam	Functie/Rol	Datum
Gemeentelijk managementteam	Opdrachtgever	
College B&W	Verantwoordelijk	

Inleiding
De gemeente werkt met een grote hoeveelheid informatie. Die informatie beslaat een breed terrein. Van privacy-gevoelige informatie in het sociaal domein tot informatie over de inrichting van de openbare ruimte. Inwoners en ondernemingen verwachten dat de gemeente zorgvuldig omgaat met deze gegevens (dat gevoelige informatie niet op straat komt te liggen), dat informatie beschikbaar is als die nodig is en dat de informatie klopt. De maatregelen die de gemeente neemt om dat te organiseren noemen we informatiebeveiliging.

Informatiebeveiliging gaat dus over de beschikbaarheid van de informatie, de integriteit van de informatie en over de vertrouwelijkheid van de informatie. De beveiligingsmaatregelen worden afgestemd op het soort informatie en op het gebruik ervan. Bijvoorbeeld: gegevens over schuldhulpverleningstrajecten zijn vertrouwelijk en moeten daarom goed afgeschermd zijn voor inzage door onbevoegden, gegevens over gebouwen zijn openbaar maar moeten wel altijd kloppen en beschikbaar zijn.

In het informatiebeveiligingsbeleid stelt het college de kaders en geeft het richtlijnen aan de uitvoering over de inrichting van de informatiebeveiliging: welke normen worden gehanteerd en hoe zijn de verantwoordelijkheden verdeeld. Dat maakt dat dit stuk vooral intern gericht is. Daarnaast zijn er ook externe organisaties die de gemeente om informatiebeveiligingsbeleid vragen. Het ministerie van Sociale Zaken en Werkgelegenheid vraagt dat voor het gebruik van Suwinet, Logius vraagt dat voor het gebruik van DigiD, het ministerie van Binnenlandse Zaken vraagt dat voor de uitvoering van de BRP etc. De aanwezigheid van een actueel informatiebeveiligingsbeleid is voor die regelingen zelfs een uitdrukkelijke aansluitvoorwaarde.

Het belangrijkste uitgangspunt dat met dit informatieveiligheidsbeleid wordt vastgelegd is dat de gemeente Rijswijk zich conformeert aan de Baseline Informatiebeveiliging Overheid. De werkwijze van de BIO is gericht op risicomanagement. Dat betekent dat van het management verwacht wordt dat zij op basis van een continue risicoafweging keuzes maakt om informatie in bestaande en nieuwe processen adequaat te beveiligen. Voor de ondersteuning van bestuurders bij de uitvoering van goed risicomanagement zijn door de VNG in aanvulling op de BIO de 10 bestuurlijke principes voor informatiebeveiliging opgesteld[1]:

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

De BIO is van toepassing bij alle bestuurslagen en bestuursorganen van de overheid, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn.Dit is verankerd in de Cyberbeveiligingswet.

De vorige versie van het informatiebeveiligingsbeleid werd vastgesteld in 2023. De BIO bepaalt dat het beleid ieder jaar wordt beoordeeld en zo nodig wordt bijgesteld.

[1] https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

Over het gevoerde informatiebeveiligingsbeleid wordt jaarlijks verantwoording afgelegd aan de gemeenteraad via de paragraaf Bedrijfsvoering in de jaarrekening. Voor die verantwoording is landelijk een eenduidige systematiek ontwikkeld (ENSIA, eenduidige normatiek single information audit). In feite wordt met de ENSIA verantwoording afgelegd over de mate waarin de BIO is geïmplementeerd.

De ENSIA begint ieder jaar met een zelfevaluatie waarin ruim 300 vragen beantwoord worden. Aan de hand van de beantwoording van die vragen wordt duidelijk welke maatregelen van de BIO voldoende zijn ingevoerd en welke maatregelen nog om aandacht vragen. Daar stelt het Gemeentelijk Managementteam vervolgens een actieplan voor op. Dit actieplan wordt definitief vastgesteld door het college van burgemeester en wethouders.

Informatiebeveiliging en privacy

Bij het organiseren van de informatiebeveiliging is de bescherming van persoonsgegeven***s*** een onlosmakelijk onderdeel. Elke inwoner heeft het recht om erop te kunnen rekenen dat vertrouwelijke gegevens alleen gebruikt worden voor het doel waarvoor ze verstrekt zijn, dat de verzameling van gegevens beperkt blijft tot de strikt noodzakelijke gegevens in relatie tot de te leveren dienst, dat deze gegevens niet langer bewaard worden dan noodzakelijk en tijdig vernietigd worden conform wetgeving. Tevens heeft een inwoner het recht om de eigen gegevens in te zien.

De Algemene verordening gegevensbescherming (AVG) van kracht is de wettelijke basis waarin het recht op privacy is belegd. De AVG geeft de gebruiker rechten en organisaties verantwoordelijkheid om zorgvuldig met (digitale) persoonsgegevens om te gaan. De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van de AVG. De AP is bevoegd om sancties op te leggen als een organisatie de privacywetgeving overtreedt.

Wet politiegegevens

De gemeente verwerkt in het kader van haar handhavingstaken politiegegevens als bedoeld in de Wet politiegegevens (Wpg). Op grond van artikel 33 Wpg wordt minimaal eens per vier jaar een onafhankelijke audit uitgevoerd naar de naleving van deze wet en het bijbehorende Besluit politiegegevens.

De audit richt zich op de werking en effectiviteit van de getroffen maatregelen voor beveiliging, rechtmatigheid, logging, bewaartermijnen en toegangsbeheer binnen de processen waarin politiegegevens worden verwerkt. De uitkomsten van de audit vormen input voor het continu verbeteren van de informatiebeveiliging en privacybescherming.

Reikwijdte informatiebeveiliging
Informatiebeveiliging gaat om meer dan ‘ICT’, computers en techniek. Het gaat om alle vormen van informatie en informatiedragers. Van een papieren document, via een digitaal document of video tot en met de kennis in de hoofden van mensen. Informatiebeveiliging omvat alle informatie verwerkende systemen (on-premise-applicaties, webapplicaties en SAAS-applicaties, databases, hardware etc.) maar vooral ook mensen en processen. Technisch gezien kunnen informatiesystemen nog zo goed beveiligd worden, maar als iemand bewust of onbewust informatie ‘laat slingeren’ of als er geen toezicht georganiseerd is, dan blijft het risico groot. De bescherming van waardevolle informatie is waar het uiteindelijk om gaat. Hoe waardevoller de informatie is, hoe meer maatregelen er getroffen moeten worden.

Dit beleid is van toepassing op de gehele organisatie en alle middelen, inclusief door de gemeente ingezette derden (inhuur, uitbesteding van taken aan andere partijen), informatiesystemen/ middelen waarbij het beheer door de gemeente bij derden is belegd (de verwerkers) en privé middelen van medewerkers die worden gebruikt in / voor toegang tot de werkomgeving. Het beleid is ook van toepassing op (de afspraken die worden gemaakt in het kader van) samenwerkingsverbanden.

Binnen de gemeente wordt ook Operationele Technologie (OT) ingezet. OT gaat over het besturen van onder andere gebouwen, verkeer en gemalen. Voor de bescherming van OT gebruikt de gemeente de OT-aanpak van de IBD, die gebaseerd is op de Cybersecurity Implementatie Richtlijn (CSIR).

Opbouw document

Dit document bestaat uit twee delen:

1. het informatiebeveiligingsbeleid, bestaande uit visie, inrichtingsprincipes en risicobenadering;
2. de organisatie van informatiebeveiliging: hoe zijn de verantwoordelijkheden verdeeld en hoe ziet de kwaliteitscyclus met verantwoording richting college en raad eruit.

Visie
Informatie is één van de belangrijkste bedrijfsmiddelen van de Gemeente Rijswijk. Zonder actuele en betrouwbare informatie, op de juiste plaats en op de juiste tijd, kunnen wij onze taken niet naar behoren vervullen. We werken met informatie om diensten te leveren aan onze inwoners en bedrijven, en om richting te geven aan de ontwikkeling van onze gemeente. We zijn open en transparant in wat we doen en waarom we het doen. We helpen onze inwoners en bedrijven 'in één keer goed' en voorkomen dat we dezelfde vraag twee keer stellen door goed gebruik van de informatie die wij hebben. Om dit te kunnen doen zien wij informatie als 'open tenzij'.

Maar met een nadrukkelijke 'tenzij', omdat informatie privacy of belangen van personen of organisaties kan schaden. Het is onze verantwoordelijkheid om deze rechten te beschermen. Zodat iedereen erop kan vertrouwen dat zorgvuldig met zijn/haar gegevens wordt omgegaan en dat privacy gewaarborgd is. Wij zoeken daarbij naar een goede balans tussen de te nemen maatregelen en het behouden van een goede en efficiënte dienstverlening, een transparant proces en acceptabele kosten.

Wij zorgen ervoor dat we bewust en veilig omgaan met informatie door een combinatie van organisatorisch en technisch borgen van de juiste toegankelijkheid van informatie, het opbouwen en onderhouden van het bewustzijn over informatieveiligheid en privacy en tijdige signalering en opvolging van incidenten. We zijn transparant: we maken inzichtelijk waarvoor wij de gegevens van onze inwoners gebruiken, en bieden mogelijkheden tot inzage in het eigen dossier of tot een verzoek voor wijziging/ vernietiging van de eigen gegevens.

Onze verantwoordelijkheid voor informatiebeveiliging en privacy beperkt zich niet tot onze eigen organisatie. Ook in samenwerking met andere organisaties nemen wij onze verantwoordelijkheid voor het zorgvuldig omgaan met informatie en privacy in de keten door te zorgen voor duidelijke afspraken over deze onderwerpen.

De ontwikkelingen in de samenleving en technologie maken dat informatiebeveiliging en privacy steeds belangrijker worden. Toenemende digitalisering en samenwerking met andere partijen in dienstverleningsketens leidt tot meer en makkelijker uitwisselen van informatie. Onze inwoners en bedrijven willen snel en digitaal geholpen worden, maar willen dit doen met behoud van hun recht op privacy. Onze medewerkers willen en moeten steeds meer 'anytime en anyplace' kunnen werken, maar dit mag niet leiden tot informatie die 'op straat ligt'.

Daarom zetten we ook de komende jaren in op het optimaliseren van de informatieveiligheid en privacy en het verder professionaliseren van de informatiebeveiligingsfunctie. Zodat we blijven aansluiten op de veranderende wetgeving op het gebied van persoonsgegevens, en informatiebeveiliging en privacy bij alle ontwikkelingen vanaf het begin als belangrijk thema worden meegenomen.

13 Richtinggevende principes

We zorgen er als Gemeente Rijswijk voor dat we onze informatiebeveiliging (en als onlosmakelijk onderdeel daarvan de privacy) goed georganiseerd hebben en houden. Bij de invulling daarvan hanteren we de volgende inrichtingsprincipes:

1. er is wet- en regelgeving waaraan altijd voldaan moet worden, met als voorbeelden (niet uitputtend): de Cyberbeveiligingswet, de wetgeving op het gebied van de Basisregistratie Personen (BRP), Structuur Uitvoeringsorganisaties Werk en Inkomen (SUWI), Paspoortuitvoeringsregeling 2001 (PUN), de wet Politiegegevens (WPG), Archiefwet en ook de Algemene verordening gegevensbescherming (AVG);
2. de Baseline Informatiebeveiliging Overheid (BIO) gebruiken we als basis voor de inrichting van onze informatiebeveiliging, daarbij hanteren we de 10 bestuurlijke principes voor informatiebeveiliging;
3. voor wet- en regelgeving die aanvullend op de BIO specifieke normenkaders voorschrijft, worden aparte regelingspecifieke beveiligingsplannen opgesteld. Dit geldt in ieder geval voor de uitvoering van de BRP en de aansluiting op Suwinet en DigiD;
4. om de groeiende toepassing van SAAS-applicaties (SAAS staat voor software-as-a-service[2]) beheersbaar te houden, zijn voor het gebruik van die applicaties randvoorwaarden opgesteld. Die randvoorwaarden zijn opgenomen in de Cloud Readiness Checklist. Deze checklist wordt gebruikt bij de vervanging van bestaande applicaties door SAAS-applicaties. Bij aanschaf van nieuwe applicaties worden de randvoorwaarden uit de checklist gebruikt bij het opstellen van het programma van eisen;
5. binnen deze kaders gaan we voor het beheersen van risico's tegen acceptabele kosten, waarbij we een zorgvuldige en transparante afweging maken van informatiebeveiliging en het recht op privacy versus de gewenste transparantie en het 'in één keer goed' onze diensten kunnen leveren;
6. de toegang tot, het gebruik van en de uitwisseling van vertrouwelijke / geheime informatie moet aantoonbaar gebonden zijn aan het vervullen van een aan onze gemeente toegewezen taak;
7. informatiebeveiliging gaat niet alleen om techniek en procedures maar vooral om mensen en gedrag, daarom ligt de verantwoordelijkheid voor informatiebeveiliging bij het lijnmanagement, met het College van B&W als eindverantwoordelijke;
8. bij samenwerking in ketens, bij uitbesteed werk of in samenwerkingsverbanden blijven we verantwoordelijk voor informatiebeveiliging. Wij zijn transparant in welke informatie wij met hen uitwisselen en welke afspraken we gemaakt hebben;
9. het toepassen van het beleid, namelijk veilig omgaan met informatie, is een zaak voor iedereen die werkt namens de gemeente. Ongeacht of deze vast of tijdelijk in dienst is of wordt ingehuurd;
10. elke medewerker weet wat informatiebeveiliging en privacy inhouden en is zich ervan bewust dat hij/zij een duidelijke eigen verantwoordelijkheid heeft. Zowel in het zelf veilig omgaan met en uitwisselen van informatie als in het melden van 'beveiligingsincidenten';
11. informatiebeveiliging vraagt om toezicht en onderhoud en is een integraal onderdeel in de bedrijfsvoering, door de verdergaande 'verSAASing' wordt het contractmanagement daarbij steeds belangrijker;
12. informatiebeveiliging vraagt onafhankelijke regie en af en toe ingrijpen in bestaande structuren, en dus centrale en onafhankelijke functionarissen;
13. door toepassing van de Eenduidige Normatiek Single Information Audit (ENSIA) legt het college jaarlijks verantwoording af aan de Gemeenteraad over informatieveiligheid (horizontaal toezicht).

[2] De software wordt dan niet aangeschaft en op de apparatuur van de gemeente geïnstalleerd. In plaats daarvan wordt met de leverancier een contract afgesloten voor het gebruik van de software op een door de leverancier beheerde locatie.

Risicobenadering
Risicomanagement vormt de kern van informatiebeveiliging binnen de gemeentelijke context. Uitgangspunt voor informatiebeveiliging is het systematisch identificeren, analyseren en behandelen van risico's die de beschikbaarheid, integriteit en vertrouwelijkheid van informatie kunnen aantasten. Voor privacy geldt dat er risicobeoordelingen moeten worden uitgevoerd om de risico's voor rechten en vrijheden van betrokkenen te beoordelen.

De Cyberbeveiligingswet richt zich op de essentiële dienstverlening. De selectie van de processen en systemen die in Rijswijk onder deze noemer vallen is bepaald aan de hand van twee criteria:

- leidt een verstoring van het proces (of systeem) tot maatschappelijke ontwrichting
- leidt een verstoring van het proces (of systeem) tot economische schade

Voor ieder van deze processen/systemen wordt een risicoinventarisatie gemaakt om te bepalen welke beveiligingsmaatregelen nodig zijn om de naleving van wet- en regelgeving, de bescherming van persoonsgegevens en de continuïteit van de betreffende processen en systemen zoveel mogelijk te borgen. De BIO is daarbij leidend. Als maatregelen uit de BIO niet of niet volledig zijn ingevoerd wordt het risico daarvan ingeschat. De proces/systeemeigenaar maakt een risicoafweging, tussen enerzijds het risico en anderzijds de kosten en consequenties van de maatregelen conform de beschermingseisen. Deze inschatting is bepalend of die risico's worden geaccepteerd of dat er aanvullende actie nodig is. De effectiviteit van de beveiligingsmaatregelen blijft primair de verantwoordelijkheid van de proces/systeemeigenaar. De risicoinschatting wordt gedocumenteerd en jaarlijks geëvalueerd.

Dataclassificatie

Dataclassificatie helpt bij het bepalen van de beveiligingsmaatregelen die nodig zijn om informatie op het juiste niveau te beschermen. De gemeente Rijswijk sluit aan bij de uitkomsten van de classificatie die is vastgelegd in het model documentair structuurplan (DSP)[3]. Proceseigenaren/systeemeigenaren kunnen afwijken van deze standaardbeoordeling door onder eigen verantwoording een classificatie uit te voeren. De uitkomst daarvan wordt geregistreerd in het DSP en is mede bepalend voor de beveiligingsmaatregelen die moeten worden toegepast voor het betreffende proces/systeem.

Als de data binnen een proces/systeem wordt geclassificeerd op het niveau midden dan voldoen de maatregelen uit de BIO. Als één van de waardes een hogere score heeft dan bepaalt de proceseigenaar (of de eigenaar van het informatiesysteem) op basis van een aanvullende risicoanalyse welke extra maatregelen genomen moeten worden.

[3] Een compleet documentair structuurplan (DSP) bevat een inventarisatie van alle processen, alle registraties en alle informatiesystemen binnen een organisatie met hun onderlinge verbanden. Per proces en registratie is vastgelegd welke informatie een rol speelt, wat de kenmerken zijn van die informatie en hoe die informatie moet worden beheerd. De kerngedachte achter het DSP is dat het binnen de organisatie geldt als Single Point of Truth (SPOT) voor processen en informatie. Het model-DSP fungeert als procesinventarisatie, als zaaktypecatalogus voor het zaaksysteem, als rubriceringsschema voor de BIO en eventueel als verwerkingsregister voor de AVG. Het DSP van Rijswijk is vastgelegd in de applicatie iNavigator.

Niveau	Vertrouwelijkheid	Integriteit	Beschikbaarheid
Geen	**Openbaar** Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.	**Niet zeker** Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.	**Niet nodig** De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.
Laag	**Bedrijfsvertrouwelijk** Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.	**Beschermd** Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-) fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van integriteit kan enige (in-)directe schade toebrengen.	**Belangrijk** De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van beschikbaarheid kan enige (in)directe schade toebrengen.
Midden	**Vertrouwelijk** Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers[4]. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.	**Hoog** Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van integriteit kan serieuze (in)directe schade toebrengen.	**Noodzakelijk** De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van beschikbaarheid kan serieuze (in)directe schade toebrengen.
Hoog	**Geheim** Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen. Weerstand tegen statelijke actoren, georganiseerde misdaad en ondermijning is noodzakelijk.	**Absoluut** Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-)fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen	**Essentieel** De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van beschikbaarheid kan (zeer) grote schade toebrengen.

[4] Onder de term ‘beperkte groep gebruikers’ in de definitie van ‘vertrouwelijk’ wordt een verzameling identiteiten met een specifieke en gemeenschappelijke taak en/of functie bedoeld; niet het lid zijn van een bepaald team of domein.

Organisatie van de informatiebeveiliging
Binnen de gemeente Rijswijk worden de verantwoordelijkheden voor informatiebeveiliging op de volgende manier verdeeld:

- De Gemeenteraad houdt 'horizontaal toezicht'.
- Het college van B en W van de gemeente Rijswijk draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor het bewerkstelligen van een passend niveau van informatiebeveiliging. Het college stelt de kaders ten aanzien van informatiebeveiliging vast, op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatiebeveiligingsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen.

  Het college ziet toe op de risico-identificatie, de inschatting van de risico's en de toegepaste beveiligingsmaatregelen.

- Het gemeentelijk managementteam (GMT) adviseert het college over de te stellen kaders en is verantwoordelijk voor de nadere uitwerking van het informatiebeveiligingsbeleid binnen die kaders en de sturing daarop.
  Het GMT:
  - draagt zorg voor het risicomanagementproces op organisatieniveau. Ze zorgen ervoor dat er een goed gedefinieerd risicobeheerproces bestaat en dat de belangrijkste risico's adequaat worden beheerd;
  - controleert of de getroffen maatregelen overeenstemmen met de betrouwbaarheidseisen en of deze voldoende bescherming bieden;
  - evalueert periodiek beleidskaders en stelt deze waar nodig bij;
  - zorgt dat voor alle processen en (ketens van) informatiesystemen een domein-/teammanager als eigenaar is aangewezen.
- De domein-/teammanagers zijn verantwoordelijk voor de integrale beveiliging van de informatie binnen hun bestuurlijke opdracht/team. De domein-/teammanager:
  - Identificeert de risico's van de in de bestuurlijke opdracht/het team gebruikte systemen en processen en implementeert de nodige risicobeheersmaatregelen. Dit kan door middel van de uitvoering van risicobeoordelingen en het nemen van passende actie. Ze houden hierbij rekening met factoren zoals prioriteit, beschikbare middelen en de capaciteit om maatregelen effectief uit te voeren;
  - is verantwoordelijke voor de keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
  - stuurt op beveiligingsbewustzijn, bedrijfscontinuïteit en naleving van regels en richtlijnen;
  - zorgt ervoor dat toegangscontrole en de beveiliging van bedrijfsmiddelen en persoonsgegevens effectief wordt uitgevoerd. Dit omvat het implementeren van passende toegangsbeperkingen en het monitoren van deze toegang;
  - rapporteert over compliance aan wet en regelgeving;
  - is verantwoordelijk voor het invullen van de vragenlijsten die nodig zijn voor de zelfevaluatie in het kader van de ENSIA.
- De adviseur informatiebeveiliging (CISO) is onafhankelijk van de lijn gepositioneerd, door het college aangesteld en kan escaleren indien nodig. De adviseur informatiebeveiliging (CISO) heeft een adviserende functie en controleert tevens op de uitvoering van het IB beleid van de gemeente:
  - Ontwikkelen van visie en beleid op informatie beveiliging;
  - uitwerking daarvan in een informatiebeveiligingsplan
  - IB-planning en control voorbereiden;
  - Coördineren en evalueren incidenten;

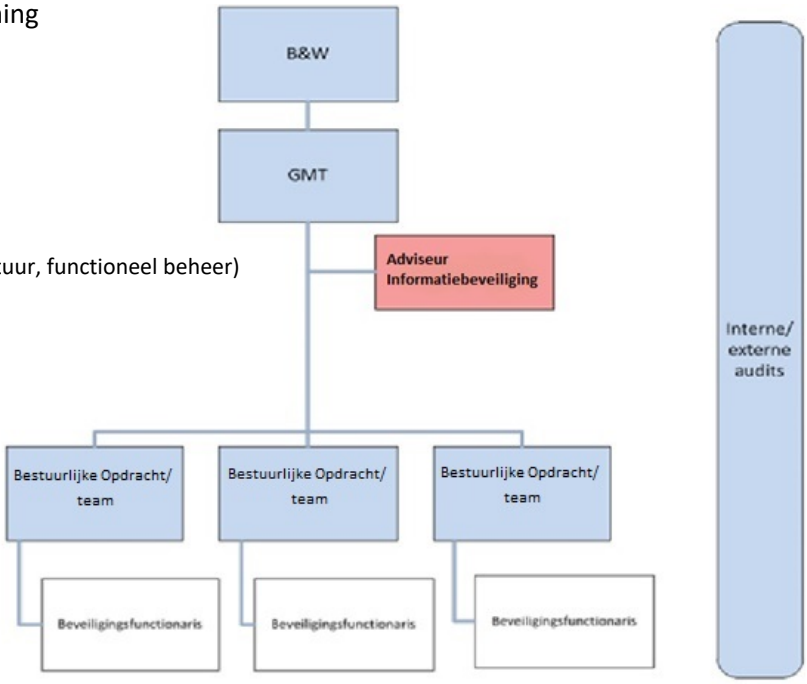
- Communicatie eindgebruikers informatiebeveiliging;
- Juist afhandelen van incidenten;
- Adviserende rol voor GMT en teammanagers.

- De functionaris gegevensbescherming (FG) is de interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de Algemene verordening gegevensbescherming.
-

  De functionaris gegevensbescherming:
  - adviseert organisatiebreed over privacybescherming en over activiteiten ter bescherming van persoonsgegevens;
  - geeft aanwijzingen aan gebruikers van systemen over de correcte handelswijze bij persoonsregistraties;
  - brengt gevraagd of ongevraagd advies uit over alle procedures en producten die betrekking hebben op de registratie van personen;
  - fungeert binnen de gemeente als contactpersoon voor de Autoriteit Persoonsgegevens (AP).
- De beveiligingsfunctionaris is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures (voor het aan hem/haar toegewezen deelgebied) die voortkomen uit het informatiebeveiligingsbeleid en het onderliggende Informatiebeveiligingsplan. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons. De medewerker coördineert de toepassing van specifieke wet- en regelgeving. De beveiligingsfunctionaris rapporteert aan diens teammanager en aan de adviseur Informatiebeveiliging. In het kader van de ENSIA vult de beveiligingsfunctionaris de vragenlijsten in die nodig zijn voor de zelfevaluatie.

  Binnen wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden, ten aanzien van specifieke methodes van gegevensverzameling. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan de beveiligingsfunctionaris.

  De deelgebieden waarbij een beveiligingsfunctionaris is aangewezen zijn de volgende:
  - Publieke dienstverlening
    - BRP
    - Reisdocumenten
    - Rijbewijzen
  - Sociaal Domein
    - SUWI
  - Informatie
    - ICT (advies, architectuur, functioneel beheer)
    - BAG
    - BGT
    - BRO
    - DM
  - HRM
  - Facilitaire Zaken
  - Juridische Zaken



Team Uitvoering Informatieveiligheid

Elk kwartaal is er een overleg over ontwikkelingen en gebeurtenissen op het gebied van informatieveiligheid binnen de gemeente Rijswijk. Hiervoor is het team uitvoering informatieveiligheid ingesteld. Binnen dit overleg worden de activiteiten die nodig zijn voor de implementatie van de BIO en eventuele aanvullende maatregelen afgestemd en gemonitord. In dit team worden ook afspraken gemaakt om tot een tijdige en volwaardige verantwoording volgens de ENSIA te komen. De kern van het team wordt gevormd door de beveiligingsfunctionarissen van de deelgebieden Publieke Dienstverlening, Sociaal Domein en Informatie en door de adviseur informatieveiligheid (tevens voorzitter van dit overleg). Facultatief sluiten de beveiligingsfunctionarissen van de deelgebieden HRM, Facilitaire Zaken en Juridische Zaken en de privacyfunctionarissen bij dit overleg aan.

Dienstverlening door de Gemeenschappelijke Regeling Bedrijfsvoering Delft-Rijswijk

Technisch IT-beheer is uitbesteed aan de Gemeenschappelijke Regeling Bedrijfsvoering Delft-Rijswijk (GR). Uitgangspunt is dat de gemeente Rijswijk voor zover mogelijk en relevant de (technische)beveiligingsrichtlijnen van de GR volgt. In de meeste gevallen zullen deze richtlijnen ook gelden voor de gemeente Rijswijk.
De gemeente Rijswijk blijft als gemeente zelf verantwoordelijk voor haar eigen beveiligingsbeleid. Daardoor zijn er eisen te stellen aan de beveiliging op systemen en applicaties van de gemeente Rijswijk om beschikbaarheid en continuïteit van de eigen Rijswijkse dienstverlening te waarborgen. Deze eisen en beleidsuitgangspunten hebben uitsluitend betrekking op het uitvoeren van de IT Dienstverlening door de GR.
De (beveiligings-) afspraken en de service levels worden namens de gemeente Rijswijk bewaakt door de aangestelde Service Level Manager in samenspraak met de Servicemanager(s) en security officer(s)van de andere deelnemer(s) in de GR, de security officer van de GR en de adviseur informatiebeveiliging van Rijswijk.
Beleidsuitgangspunten vanuit de gemeente Rijswijk:

1. De GR heeft een op de BIO gebaseerd beveiligingsbeleid en geëffectueerde maatregelen, die zij aan de gemeente Rijswijk inzichtelijk maakt.
2. De GR is verantwoordelijk voor een correcte inrichting van het beleid en naleving hiervan binnen de eigen organisatie. De GR voldoet aan de normen en eisen die gesteld zijn in het Informatiebeveiligingsbeleid en de van toepassing zijnde wet- en regelgeving.
3. Binnen de GR is een Security Officer aanwezig die verantwoordelijk is voor het Informatiebeveiligingsbeleid van de GR en die contactpersoon is voor de adviseur informatiebeveiliging van de gemeente Rijswijk.
4. De normen en eisen aangaande de beveiliging maken onderdeel uit van de dienstverleningsovereenkomst (DVO) en verwerkersovereenkomst, die tussen de gemeente Rijswijk en de GR afgesproken is.
5. De GR stelt uitsluitend in opdracht van de gemeente Rijswijk gegevens en systemen van de gemeente Rijswijk beschikbaar aan medewerkers uit de gemeente, de GR en aan derde partijen.
6. De GR stelt capaciteit en informatie beschikbaar voor audits, die in opdracht van de gemeente Rijswijk uitgevoerd worden.

De kwaliteitscyclus

Informatiebeveiliging vraagt om continue verbetering. Deze kwaliteitscyclus begint met de vaststelling van het informatiebeveiligingsbeleid. Dit wordt minimaal één keer per drie jaar beoordeeld en zo nodig bijgesteld. Binnen deze 3-jaarlijkse cyclus wordt een actieplan (informatiebeveiligingsplan) opgesteld, daarbij wordt de uitkomst van de zelfevaluatie in de ENSIA gebruikt. Dit plan wordt ieder jaar opnieuw beoordeeld en zo nodig herzien. Voor proces specifieke activiteiten wordt zo nodig een specifiek plan opgesteld door de proceseigenaar.

De (voortgang van de) uitvoering van de verbeteracties uit het plan wordt gemonitord en periodiek gerapporteerd aan het GMT. Het daadwerkelijke effect van de inspanningen op het gebied van informatiebeveiliging wordt getoetst binnen het proces (incidentregistratie, verbetervoorstellen). Maar ook in de vorm van controles van 'buiten het proces': door onafhankelijke interne/externe auditors en externe toezichthouders (rijksoverheid voor basisregistraties, accountant). Met welke frequentie en door wie is afhankelijk van de risico's en wetgeving voor het betreffende proces of informatiesysteem.

Het college rapporteert bij de jaarrekening over de uitvoering van het informatiebeveiligingsbeleid (conform de ENSIA). Op deze manier kan de raad haar verantwoordelijkheid voor 'horizontaal toezicht' invullen.

Kwaliteitssysteem

De kwaliteitscyclus wordt vastgelegd in het kwaliteitssysteem, ook wel information security management system (ISMS) genoemd. Dit is geen fysiek systeem, maar een zorgvuldig beheerste verzameling van vastgelegde processen, procedures en andere beheersmaatregelen (organisatorische, personele of technische maatregelen). Ook de vastlegging van de risico-afweging en het besluit over de beheersmaatregelen zullen in dit systeem worden opgenomen.