Strategisch Beleidskader

Informatiebeveiliging Concern
Gemeente Rotterdam



2024 - 2026

Gemeente Rotterdam

Gemeente Rotterdam

Strategisch beleidskader

Informatiebeveiliging Concern

2024-2026

Van:	CISO-team
Datum:	9 januari 2024
Cluster:	Bestuurs- en Concernondersteuning
Afdeling:	IIFO/CIO-Office

Inhoudsopgave

Voorwoord		**3**
1	**Inleiding**	**4**
2	**Aanleiding/context**	**6**
2.1	Leeswijzer	6
2.2	Wat is informatiebeveiliging?	6
2.3	Scope van het Concern Informatiebeveiligingsbeleid	7
2.4	Dreigingslandschap gemeente Rotterdam	8
2.5	Doelstellingen Concern Informatiebeveiligingsbeleid	9
2.6	Doelgroepen	9
2.7	Besluitvorming	10
3	**Uitgangspunten voor informatiebeveiliging**	**11**
3.1	Bestuurlijke principes informatiebeveiliging	11
3.2	Wet- en regelgeving	12
3.3	Normen en standaarden	13
3.4	Strategisch risicomanagement informatiebeveiliging	14
3.5	Raakvlakken met organisatie domeinen	14
3.6	Verhogen Digitale Weerbaarheid	16
4	**Organisatie van informatiebeveiliging**	**18**
4.1	De informatiebeveiligingsorganisatie	18
4.2	Managementsysteem voor informatiebeveiliging (ISMS)	19
4.3	Controle en verantwoording	21
4.4	Afwijkingen van de informatiebeveiligingsprincipes	22
Bijlage A: Relevante documenten en bronnen		**23**
Bijlage B: Overige gebruikte afkortingen		**25**



Voorwoord

Het Concern Informatiebeveiligingsbeleid van de gemeente Rotterdam heeft als doel het beschermen van de gemeentelijke informatie, waaronder informatie van burgers, ondernemers en ketenpartners, het beschermen van de infrastructurele objecten met een ICT-component en toepassing van de relevante wet- en regelgeving. Het uitgangspunt bij deze bescherming betreft zowel effectieve omgang met beveiligingsuitdagingen die voortkomen uit een voortdurend veranderend dreigingslandschap, als het minimaliseren van risico's in de dienstverlening en bedrijfsvoering. Het college van B en W hecht grote waarde aan informatieveiligheid en verwacht dat iedere werknemer zich individueel verantwoordelijk voelt voor het veilig omgaan met informatie en objecten.

Dit strategische informatiebeveiligingsbeleid is kaderstellend en richtinggevend ten aanzien van informatieveiligheid van de gemeente Rotterdam en dient als leidraad voor de uitwerking op tactisch en operationeel niveau zoals beleidsstukken, procedures en werkinstructies die gerelateerd zijn aan het vakgebied van informatieveiligheid.

Onze ambities voor informatieveiligheid zijn als volgt:

- We willen een aantoonbaar betrouwbare partner zijn voor de burgers, ondernemers en ketenpartners van de gemeente Rotterdam op het gebied van informatieveiligheid.
- We zullen informatiebeveiliging professioneel inrichten in de gemeentelijke organisatie, waarbij we rekening houden met onze verantwoordelijkheid als eigenaar, leverancier en/of afnemer van gegevens.
- We zullen de gegevens van burgers en ondernemers op een veilige manier verwerken door het implementeren van organisatorische en technische beveiligingsmaatregelen, zoals vereist door wet- en regelgeving, waaronder de Algemene Verordening Gegevensbescherming (AVG), de Wet basisregistratie personen (BRP) en de Baseline Informatiebeveiliging Overheid (BIO).
- We zorgen voor de beveiliging van operationele technologie, industriële automatisering en procesautomatisering binnen de gemeente Rotterdam door te voldoen aan de BIO in samenhang met de Cyber Security Implementatie Richtlijn Objecten (CSIR).
- We dragen bij aan het voorkomen en bestrijden van digitale criminaliteit en ondersteunen de samenleving bij het optreden van digitale incidenten.
- We integreren ons informatiebeveiligingsbeleid in verschillende veiligheidsgebieden en werken nauw samen.

Het Concern Informatiebeveiligingsbeleid draagt bij aan het begrip dat niet alle elementen van informatieveiligheid volledig kunnen worden gecontroleerd. Dit begrip stelt ons in staat om te focussen op gebieden waar controle en invloed mogelijk zijn, die gepaard gaan met robuuste bescherming en voorbereiding tegen bekende dreigingen. Tegelijkertijd begrijpen we dat nieuwe, onvoorziene dreigingen kunnen ontstaan, waarvoor we voortdurend weerbaarheid en response moeten blijven ontwikkelen.



1 Inleiding

Onze samenleving digitaliseert snel en als gemeente passen wij onze dienstverlening aan op deze mogelijkheden. Ook de Rotterdammer benut volop de mogelijkheden van nieuwe digitale middelen. Tegelijkertijd brengen toenemende nieuwe mogelijkheden van technologie en de voortdurende digitalisering van onze diensten een groeiende complexiteit met zich mee. Dit heeft impact op het gebied van effectieve en verifieerbare informatiebeveiliging van zowel de dienstverlening als de bedrijfsvoering. De complexiteit manifesteert zich met nieuwe dreigingen bij verschillende aspecten, zoals de technische infrastructuur, applicaties, processen en het gebruik van informatie. Het vergt een doortastende aanpak om ervoor te zorgen dat onze informatiebeveiliging bij deze aspecten gelijke tred kan houden met steeds veranderende dreigingen.

In verschillende wet- en regelgeving worden de eisen aan informatieveiligheid aangescherpt. Toezichthouders stellen meer en hogere eisen aan aantoonbare informatiebeveiliging. Vraagstukken met betrekking tot de digitale veiligheid worden door wetgeving steeds meer gekoppeld aan de verantwoordelijkheden van eigenaren, zoals de bronhouders. Hierbij zijn zowel interne als externe partijen en toezichthouders betrokken. Het is verplicht om de juridische aspecten, zoals bij aanbestedingen en in contracten met leveranciers, af te stemmen op de gewenste en noodzakelijke informatieveiligheid van de gemeente. Ook bij de uitwisseling van gegevens met samenwerkingsverbanden en ketenpartners moeten de juiste maatregelen worden getroffen om risico's als datalekken te voorkomen. Het is van toenemend belang om als gemeente het overzicht en de controle te behouden over onze toeleveringsketen. Dit met het doel om de afhankelijkheden in de keten voor onze bedrijfskritische informatiesystemen te beheersen. Wereldwijde incidenten hebben aangetoond dat juist deze keten potentiële risico's meebrengt voor de continuïteit van onze bedrijfsvoering. Enkele voorbeelden hiervan zijn: het misbruik van kwetsbaarheden in software (zoals Citrix[1] en Log4J[2]) en ransomware aanvallen (zoals bij gemeente Antwerpen, Buren, Hof van Twente, de Bibliotheek Rotterdam, en de Universiteit Maastricht).

In de snel digitaliserende wereld van vandaag, waar Kunstmatige Intelligentie (AI) een steeds grotere rol speelt, wordt het steeds complexer om echte informatie te onderscheiden van valse informatie. Dit heeft wereldwijd geleid tot problemen zoals nepnieuws, deepfakes, vermoedelijke inmenging in verkiezingen en het stelen van digitale identiteiten. Het is van cruciaal belang om de identiteit van gebruikers en apparaten te waarborgen, aangezien dit de basis vormt voor veilige toegang tot essentiële diensten en informatiesystemen.

Het Concern Informatiebeveiligingsbeleid geeft de strategie en kaders voor de gemeentelijke informatiebeveiliging. Uitwerkingen voeden het meerjarenplan informatiebeveiliging, welke onder regie van de Chief Information Security Officer (CISO) wordt uitgevoerd. Er wordt een duurzame beveiligingsarchitectuur ontwikkeld en onderhouden, zodat het zich aanpast aan de veranderende dreigingen.

[1] Citrix, wereldwijd incident | De impact van één beveiligingslek | Kwetsbaarheid | NCSC Magazine
[2] Log4J incident| Actief misbruik van kwetsbaarheid in Apache Log4j 2 | Digital Trust Center (Min. van EZK)

Vanwege de ontwikkelingen inzake informatieveiligheid in de afgelopen beleidsperiode (2021-2023) is vaststelling van het geactualiseerde Concern Informatiebeveiligingsbeleid voor de periode 2024-2026 nodig. Het Concern Informatiebeveiligingsbeleid geeft richting aan de Rotterdamse informatiebeveiligingsaanpak, waarbij de belangrijkste doelen zijn om te voldoen aan wet- en regelgeving en effectief om te gaan met beveiligingsuitdagingen die voortkomen uit een voortdurend veranderend dreigingslandschap. Tevens zal het Concern Informatiebeveiligingsbeleid het clustermanagement ondersteunen bij hun verantwoordelijkheid voor het veilig houden van dienstverlening aan Rotterdammers en ondernemers.



2 Aanleiding/context

Het Concern Informatiebeveiligingsbeleid is als strategisch beleid **kaderstellend en richtinggevend** voor de informatieveiligheid van de gemeente Rotterdam. Het geeft de kaders voor de ontwikkeling van onderwerpspecifieke documenten op tactisch niveau, waaronder specifiek de uitwerking van de beleidsnormen uit de Baseline Informatiebeveiliging Overheid (BIO). Daarnaast is het Concern Informatiebeveiligingsbeleid richtinggevend voor de inrichting op operationeel niveau met betrekking tot informatiebeveiligingsprocessen en -werkinstructies.

2.1 Leeswijzer

Het Concern Informatiebeveiligingsbeleid is als volgt opgebouwd:

- Hoofdstuk 2 behandelt het dreigingsbeeld en de uitgangspunten en strategische principes van informatiebeveiliging binnen de gemeente Rotterdam.
- Hoofdstuk 3 zet de kern van het strategisch beleid uiteen, benadrukt de raakvlakken met andere domeinen binnen het Concern en beschrijft hoe de weerbaarheid verhoogd wordt.
- Hoofdstuk 4 beschrijft de verantwoordelijkheden en de organisatie van informatiebeveiliging binnen de gemeente Rotterdam.

Het Concern Informatiebeveiligingsbeleid is in lijn met:

- het VNG-manifest 'De tien bestuurlijke principes voor informatiebeveiliging' (2019);
- het 'Concern Integraal Beveiligingsbeleid' (Directie Veiligheid, nov. 2020);
- de VNG-resolutie 'Digitale Veiligheid: kerntaak voor de gemeenten' (VNG, feb. 2021);
- het 'Bestuurlijk convenant digitale veiligheid gemeenten' (VNG, dec 2022);
- de 'Kadernota Sturen en Verantwoorden Rotterdam 2023' (okt. 2023).

2.2 Wat is informatiebeveiliging?

Informatiebeveiliging omvat de processen en maatregelen die zijn ingericht om de **betrouwbaarheid** van gemeentelijke processen, informatiesystemen en de daarin opgeslagen gegevens, zowel digitaal als analoog (tekst, video, geluid) te waarborgen en te beschermen tegen mogelijke schade, zowel opzettelijk als onopzettelijk veroorzaakt.
Deze betrouwbaarheid betreft de aspecten:

- Beschikbaarheid **(B)** / continuïteit: ervoor zorgen dat informatie en informatieverwerkende (bedrijfs)middelen beschikbaar zijn voor de gebruikers op de juiste tijd en op de juiste plaats.
- Integriteit **(I)** / juistheid: waarborgen van de juistheid, correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking.
- Vertrouwelijkheid **(V)** / exclusiviteit: het beschermen van informatie tegen ongeautoriseerde verwerking (kennisname, muteren, verwijderen).

Deze indeling van **betrouwbaarheid** wordt aangeduid met de afkorting **BIV.**

Informatiebeveiliging borgt de betrouwbaarheid met **beveiligingsmaatregelen** tegen bedreigingen en risico's ter voorkoming en vermindering van:

- ongewenst verlies van informatie, zowel tijdelijk als permanent;
- ongewenste corruptie van informatie, zowel bewust als onbewust;
- ongewenste openbaarmaking van informatie, zowel bewust als onbewust.

Normen voor informatiebeveiligingsmaatregelen worden in de BIO versie 1.4[3] omschreven op vier verschillende niveaus die bekend staan als de **Basis Beveiliging Niveaus** (BBN). Voor elk gedefinieerd bedrijfsbelang wordt het juiste niveau van passende[4] BIV-maatregelen vastgesteld om een adequate bescherming te bieden tegen de geïnventariseerde dreigingen.

De gemeente Rotterdam voldoet standaard aan het BBN2. Als er vanwege mogelijke dreigingen voor de te beschermen bedrijfsbelangen (TBB)[5] een hoger BBN-niveau wordt vereist, (zoals BBN2+ of BBN3) dan zal via een diepgaande risicoanalyse worden bepaald welke aanvullende passende BIV-maatregelen getroffen moeten worden om de geïdentificeerde risico's te minimaliseren.

2.3 Scope van het Concern Informatiebeveiligingsbeleid

Het Concern Informatiebeveiligingsbeleid volgt de uitgangspunten voor informatieveiligheid zoals vastgesteld door de Vereniging van Nederlandse Gemeenten (VNG) en de aanvullende beveiligingseisen die voortvloeien uit wet- en regelgeving.

Het Concern Informatiebeveiligingsbeleid is van toepassing op een breed scala van situaties en entiteiten binnen de gemeente Rotterdam, namelijk op:

- **Alle informatie** waarvan de gemeente Rotterdam de eigenaar, de leverancier en/of de afnemer is.
- Alle informatie die wordt **verwerkt** door de processen en onderliggende informatie-systemen van de gemeente, (keten)partners, samenwerkingsverbanden en/of diensten;
- Alle informatie in de dienstverlening die **door externe partijen** wordt verwerkt namens gemeente Rotterdam.
- **Alle processen** van de gemeente. Dit borgt dat de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de gebruikte technologie en de aard van de informatie, voldoet aan de normen en standaarden van informatiebeveiliging.
- De infrastructurele objecten met een ICT-component, waarvan de gemeente Rotterdam de eigenaar, de leverancier en/of de afnemer is.
- De **locatie-onafhankelijkheid.** Dit betreft alle werklocaties en werkplekken (inclusief thuiswerkplek) die werknemers gebruiken voor hun werkzaamheden.
- Tot slot beperkt het zich niet alleen tot de technische aspecten van ICT, informatie en objecten maar heeft het ook betrekking op de **organisatorische aspecten,** waaronder bestuur, management, alle werknemers, leveranciers, bezoekers en externe relaties.

Er zijn **verschillende domeinen** met inhoudelijke aspecten van informatieveiligheid. Deze domeinen moeten voldoen aan de informatiebeveiliging en -normen van het Concern Informatiebeveiligingsbeleid. Het domein privacy, waar persoonsgegevens worden beschermd door middel van passende organisatorisch en technische

[3] Staatscourant 2020, 7857 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)
[4] Passend volgens de NORA definities | Passend beschermingsniveau, proportioneel en subsidiair - NORA Online
[5] Zie integraal beveiligingsbeleid

beveiligingsmaatregelen, heeft een groot raakvlak met informatieveiligheid. Andere domeinen met relevante raakvlakken zijn beschreven in paragraaf 3.6. Het is hierbij belangrijk om op te merken dat de beleidsmatige aspecten van deze domeinen, zoals bepaald in relevante wet- en regelgeving, buiten de scope vallen van dit Concern Informatiebeveiligingsbeleid.

2.4 Dreigingslandschap gemeente Rotterdam

De gemeente Rotterdam heeft te maken met een voortdurend veranderend dreigingslandschap. De arena rondom digitale aanvallen wordt niet alleen groter en intensiever, maar ook complexer. Mensen, informatiesystemen en apparaten zijn via netwerken op verschillende manieren met elkaar verbonden ('internet of everything'). In al deze verbindingen kunnen beveiligingsproblemen ontstaan. Dit kan bewust of onbewust schade veroorzaken aan de informatievoorziening van de gemeentelijke organisatie, de werknemers of de burger.

De digitale dreiging is permanent en door steeds verdergaande digitalisering groeien zowel de aanvalsmogelijkheden van de actoren als het aantal actoren. Vanuit het perspectief van nationale veiligheid zijn de voornaamste dreigingen gerelateerd aan (de voorbereidingen voor) sabotage, spionage en het beïnvloeden van verkiezingen. Statelijke actoren maken vaak misbruik van actualiteiten, zoals bij een pandemie, een ramp, oorlogsdreigingen en politieke verkiezingen. Dreigingen vanuit criminele actoren zijn hoofdzakelijk te doen om financieel gewin.

Digitale incidenten en beveiligingsproblemen kunnen leiden tot maatschappij-ontwrichtende schade, (grootschalige) uitval van digitale diensten, processen, infrastructurele objecten of systemen. Naast digitale dreigingen van buitenaf, vormt het informatieveilig gedrag van werknemers bewust of onbewust ook een dreiging met impact op de gemeentelijke informatievoorziening.

Het onderkennen en kunnen herkennen van dreigingen is randvoorwaardelijk voor een snelle en effectieve respons. Om goede risicoafwegingen te kunnen maken en te kunnen prioriteren in de te treffen maatregelen, moet duidelijk zijn wat de meest relevante dreigingen zijn. Het Dreigingsbeeld Informatiebeveiliging Gemeente Rotterdam biedt hier inzicht in.[6] Het dreigingsbeeld en de onderliggende dreigingsanalyses die hier periodiek op worden gedaan, stelt de gemeente beter in staat om haar kennis, aandacht en middelen te besteden aan de belangrijkste dreigingen en kwetsbaarheden.

Gezien de mondiale ontwikkelingen van de dreigingen is stilstaan met informatiebeveiliging een groot risico voor de gemeente. De informatiebeveiligingsorganisatie heeft continu werk aan het monitoren van de dreigingen om zo incidenten en datalekken te voorkomen die potentieel aanzienlijke schade voor Rotterdam zouden kunnen betekenen.

Het is onmogelijk om incidenten volledig te voorkomen. Wat we wél kunnen doen is weerbaarder worden en weten hoe we moeten handelen als een digitaal incident de gemeente treft. Hiermee kunnen we de negatieve gevolgen zo klein mogelijk proberen te houden. Goed voorbereid zijn, klaarstaan en alertheid vormen de kern van de veerkracht van de gemeente Rotterdam op het gebied van informatiebeveiliging. Deze veerkracht en weerbaarheid omvatten de activiteiten en maatregelen welke nodig zijn om netwerken, (keten-)informatiesystemen, infrastructurele objecten, gebruikers van dergelijke systemen, en personen die getroffen kunnen worden te beschermen tegen de dreigingen.

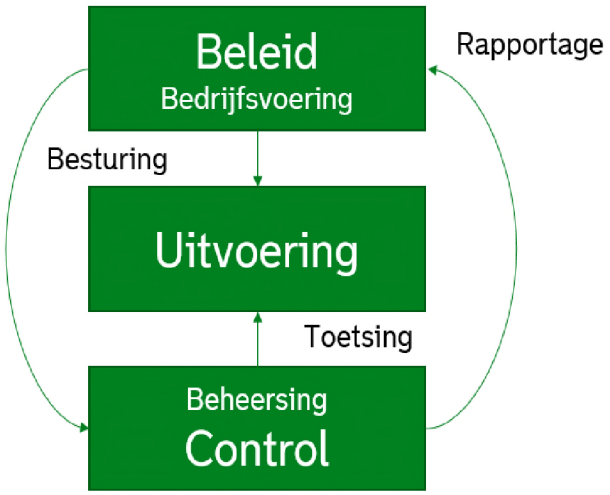
[6] Dreigingsbeeld Informatiebeveiliging Gemeente Rotterdam | Dreigingsbeeld (rotterdam.nl)

2.5 Doelstellingen Concern Informatiebeveiligingsbeleid

De hoofddoelen van het Concern Informatiebeveiligingsbeleid zijn:

- het voldoen aan wet- en regelgeving;
- het beschermen van de gemeentelijke informatie, waaronder informatie van burgers, ondernemers en ketenpartners en infrastructurele objecten met een ICT-component;
- het eenduidig beschrijven en laten vaststellen van de uitgangspunten voor informatieveiligheid in de gemeente;
- het effectief omgaan met de beveiligingsuitdagingen die voortkomen uit het voortdurende wijzigende dreigingslandschap;
- het beheren van risico's en treffen van de juiste maatregelen om de informatie adequaat te beveiligen tegen digitale en fysieke invloeden.

Om deze doelen te bereiken, heeft de gemeente Rotterdam een geformaliseerd en gestructureerd Meerjarenplan Informatiebeveiliging. Dit bevat een overzicht en prioritering van alle trajecten, projecten en activiteiten tot en met 2026. Deze zijn uitgewerkt langs de indeling van 'beleid', 'uitvoering' en 'control' (kortweg BUC). De BUC-methode wordt gebruikt in de BIO, de BIO thema's en diverse normeringen van informatiebeveiliging en is het ondersteunende raamwerk voor het informatiebeveiligingsbeleid.



2.6 Doelgroepen

Het Concern Informatiebeveiligingsbeleid is een kader voor iedereen binnen en buiten de gemeentelijke organisatie. In onderstaande tabel zijn de doelgroepen weergegeven inclusief hun taken en verantwoordelijkheden met betrekking tot informatieveiligheid en verwijzingen naar onderliggende bronnen waarin dit is vastgesteld.

Doelgroep	Relevantie
College van burgemeester en wethouders	Draagt integrale verantwoordelijkheid om de gemeentelijke informatiehuishouding veilig te organiseren (1) en (4). Het bevorderen van een veilige cultuur (4).
Gemeentesecretaris	Draagt de eindverantwoordelijkheid voor het beveiligingsbeleid en voor de uitvoering van organisatiebrede vraagstukken met betrekking tot informatiebeveiliging (2).

Proceseigenaren	Zijn verantwoordelijk voor de beveiliging van het specifieke proces, de data en informatiesystemen en/of objecten horende bij het proces (2) en voor een zodanige inrichting van het proces dat de kwaliteit van producten en diensten die met het proces worden geleverd kunnen voldoen aan de normen (3). De proceseigenaar is ook systeem-eigenaar en data-eigenaar (3).
Proceseigenaren in relatie met BCO-eigenaarschap	De proceseigenaar is eigenaar van de geautomatiseerde systemen die bij het uitvoeren van het proces worden gebruikt en de data die daartoe worden verwerkt, met uitzondering van geautomatiseerde systemen die concernbreed worden gebruikt en waarvan de directeur BCO de eigenaar is (3).
Clustermanagement	Het management van de clusters is integraal verantwoordelijk voor de inrichting en uitvoering van haar processen (inhoud, mensen en middelen) (3).
Informatiebeveiligings-functionarissen	Voor het invullen van integraal management worden de managers vanuit expertise ondersteund door het cluster BCO op de gebieden financiën, inkoop, HR, ICT, facilitaire zaken, huisvesting, privacy, security, informatiehuishouding, fiscaal, juridisch en communicatie. Deze ondersteuning bestaat uit dienstverlening in de vorm van uitvoeren, adviseren, bewaken, signaleren en regisseren op het gebied van de bedrijfsvoering (3).
Functionarissen Beheer (functioneel, technisch, web)	Hebben de verantwoordelijkheid om de beheermaatregelen voor hun informatie en informatiesystemen te beheren en te beheersen (2).
Financial Audit en Concern Auditing	Stellen vanuit een onafhankelijke positie vast of doelstellingen zijn gerealiseerd, of er doelmatig en rechtmatig is gehandeld en of er betrouwbaar wordt gerapporteerd (3).
Dienstenleveranciers	Zijn externe organisaties in de markt waaraan de gemeentesecretaris of proceseigenaar een (deel van) de beveiligingstaak in- of uitbesteedt (2). Dienstenleveranciers leggen verantwoording af aan hun opdrachtgever (2).
Werknemers	Passen de regels en procedures aangaande informatiebeveiliging toe (2). Informatieveiligheid is van iedereen (1 en 4).

Legenda bronnen informatieveiligheid:
(1) De VNG-resolutie 'Digitale Veiligheid: kerntaak voor de gemeenten' (VNG, feb. 2021)
(2) BIO, versie 1.4, 2020
(3) Kadernota 'Sturen en Verantwoorden Rotterdam 2023'
(4) Het VNG-manifest "de tien bestuurlijke principes voor informatiebeveiliging" (2019)

2.7 Besluitvorming

Het Concern Informatiebeveiligingsbeleid voor de periode 2024-2026 is vastgesteld door het college van B en W. Het vorige Concern Informatiebeveiligingsbeleid (periode 2021-2023) is ingetrokken. Uiterlijk in 2026 wordt het Concern Informatiebeveiligingsbeleid, waar nodig, gewijzigd en opnieuw ter vaststelling aangeboden. Indien een nieuw, dan wel gewijzigd, Concern Informatiebeveiligingsbeleid nog niet is vastgesteld, blijft het huidige Concern Informatiebeveiligingsbeleid van kracht.

Jaarlijks wordt via het ENSIA-verantwoordingsproces gerapporteerd aan zowel het college van B en W als aan de gemeenteraad over de status van informatieveiligheid van de gemeente. Hierbij wordt het informatiebeveiligingsbeleid getoetst op effectiviteit en actualiteit.

3 Uitgangspunten voor informatiebeveiliging

Dit hoofdstuk beschrijft de belangrijkste uitgangspunten voor informatiebeveiliging die van toepassing zijn binnen de gemeente Rotterdam. Informatiebeveiliging is het middel om het bestuurlijke beleidsdoel informatieveiligheid vorm te geven. De uitgangspunten voor informatiebeveiliging omvatten:

- Bestuurlijke principes
- Wet- en regelgeving
- Normen en standaarden
- Strategische risicomanagement

Het Concern Informatiebeveiligingsbeleid benadrukt dat informatiebeveiliging geen op zichzelf staand thema is. Informatiebeveiliging is één van de kwaliteitsaspecten van informatievoorziening en mede daardoor nauw verweven met andere domeinen binnen de gemeente. Bovendien wordt de cruciale rol van een informatieveilige cultuur en bewustwording van informatiebeveiliging benadrukt.

3.1 Bestuurlijke principes informatiebeveiliging

Het Concern Informatiebeveiligingsbeleid is gebaseerd op het VNG-manifest '*De tien bestuurlijke principes voor informatiebeveiliging*'[7]. Deze principes betreffen de bestuurlijke aanvulling op de BIO en benadrukken de waarden die door bestuurders worden gehanteerd en uitgedragen.

De informatiebeveiligingsprincipes uit het VNG-manifest dienen als algemene uitgangspunten die ten grondslag liggen aan de inrichting van de gemeentelijke organisatie. Ze zijn universeel van toepassing en ze vormen zo de uitgangspunten voor het bestuur, directie en management, het Concern Informatiebeveiligingsbeleid, de inrichting en werkwijze voor informatiebeveiliging van de gemeente. De gemeente Rotterdam stelt aanvullende bestuurlijke afspraken voor informatiebeveiliging:

1. **Proceseigenaren en clustermanagement**
   - ✓ zijn eindverantwoordelijk voor het uitvoeren van risicoanalyses voor het beveiligen van hun processen, informatiesystemen, gegevens, webapplicaties en/of objecten;
   - ✓ bepalen op basis van de informatiebeveiligingsrisico's de risicobereidheid om de doelstellingen van de organisatie te behalen;
   - ✓ leggen verantwoording af over gemaakte keuzes als risicovolle situaties niet volledig worden afgedekt met beveiligingsmaatregelen, dit vereist expliciete besluitvorming;
   - ✓ zijn eindverantwoordelijk om de maatregelen voor informatiebeveiliging te implementeren en te onderhouden waarmee de risico's worden verminderd tot een voor de gemeente acceptabel niveau;
   - ✓ dragen het Concern Informatiebeveiligingsbeleid uit, inclusief de daaruit voortkomende uitwerkingen, richtlijnen en werkinstructies.

[7] VNG-manifest | https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf

2. Een belangrijk principe van informatiebeveiliging is **security-by-design**. Dit principe houdt in dat passende informatiebeveiligingsmaatregelen in een zo vroeg mogelijk stadium worden geïntegreerd bij het ontwikkelen en implementeren van nieuwe processen, applicaties en innovaties (bijvoorbeeld met AI, algoritmes en chatbots). De gemeente houdt hierbij rekening met bestaande en toekomstige dreigingen en het benoemen en mitigeren van de beveiligingsrisico's. Bij het toepassen van dit uitgangspunt werkt de gemeente Rotterdam zowel **norm- als risicogebaseerd.**
3. Bij het toepassen van bestuurlijke principes moet altijd worden gezocht naar een goede **balans** tussen informatieveiligheid, gebruiksvriendelijkheid (werkbaarheid) en kosten. Dit betekent dat de maatregelen effectief moeten zijn zonder de bruikbaarheid en betaalbaarheid uit het oog te verliezen.
4. Gedegen **samenwerking** zowel binnen de informatiebeveiligingsorganisatie als met de domeinen waar raakvlakken mee zijn, is van cruciaal belang om een betrouwbare en open omgeving te waarborgen.

3.2 Wet- en regelgeving

Het Concern Informatiebeveiligingsbeleid van de gemeente Rotterdam wordt bepaald door verschillende wet- en regelgeving. Dit omvat onder andere[8]: de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG (UAVG), de Archiefwet, de Telecommunicatiewet, de eIDAS-verordening, de Wet Open Overheid (WOO), de Wet Basisregistratie personen (BRP), de Wet SUWI, de Wet politiegegevens (Wpg), de Uitvoeringswet cyberbeveiligingsverordening, de EU-data-governance verordening en het intellectueel eigendomsrecht.

Daarnaast zijn er ook aanvullende overheidsrichtlijnen en –convenanten relevant voor het Concern Informatiebeveiligingsbeleid. Dit zijn de Baseline Informatieveiligheid Overheid versie 1.4 (BIO), de Nederlandse Overheid Referentie Architectuur (NORA), de Gemeentelijke Model Architectuur (GEMMA), de eenduidige Normering Single Information Audit (ENSIA), de Cyber Security Implementatie Richtlijn Objecten (CSIR) en de Richtlijn Netwerk- en Informatie-Security (NIS2).

Door de continue aandacht voor informatieveiligheid vanuit de wetgever, wordt er aangepaste en nieuwe Europese en nationale wet- en regelgeving verwacht zoals de Kunstmatige Intelligentie verordening (2025), en de European Dataspaces, de BIO 2.0 (2025) en de eIDAS2.0. Na besluitvorming over de impact van deze veranderingen voor informatieveiligheid worden de nieuwe normen en richtlijnen toegevoegd aan het Concern Informatiebeveiligingsbeleid.

Voor de domeinen (zie 3.6) die specifieke wet- en regelgeving (materiële wetten) hebben waarin eisen aan informatieveiligheid worden gesteld, geldt dat deze domeinen moeten voldoen aan het Concern Informatiebeveiligingsbeleid.

Naleven van wet- en regelgeving ten aanzien van informatieveiligheid vergt steeds meer externe verantwoording, met name voor het gebruik van DigiD, SUWI en BRP.
De gemeente moet aantoonbaar voldoen aan deze wet- en regelgeving en wordt door meerdere toezichthouders, waaronder de gemeenteraad, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) en de Autoriteit Persoonsgegeven (AP), periodiek gecontroleerd. Rotterdam is voor deze verantwoording aangesloten bij de landelijk ingevoerde ENSIA-systematiek.

[8] Zie onderzoek BZK 2020 inzake relevante wet- en regelgeving | Wetgevingskader informatieveiligheid - Digitale Overheid

3.3 Normen en standaarden

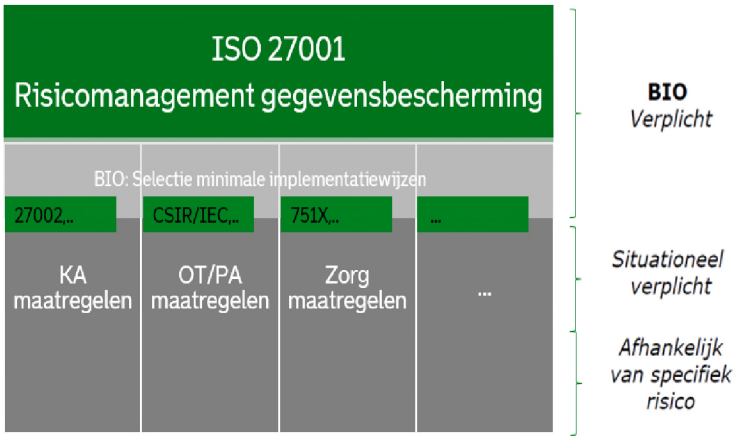
Vanwege de steeds snellere ontwikkelingen in informatietechnologie en digitalisering wordt de wereldwijde omgeving complexer, onzekerder en onveiliger. Dit brengt meer risico's met zich mee met betrekking tot de beveiliging van de (persoons)gegevens en informatiesystemen. Om deze risico's te beheersen en te voldoen aan de eisen van aantoonbaarheid, volgt de gemeente Rotterdam de beleidskaders en standaardproducten voor informatiebeveiliging die zijn ontwikkeld door de Informatiebeveiligingsdienst voor gemeenten (VNG/IBD), het Centrum voor Informatiebeveiliging en Privacy (CIP) en het Nationaal Cyber Security Centrum (NCSC).

De gemeente houdt zich aan de informatiebeveiligingsstandaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie zoals voorgeschreven in de Wet Digitale Overheid 2023 (WDO). Deze standaarden verbeteren de samenwerking tussen bedrijven, burgers en de overheid rondom het veilig uitwisselen van gegevens. Het toepassen van deze standaarden volgt de BIO-aanpak voor risicobeheersing, het 100% voldoen aan deze 'pas toe of leg uit'-lijst van het Forum Standaardisatie is geen doel op zichzelf.

Een internationale erkende norm voor het adequaat beveiligen van informatie en informatiesystemen is vastgelegd in de ISO27001/2. Voor de Nederlandse overheid (alle bestuurslagen) is deze normering vertaald naar de BIO[9] door de VNG/IBD. De BIO is een verplichte norm voor overheden met minimale implementatiewijzen van een risico-gebaseerd managementsysteem en beheersmaatregelen die aansluiten op de verschillende omgevingen van de overheid, waar op een eenduidige wijze verantwoording mee kan worden afgelegd. De VNG/IBD helpt gemeenten met aanvullende producten en handreikingen om de BIO te implementeren. De beheersmaatregelen van de BIO zijn vertaald in operationele richtlijnen voor de gemeente in een Rotterdamse Informatiebeveiliging Framework (RIF), welke onderdeel is van het Rotterdamse Information Security Management System (ISMS) zoals beschreven in hoofdstuk 4.

De gemeente Rotterdam past, als aanvulling op de ISO27001/2 en de BIO, de volgende normen en standaarden toe:

- De CSIR wordt gebruikt als vastgestelde implementatie-richtlijn voor Operationele Technologie (OT).
- De IEC 62443 wordt gebruikt voor industriële controles-ystemen (ICS/PA).
- De NEN7510 en NTA 7516 worden gebruikt voor het zorgdomein.
- De SSD, NPR5326, IEC25010 en de ICT-beveiligingsrichtlijnen voor webapplicaties en de aansluitvoorwaarden DigiD worden gebruikt voor het veilig ontwikkelen van software en voor het ontwikkelen van veilige en toegankelijke websites.



[9] Zie Staatscourant 2019, nr 26526 | https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html

3.4 Strategisch risicomanagement informatiebeveiliging

De kern van strategisch risicomanagement is het bewust komen tot betrouwbaarheidseisen en beveiligingsmaatregelen en het bewust accepteren van beheersbare risico's. Hierbij wordt uitgegaan van het principe 'van onbewust risico's lopen naar bewust risico's nemen' [10].

Strategisch risicomanagement voor informatiebeveiliging houdt in dat informatie-beveiligingsrisico's inzichtelijk en systematisch worden geïnventariseerd en worden beoordeeld. Daarna zal de informatiebeveiligingsorganisatie adviseren over de te treffen maatregelen om de risico's te mitigeren. Dit advies ondersteunt de proceseigenaar en het clustermanagement om verantwoording af te leggen over haar besluiten. Deze verantwoording betreft zowel de opvolging van de geadviseerde maatregelen als de eventueel geaccepteerde risico's. Door dit risicomanagementproces te integreren in de bedrijfsprocessen die zijn ingericht om de doelstellingen van de organisatie te realiseren wordt de weerbaarheid tegen dreigingen verhoogd.

3.5 Raakvlakken met organisatie domeinen

De principes voor informatiebeveiliging gelden voor de hele gemeentelijke organisatie. Binnen de gemeentelijke organisatie zijn specifieke domeinen waar informatiebeveiliging een positieve impact heeft. Hieronder wordt per domein een korte toelichting gegeven waarin de samenhang is beschreven met het strategisch perspectief van informatie-beveiliging:

- **Privacy:** de proceseigenaar dient als verantwoordelijke voor het verwerken van persoonsgegevens te voldoen aan de verplichtingen van de AVG. Privacy richt zich vooral op het inzichtelijk krijgen van risico's bij de verwerking van persoonsgegevens en het nemen van maatregelen om deze risico's te verminderen. Gemeente Rotterdam is als verwerkingsverantwoordelijke verplicht om passende organisatorische en technische beveiligingsmaatregelen te nemen, zoals bedoeld in de artikelen 5, 24, 25 en 32 van de AVG. Daarnaast moet de gemeente Rotterdam kunnen laten zien dat de juiste organisatorische en technische maatregelen zijn genomen om de persoonsgegevens te beveiligen. Om persoonsgegevens veilig te verwerken neemt de gemeente Rotterdam verschillende maatregelen zoals Privacy-by-Design, het autoriseren van toegang, het loggen van applicatiegebruik en het vergroten van het bewustzijn bij werknemers over mogelijke risico's. Daarnaast heeft de gemeente Rotterdam de werkprocessen waarin persoonsgegevens worden verwerkt, vastgelegd in een verwerkingsregister.

- **Informatiebeheer:** de proceseigenaar dient als verantwoordelijke voor het verwerken, opslaan en verwijderen van informatie de kaders en richtlijnen van informatiebeheer toe te passen. Dit zorgt ervoor dat informatie vindbaar, beschikbaar, toekomstbestendig, interpreteerbaar, leesbaar, en betrouwbaar is en in overeenstemming blijft met de Archiefwet. Deze kwaliteit van informatie is nodig voor het correct uitvoeren van processen, het afleggen van verantwoording, het uitvoeren van onderzoek en het borgen van cultuurhistorische waarden. Er wordt speciale aandacht besteed aan het openbaar maken van informatie ('open tenzij...') zoals voorgeschreven in de Wet open overheid (Woo) en de Wet hergebruik overheidsinformatie (Who). Door een classificatieschema te gebruiken, naast de BBN-classificatie, wordt bepaald welke passende maatregelen nodig zijn naast de beveiligingsmaatregelen, om de genoemde kwaliteit te waarborgen. Dit helpt om de informatiehuishouding op orde te brengen en te houden.

[10] Bron: Concern Integraal Beveiligingsbeleid Rotterdam

- **Datamanagement:** is een op zichzelf staande discipline die de hele datalevenscyclus afdekt van creatie, beschrijving en organisatie via beheer en integratie tot delen en vernietigen. De proceseigenaar is verantwoordelijk voor het beheer en gebruik van data over de hele levenscyclus. Als data voor een ander proces gebruikt gaat worden dan ontstaat er een afspraak tussen de twee proceseigenaren, die van de databron en het daadwerkelijke gebruik. Beide proceseigenaren zijn uiteraard gehouden aan wet- en regelgeving en Rotterdamse kaders als het open databeleid, de Datastrategie; Datamanagement Functie Ontwerp; Governance van hoog risico algoritmen; en het Afwegingskader voor sensoren, data-toepassingen en AI. Uit Rotterdamse kaders én Nederlandse en Europese wetgeving (o.a. Who) volgt een ambitie en verplichting om data te delen. Datamanagement helpt om data intern en extern te ontsluiten en om te kunnen beschikken over betrouwbare data van de juiste betekenis. Het maakt data vindbaar, toegankelijk, begrijpelijk, betrouwbaar, herleidbaar naar de bron en transparant in verantwoordelijkheid.

- **Data ethiek:** de proceseigenaar van data-en analyseproducten zorgt voor verantwoord gebruik. Data ethiek kijkt naar de bewuste afweging die gemaakt wordt over hoe we willen dat er met data om mag worden gegaan, vooral bij data-en analyseproducten waar ethische dillema's spelen. De afweging die we (impliciet) maken wordt transparant gemaakt door deze te concretiseren en te documenteren. Bij algoritmes wordt dit meegenomen in het algoritmeregister[11].

- **Architectuur:** de proceseigenaar draagt zorg voor het inpassen van voorgestelde veranderingen in de bestaande architectuurprincipes, -richtlijnen en -modellen van de gemeente. Hiermee zorgt hij ervoor dat verandering voldoet aan de gemeentelijke kaders, in dit geval de kaders op het gebied van informatiebeveiliging. De bijbehorende informatiebeveiligingsarchitectuur is een verzameling samenhangende principes, richtlijnen en modellen die richting geven aan de implementatie van het Concern Informatiebeveiligingsbeleid. Dit borgt dat de juiste beveiligingsmaatregelen genomen en onderhouden worden. De Rotterdamse architectuur kaders staan niet op zichzelf maar zijn een afgeleide van de Europese en nationale referentiearchitecturen zoals de NORA en de verbijzondering voor de gemeenten de GEMMA.

- **Fysieke beveiliging**: de proceseigenaar of clustermanagement geeft als verantwoordelijke van het pand of de ruimte alleen geautoriseerde werknemers toegang tot het pand of de ruimte waar gevoelige informatie fysiek of digitaal aanwezig is. Alle interne werknemers van de gemeente Rotterdam hebben algemene autorisatie tot alle werklocaties inclusief alle ruimtes die geen extra beveiliging nodig hebben binnen deze werklocatie. Externe werknemers krijgen enkel toegang tot hun specifieke werklocatie. Concern Huisvesting past beveiligingsmaatregelen toe op basis van een risicoafweging om de aanwezige fysieke informatie te beschermen conform de geldende eisen uit het Concern Informatiebeveiligingsbeleid.

- **Business Continuity Management (BCM):** de proceseigenaar draagt zorg voor het tijdig herstel van de werking van zijn proces in geval van een onderbreking als gevolg van een incident of calamiteit. Als het gaat over de continuïteit van de informatie-voorziening worden de benodigde maatregelen genomen conform het Concern Informatiebeveiligingsbeleid.

[11] Algoritmeregister Rotterdam: Algoritmeregister | Rotterdam.nl

- **Softwareontwikkeling**: de proceseigenaar hanteert bij het ontwikkelen, het testen en het onderhouden van software, de normen en standaarden om te komen tot blijvend veilige software.

- **ICT:** de proceseigenaar ICT draagt zorgt voor het veilige beheer van informatiesystemen. Dit omvat een breed scala aan on-premise systemen, de Rotterdamse ICT-infrastructuur en koppelingen met externe cloudoplossingen.

- **HR:** werknemers die met informatie werken kunnen al dan niet bewust een risico vormen voor informatieveiligheid. De HR-afdeling realiseert maatregelen op het gebied van arbeidsvoorwaarden, gedragsregels en maatregelen en ter voorkoming of verkleining van de risico's. Dit is bijvoorbeeld door bij indiensttreding een geldige Verklaring Omtrent Gedrag (VOG) te eisen, het laten afleggen van een ambtseed en/of het laten tekenen van een geheimhoudingsverklaring.

- **Operationele Technologie (OT), Industriële Automatisering (IA), Proces automatisering (PA), ICS/SCADA:** de proceseigenaar houdt rekening met extra beveiligingseisen die gelden voor Operationele Technologie (OT). OT is een overkoepelende term voor verschillende systemen waaronder Industrial Control Systems (ICS), Supervisory Control And Data Acquisition (SCADA), Programmable Logic Controllers (PLC), Industrial en Internet of Things toepassingen (IIot/IoT). Hieronder vallen bijvoorbeeld systemen voor het beheren van bruggen, sluizen, gemalen, tunnels, verkeerslichten, camera's, parkeergarages, liften, toegangspoorten, (straat)verlichting en sensoren die worden gebruikt voor het verzamelen van data. De gevolgen van een incident in dit domein kunnen levensbedreigend en/of verstorend/ontwrichtend zijn voor de samenleving.

3.6 Verhogen Digitale Weerbaarheid

Het Concern Informatiebeveiligingsbeleid geeft richting aan het waarborgen en verhogen voor veilig werken zowel door als voor alle werknemers. Door continu aandacht te besteden aan het belang van het veilig werken met informatie, wordt de digitale weerbaarheid en veerkracht van de gemeente verhoogd. Hierbij zijn een aantal onderwerpen belangrijk:

- **Informatiebeveiliging is van iedereen**
  In ons dagelijks leven en werk zijn we steeds meer afhankelijk geworden van internet, social media en cloudopslag. Dit brengt beveiligingsrisico's met zich mee, met name op het gebied van de beschikbaarheid, integriteit en vertrouwelijkheid van onze informatie. Werknemers moeten zich daarom bewust zijn van deze risico's. Want, naast het hebben van een technisch veilige omgeving, zijn het de werknemers en hun handelen die onze digitale omgeving écht veilig of onveilig maken. Het verantwoord en veilig omgaan met informatie en onze werkomgeving is daarom de gedeelde verantwoordelijkheid van iedereen.

- **Houding en gedrag**
  De meeste incidenten worden, vaak onbewust, veroorzaakt door fouten van werknemers. Het Concern bewustwordingsprogramma *Blijf alert!* leert werknemers op een gestructureerde manier hoe ze bewust en veilig met informatie en onze werkomgeving moeten omgaan, onder andere met e-learnings en bij instromen van nieuwe werknemers. Dit programma is herkenbaar en sluit aan bij de dreigingen en risico's rondom onze informatievoorziening. De uitleg van de gewenste houding en gedrag inclusief normen, waarden en verantwoordelijkheden sluit goed aan bij

werknemers. De situaties die worden besproken zijn vergelijkbaar met wat werknemers zowel op de werkvloer als ook in hun privéleven tegenkomen. Het bewustwordingsprogramma ondersteunt via maatwerk ook een gehele afdeling of team. Tevens is er aansluiting op de campagnes vanuit privacy en informatiebeheer, met als doel de boodschap te versterken en bij de werknemers centraal aandacht te vragen.

- **Informatieveilige cultuur**
  Het bewustwordingsprogramma bevordert een gewenste cultuurverandering om het gewenste gedrag te stimuleren. De gemeente Rotterdam streeft naar een cultuur waarin informatieveiligheid en privacy in het DNA van elke werknemer zit. Dit omvat een open cultuur waarin werknemers elkaar kunnen helpen en corrigeren, evenals een veilige meldcultuur waarin het melden van incidenten en het signaleren van risico's wordt aangemoedigd. Werknemers moeten zich vrij voelen om incidenten te melden, risico's te herkennen en elkaar aan te spreken op onveilig gedrag.

- **Goed voorbeeld doet goed volgen**
  Informatieveilig gedrag is alleen effectief als iedereen meewerkt. Dit betekent dat zowel het bestuur, de directie, het management en de werknemers betrokken moeten zijn en blijven. Het management heeft hierin een voorbeeldfunctie. Hun houding en gedrag zijn van essentieel belang; zij stimuleren veilig gedrag en dragen dit uit naar de rest van de organisatie. Het bewustwordingsprogramma biedt ondersteunende hulpmiddelen om veilig werken te vergemakkelijken.

- **Crisisoefeningen**
  Het uitvoeren van crisisoefeningen helpt ons om effectief om te gaan met digitale dreigingen. Door regelmatig te oefenen kunnen we samen leren, ervaring opdoen en beter voorbereid zijn op mogelijke incidenten. Op deze manier kunnen we onze digitale veiligheid verbeteren. Aangezien digitale dreigingen voortdurend veranderen is het continu leren belangrijk. Het is cruciaal dat we goed voorbereid zijn zodat we problemen kunnen voorkomen en ervoor kunnen zorgen dat al onze digitale diensten veilig en beschikbaar blijven. Samen met de proceseigenaren worden structureel oefeningen georganiseerd waarbij we gebruik maken van de lessons learned uit incidenten en crisissen uit andere organisaties.

- **Ethische Hackers**
  Digitale incidenten en beveiligingsproblemen ontstaan vaak door misbruik van kwetsbaarheden in software die gebruikt wordt. Onze informatiebeveiligings-organisatie neemt verschillende maatregelen om deze kwetsbaarheden op te sporen. Bovendien stimuleren we actief het melden van dergelijke kwetsbaarheden via ons 'Coordinated Vulnerability Disclosure' loket[12]. Ook organiseren we jaarlijks het evenement 'Hack010', waarbij ethische hackers worden uitgenodigd om kwetsbaarheden in onze ICT-infrastructuur te identificeren, waardoor we passende beveiligingsmaatregelen kunnen nemen.

[12] Coordinated Vulnerability Disclosure' loket Responsible Disclosure | Rotterdam.nl



4 Organisatie van informatiebeveiliging

De gemeentesecretaris is eindverantwoordelijk voor de uitvoering van de organisatiebrede vraagstukken met betrekking tot informatiebeveiliging.[13] De gemeentesecretaris wordt daarbij ondersteund door de informatiebeveiligingsorganisatie vanuit BCO/IIFO.

4.1 De informatiebeveiligingsorganisatie

De informatiebeveiligingsorganisatie van de gemeente Rotterdam is een lerende en samenwerkende organisatie. Ze zal op grond van onafhankelijkheid, de transparantie van de informatiebeveiligingsprocessen, de kwaliteit van de informatiebeveiligings-adviezen en een toegewijde uitvoering van haar taken, de proceseigenaren en het clustermanagement zo goed mogelijk ondersteunen bij hun verantwoordelijkheden voor informatieveiligheid. De proceseigenaren en het clustermanagement zijn eindverantwoordelijk:

- voor het uitvoeren van risicoanalyses voor het beveiligen van haar processen, informatiesystemen, gegevens, webapplicaties en/of objecten;
- voor het implementeren en onderhouden van de maatregelen voor informatiebeveiliging.

De informatiebeveiligingsorganisatie is opgedeeld in verschillende lagen en aansturing. Vanuit een strategisch, tactisch en operationeel niveau en een duidelijke taakverdeling worden de proceseigenaren en het clustermanagement effectief ondersteund door:

- De Chief Information Security Officer (CISO) die verantwoordelijk is voor het coördineren van de informatiebeveiliging binnen de gemeente Rotterdam. De CISO stuurt de gehele informatiebeveiligingsorganisatie functioneel aan[14]. De CISO en zijn team zijn organisatorisch belegd bij BCO/IIFO/CIO-Office en opereren op strategisch niveau, waarbij zij zich richten op het gehele concern en alle genoemde doelgroepen.
- De Information Security Officers (ISO) die op tactisch/operationeel niveau ondersteuning biedt bij de doelstellingen van het clustermanagement en de proceseigenaren. Dit team is organisatorisch belegd bij BCO/IIFO/IMP.
- Security Management die op tactisch/operationeel niveau ondersteuning biedt bij de technische aspecten van informatiebeveiliging. Deze aspecten zijn vertaald in operationele richtlijnen in een Rotterdams Informatiebeveiliging Framework (RIF). Dit team is organisatorisch belegd bij BCO/IIFO/ICT.
- Het Security Operations Centre (SOC) die op operationeel niveau de technische infrastructuur monitoren op dreigingen door middel van kwetsbaarhedenscans. Dit team is organisatorisch belegd bij BCO/IIFO/ICT.

De informatiebeveiligingsorganisatie moet voortdurend investeren in expertise door middel van permanente educatie, training, en actieve monitoring van bedreigingen. Structurele investeringen in kennis, vaardigheden en ondersteunende tools zijn essentieel om aan

[13] De taken en verantwoordelijkheden binnen de gemeente Rotterdam met betrekking tot informatiebeveiliging zijn vermeld in de doelgroepen tabel van hoofdstuk 2.6 inclusief de vermelding van de kaders waarin dit is vastgesteld.
[14] Functioneel aansturen: voeren van regie over een samenhangend geheel van werkzaamheden en ondanks het ontbreken van een hiërarchische relatie bevoegd zijn om aan alle betrokken werknemers aanwijzingen te geven. Bron: kadernota sturen en verantwoorden 2023

beveiligingsverplichtingen te voldoen en een proactieve norm te handhaven. Onder leiding van de CISO fungeert de informatiebeveiligingsorganisatie als een centrum van expertise en biedt advies aan proceseigenaren en clustermanagers. De informatiebeveiligings-organisatie moet kunnen meebewegen met de groeiende aandacht voor informatieveiligheid vanuit wet- en regelgeving en toezichthouders (zie hoofdstuk 3).

Vanuit haar onafhankelijke rol monitort de informatiebeveiligingsorganisatie of verantwoordelijkheden worden nagekomen en rapporteert hierover in relevante overlegstructuren, rekening houdend met de groeiende aandacht voor informatieveiligheid vanuit wet- en regelgeving en toezichthouders.

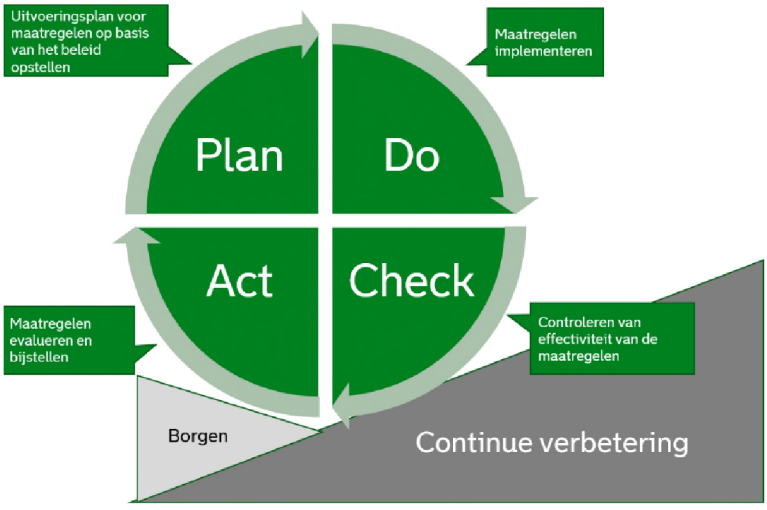
4.2 Managementsysteem voor informatiebeveiliging (ISMS)

De informatiebeveiligingsorganisatie wordt in haar werkzaamheden ondersteund door een managementsysteem voor informatiebeveiliging, ook wel bekend als het Information Security Management System (ISMS). Het ISMS ondersteunt het college van B en W, de Concerndirectie, het clustermanagement en de proceseigenaren bij het bereiken van het maximaal 'in control' zijn met betrekking tot informatieveiligheid.

De CISO is verantwoordelijk voor het Rotterdamse ISMS waarmee de principes van informatieveiligheid (zoals beschreven in hoofdstuk 3) systematisch worden beheerd. Dit gebeurt door middel van een cyclisch en iteratief risicobeheerproces. Vanuit het ISMS kan het Concern Dashboard worden gevoed met relevante prestatie indicatoren Informatieveiligheid.

Met het ISMS is informatiebeveiliging ingericht als een continu verbeterproces, om voortdurend te werken aan de best mogelijke invulling van maatregelen voor een betrouwbare informatievoorziening. Dit verbeterproces wordt ondersteund door verschillende methodes:

- De BUC-methode (Beleid, Uitvoering, Control). Deze methode wordt gebruikt als strategisch proces om het Concern Informatiebeveiligingsbeleid en het meerjarenplan informatiebeveiliging te ondersteunen (zie hoofdstuk 2.5).
- De generieke Plan-Do-Check-Act (PDCA). Deze stappen worden toegepast om de tactische en operationele processen van informatieveiligheid te ondersteunen.
- De werkwijze van het NIST-framework. Deze wordt geïmplementeerd als een effectief en specifiek kader om informatiebeveiligingsrisico's aan te pakken.



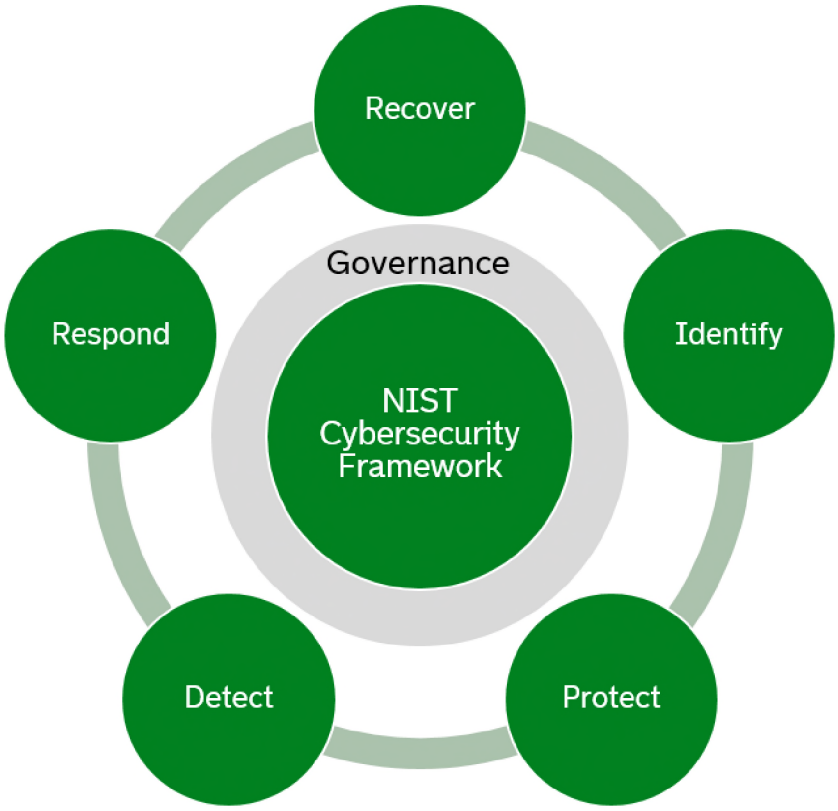
Het ISMS van de gemeente Rotterdam volgt een gestructureerde aanpak bestaande uit de volgende vier stappen:

1. **Plan:** In deze fase worden uitvoeringsplannen informatiebeveiliging ontwikkeld, conform het onderhavig **beleid.** Deze stap omvat het NIST-principe van **Identificeren en Beschermen** waarbij de gemeente zich richt op het verminderen van kansen op digitale incidenten en misbruiken van kwetsbaarheden.

2. **Do:** Hier worden zowel organisatorische als technische beveiligingsmaatregelen geïmplementeerd om gevoelige (persoons)gegevens te beschermen en risico's te beheersen. Deze stap volgt **'uitvoering'** van het strategische BUC-proces.

3. **Check:** In deze fasen worden de efficiëntie en effectiviteit van de geïmplementeerde maatregelen geëvalueerd met als doel 'in **control**' te zijn en te blijven. Deze stap omvat de NIST-principe **Detecteren, Reageren en Herstellen**, waarmee de impact van digitale incidenten en misbruik van kwetsbaarheden wordt verminderd.

4. **Act:** Indien nodig worden beleid, strategie, plannen en beveiligingsmaatregelen bijgestuurd op basis van de resultaten van de controlestap. Het doel is een doelmatige en verantwoorde toewijzing van beperkte middelen in relatie tot de bijbehorende risico's.



Stappen van het NIST-framework

4.3 Controle en verantwoording

Rotterdammers verwachten een betrouwbare overheid die zorgvuldig met hun informatie omgaat. Het gaat daarbij om het waarborgen van beschikbaarheid, integriteit en vertrouwelijkheid van gemeentelijke processen, informatiesystemen en de daarin opgeslagen gegevens. Dat zorgt zowel voor betrouwbaarheid als voor goede kwaliteit en continuïteit van de bedrijfsvoerings- en dienstverleningsprocessen.

Het college van B en W legt jaarlijks verantwoording af over de stand van zaken op het gebied van informatieveiligheid binnen Rotterdam via een collegeverklaring informatie-beveiliging. Deze verklaring is gebaseerd op de landelijke en voor gemeenten verplichte ENSIA-systematiek. De Eenduidige Normatiek Single Information Audit (ENSIA) is in 2017 ontstaan op initiatief van gemeenten en de ministeries van BZK en SZW om een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatieveiligheid te bieden. Dit stelsel omvat een zelfevaluatie gebaseerd op de informatiebeveiligingsnormen die van toepassing zijn voor de overheid. Tevens ondersteunt dit stelsel de verantwoordingsfase over informatieveiligheid, welke door het college van B en W wordt afgelegd aan enerzijds de gemeenteraad en anderzijds aan de verschillende toezichthouders van de ministeries van BZK en SZW met betrekking tot de informatiebeveiligingsnormen uit de wet- en regelgeving betreffende de BRP, PUN, SUWI, DigiD, BAG, BGT en BRO.



Bron: VNG-realisatie; ENSIA

De ENSIA-verantwoording betreft:

- Implementatie van de BIO - Zelfevaluatie
- Basis Registratie Personen (BRP) - Zelfevaluatie
- Paspoort Uitvoeringsregeling Nederland (PUN) - Zelfevaluatie
- Structuur Uitvoeringsorganisatie Werk en Inkomen (Suwinet) – Geauditeerde zelfevaluatie
- Digitale Persoonsidentificatie (DigiD) – Geauditeerde zelfevaluatie
- Basisregistratie Adressen en Gebouwen (BAG) - Zelfevaluatie op datakwaliteit
- Basisregistratie Grootschalige Topografie (BGT) - Zelfevaluatie op datakwaliteit
- Basisregistratie Ondergrond (BRO) - Zelfevaluatie op datakwaliteit

De CISO voert als ENSIA-coördinator de regie en ziet toe dat de informatie die nodig is voor de beantwoording van de zelfevaluatie (de informatiebeveiligings-audit vragen) door de informatiebeveiligingsorganisatie wordt verzameld. De proceseigenaren en het cluster-management zijn verantwoordelijk voor het verstrekken van alle benodigde informatie om de jaarlijkse zelfevaluatie informatiebeveiliging in te vullen. De Informatiebeveiligings-organisatie adviseert de ENSIA-coördinator over de aangeleverde informatie en controleert of deze volledig is. Ten slotte wordt door een onafhankelijke register-auditor (binnen de gemeente belegd bij afdeling Concern Auditing) een oordeel afgegeven over het wel of niet voldoen aan de specifieke ENSIA-normen van informatiebeveiliging.

4.4 Afwijkingen van de informatiebeveiligingsprincipes

Bij de implementatie van beveiligingsmaatregelen moet altijd een goede **balans** worden gevonden tussen informatieveiligheid, gebruiksvriendelijkheid (werkbaarheid) en kosten zoals beschreven in hoofdstuk 3.1.

De eindverantwoordelijkheid voor het tijdig en correct implementeren van beveiligingsmaatregelen ligt bij de proceseigenaren en het clustermanagement ten aanzien van haar processen, informatiesystemen, gegevens, webapplicaties en/of objecten. In uitzonderlijke gevallen, zoals bijvoorbeeld bij schaarse middelen, korte termijn vervangingsperspectief of reorganisaties, kan de verantwoordelijke voorstellen doen aan de portefeuillehouder informatiebeveiliging om af te wijken van het advies van de informatiebeveiligingsorganisatie om maatregelen te implementeren. Hierbij hoort ook de 'pas toe of leg uit'-lijst ten aanzien van de informatiebeveiligingsstandaarden zoals vermeld in hoofdstuk 3.3. Als maatregelen niet meteen of helemaal niet geïmplementeerd worden, dan ontstaat er een risico welke bewust voor kortere of langere tijd geaccepteerd moet worden.

De informatiebeveiligingsorganisatie documenteert het besluit over uitstel van implementatie van de maatregelen op basis van een risico acceptatie overeenkomst in het ISMS. De informatiebeveiligingsorganisatie bewaakt het betreffende risico en rapporteert periodiek aan de portefeuillehouder, de proceseigenaar en het clustermanagement over het risico in relatie met de stand van de vereiste beveiligingsmaatregelen. Als het risico in omvang groeit of er ontstaat een strategisch risico ten aanzien van de bedrijfsvoering of dienstverlening, dan wordt een herbeoordeling gevraagd van het besluit om af te wijken van het implementeren van de maatregelen. Strategische risico's worden door de portefeuillehouder voorgelegd aan de Concerndirectie.

Bijlage A: Relevante documenten en bronnen

Relevante documenten en bronnen	Vindplaats	URL
Algemene Verordening Gegevensbescherming (AVG) En Uitvoeringswet AVG (UAVG)	Website Wetten.nl Website gemeente Rotterdam	wetten.nl - Regeling - Uitvoeringswet Algemene verordening gegevensbescherming - BWBR0040940 (overheid.nl) https://www.rotterdam.nl/bestuur-organisatie/uw-gegevens/
Baseline Informatiebeveiliging Overheid (BIO)	Website VNG Staatscourant	https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/ Staatscourant 2020, 7857 | Overheid.nl > Officiële bekendmakingen (officielebekendmakingen.nl)
Bestuurlijk convenant digitale veiligheid gemeenten	Staatscourant 30 december 2022, nr 35231	Bestuurlijk convenant digitale veiligheid gemeenten (vng.nl)
Concern Informatiebeheerbeleid Rotterdam	Intranet gemeente Rotterdam	Wet- en regelgeving - RIO (rotterdam.nl)
Concern Integraal Beveiligingsbeleid Rotterdam	Intranet gemeente Rotterdam	Documenten - RIO (rotterdam.nl)
CSIR – Cybersecurity Implementatie richtlijn	Website VNG/IBD	Cybersecurity Implementatierichtlijn Objecten – CSIR, beveiliging van Proces Automatisering van gemeenten - Informatiebeveiligingsdienst
De 10 bestuurlijke principes voor informatiebeveiliging	Website VNG	https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
Dreigingsbeeld Rotterdam	Intranet gemeente Rotterdam	Dreigingsbeeld (rotterdam.nl)
ENSIA - Eenduidige Normatiek Single Information Audit	Website VNG	ENSIA | VNG
Forum standaardisatie	Website BZK	'Pas toe leg uit' standaarden (verplicht) | Forum Standaardisatie
ICT-Beveiligingsrichtlijnen voor Webapplicaties	Website NCSC	ICT-beveiligingsrichtlijnen voor webapplicaties | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)
IEC[15] 25010	Website NEN	https://www.nen.nl/
IEC 62443	Website NEN	https://www.nen.nl/
ISO[16] 27001 en 27002	Website NEN	https://www.nen.nl/ict/cyber-

[15] IEC (de International Electrotechnical Commission) en

[16] ISO (de International Organization for Standardization) en vormen het gespecialiseerde systeem voor wereldwijde standaardisatie

		privacy/informatiebeveiliging
Kadernota 'Sturen en Verantwoorden Rotterdam 2023'	Intranet gemeente Rotterdam	Kaders, beleid en richtlijnen financiën - RIO (rotterdam.nl)
LOG4J	Apache Log4j 2, een Java logging library.	Actief misbruik van kwetsbaarheid in Apache Log4j 2 | Digital Trust Center (Min. van EZK)
NORA	Nederlandse Overheid Referentie Architectuur	NORA Online
NEN7510	Website NEN	https://www.nen.nl/
NTA7516	Website NEN	https://www.nen.nl/
NPR5326	Website NEN	https://www.nen.nl/
Regeling ICT- en informatiegebruik	Website Bestuurlijk Informatiesysteem Rotterdam	https://www.bis.rotterdam.nl/dossiers/43022
Uitvoeringswet cyberbeveiligingsverordening	Website Wetten.nl	wetten.nl - Regeling - Uitvoeringswet cyberbeveiligingsverordening - BWBR0046349 (overheid.nl)
Verwerkingsregister gemeente Rotterdam	Website gemeente Rotterdam	https://www.rotterdam.nl/bestuur-organisatie/verwerkingsregister/
VNG-realisatie; ENSIA	Website VNG	https://www.vngrealisatie.nl/ensia
VNG resolutie 'Digitale Veiligheid: kerntaak voor de gemeenten'	Website VNG	https://vng.nl/nieuws/meer-prioriteit-voor-beveiliging-digitale-systemen-gemeenten
Werklocatie, Werknemer	Personeels-handboek 010	Personeelshandboek 010 (rotterdam.nl)
Wetgevingskader informatieveiligheid	Website Digitale Overheid	Wetgevingskader informatieveiligheid - Digitale Overheid
Woordenboek cybersecurity 2021	Website Cyberveilig Nederland	https://cyberveilignederland.nl/download/file/CybersecurityWoordenboek2021.pdf

Bijlage B: Overige gebruikte afkortingen

Afkorting	Omschrijving	Vindplaats
AP	Autoriteit Persoonsgegevens	Home | Autoriteit Persoonsgegevens
BAG	Basisregistratie Adressen en Gebouwen	wetten.nl - Regeling - Wet basisregistratie adressen en gebouwen - BWBR0023466 (overheid.nl)
BBN	Basis Beveiligingsniveau	De BIO
BCM	Business Continuïteit Management	De BIO
BGT	Basisregistratie Grootschalige Topografie	wetten.nl - Regeling - Wet basisregistratie grootschalige topografie - BWBR0034026 (overheid.nl)
BIV	Beschikbaarheid – Integriteit – Vertrouwelijkheid	De BIO
BRO	Basisregistratie Ondergrond	Wet Bro - Basisregistratieondergrond
BRP	Basisregistratie Personen	wetten.nl - Regeling - Wet basisregistratie personen - BWBR0033715 (overheid.nl)
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	
BUC	Beleid, Uitvoering en Control	De BIO
CIP	Centrum Informatiebeveiliging en Privacybescherming	Home NL - cip-overheid
CISO	Chief Information Security Officer	De BIO
DigiD	Digitale Identiteit	Logius | DigiD
ISO	Information Security Officer	De BIO
eIDAS	electronic IDentities And Trust Services	Verordening Europees kader voor een digitale identiteit
IA	Industriële Automatisering	CSIR
IBD	Informatie Beveiligingsdienst	Home - Informatiebeveiligingsdienst
ICS	Industrial Control Systems	CSIR
ISMS	Information Security Management System	De BIO
GEMMA	Gemeentelijke Model Architectuur	GEMMA Online
NCSC	Nationaal Cyber Security Centrum	Home | Nationaal Cyber Security Centrum (ncsc.nl)
NIS2	Europese Richtlijn netwerk- en informatiebeveiliging	NIS2-richtlijn NIS2-richtlijn - Digitale Overheid
NIST	National Institute of Standards and Technology	Cybersecurity Framework | NIST

NORA	Nederlandse Overheid Referentie Architectuur	NORA Online
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap	Ministerie van Onderwijs, Cultuur en Wetenschap | Rijksoverheid.nl
OT	Operationele Technologie	CSIR
PA	Proces Automatisering	CSIR
PUN	Paspoort Uitvoeringsregeling Nederland	wetten.nl - Regeling - Paspoortuitvoeringsregeling Nederland 2001 - BWBR0012811 (overheid.nl)
SCADA	Supervisory Control And Data Acquisition	CSIR
SSD	Secure Software Development	SSD normen V3.0 (cip-overheid.nl)
SUWI	Structuur Uitvoeringsorganisatie Werk en Inkomen (SUWI)	wetten.nl - Regeling - Wet structuur uitvoeringsorganisatie werk en inkomen - BWBR0013060 (overheid.nl)
TBB	Te Beschermen Belangen	Integraal Beveiligingsbeleid Rotterdam
WHO	Wet hergebruik overheidsinformatie	wetten.nl - Regeling - Wet hergebruik van overheidsinformatie - BWBR0036795
WOO	Wet Open Overheid	wetten.nl - Regeling - Wet open overheid - BWBR0045754

Gemeente Rotterdam