



Concern Informatiebeveiligingsbeleid

Gemeente Rotterdam

2021-2023

Strategisch Beleidskader

Voorwoord

Het concern informatiebeveiligingsbeleid van de gemeente Rotterdam heeft als doel het beschermen van gemeentelijke informatie en informatie van burgers, bedrijven en ketenpartners. Het uitgangspunt is dat de bescherming van de informatie aansluit bij de risico's, bedrijfsvoering en relevante wet- en regelgeving. Het college van B en W hecht grote waarde aan dit onderwerp en verwacht hetzelfde van iedere medewerker. Hierbij is ieder individueel verantwoordelijk voor het veilig omgaan met alle informatie.

Dit strategisch informatiebeveiligingsbeleid is richtinggevend ten aanzien van informatieveiligheid voor de gemeente Rotterdam en de uitwerking op tactisch en operationeel niveau voor toekomstige beleidsstukken, procedures en werkinstructies die gerelateerd zijn aan het vakgebied van informatieveiligheid.

Ten aanzien van informatieveiligheid heeft gemeente Rotterdam de volgende ambitie:

- Het op een veilige manier verwerken van gegevens van burgers en bedrijven door het toepassen van passende organisatorische en technische beveiligingsmaatregelen, zoals vereist in de Algemene Verordening Gegevensbescherming (AVG) en onder andere beschreven in de Baseline Informatiebeveiliging Overheid (BIO);
- Het voor de burgers, bedrijven en ketenpartners een aantoonbaar betrouwbare partner zijn ten aanzien van het onderwerp Informatiebeveiliging;
- Professioneel inrichten van informatiebeveiliging in het concern in relatie met de verantwoordelijkheid van de gemeente inzake eigenaar, leverancier en/of afnemer van gegevens;
- Bijdragen aan het voorkomen en bestrijden van digitale criminaliteit;
- Mede zorgen voor de samenleving bij het optreden van digitale incidenten;
- Integreren van het informatiebeveiligingsbeleid in de diverse veiligheidsgebieden en hierop intensiever samenwerken.

De collegetargets 2018-2022 geven de doelstellingen aan om de kansen en dreigingen die digitalisering met zich meebrengt te benutten en te beheersen. Dit informatiebeveiligingsbeleid draagt bij aan het identificeren van deze kansen en het beheersbaar maken van dreigingen.

Inhoud

Voorwoord.....	2
1. Inleiding.....	4
2. Aanleiding/context.....	6
2.1 Leeswijzer	6
2.2 Wat is informatiebeveiliging.....	6
2.3 Scope.....	6
2.4 Dreigingslandschap gemeente Rotterdam.....	7
2.5 Doelstellingen Concern Informatiebeveiligingsbeleid.....	8
2.6 Doelgroepen.....	9
2.7 Besluitvorming.....	9
3 Uitgangspunten voor informatiebeveiliging	10
3.1 Strategische doelen informatiebeveiliging	10
3.2 Bestuurlijke principes informatiebeveiliging	10
3.3 Wet- en regelgeving	11
3.4 Normen en standaarden.....	11
3.5 Strategisch risicomanagement	11
3.6 Overige domeinen.....	12
3.7 Verhogen Digitale Weerbaarheid.....	13
4 Organisatie van informatiebeveiliging	15
4.1 Managementsysteem	15
4.2 Verschillende rollen en verantwoordelijkheden.....	16
4.3 Controle en verantwoording	16
4.4 Afwijkingen van bestaand beleid en regelgeving	17
Bijlage A: Relevante documenten en bronnen.....	18

1. Inleiding

De informatie van de gemeente Rotterdam vertegenwoordigt in verschillende verschijningsvormen een grote waarde. De informatievoorziening, en dus de waarde van de informatie, van de gemeente Rotterdam wordt blootgesteld aan vele dreigingen, die bovendien voortdurend veranderen en complexer worden. Dit maakt het noodzakelijk om gerichte maatregelen te nemen om de risico's continu te beheersen.

In 2020 hadden meerdere digitale dreigingen en incidenten grote impact op diverse organisaties, wereldwijd. Ook de gemeente Rotterdam had kortstondig last van het beveiligingslek in Citrix, waardoor diverse werkprocessen met verstoringen te maken kregen. Tijdens de Corona crisis is veel gevraagd van vernieuwde manieren van informatie verwerken, waarbij nieuwe digitale dreigingen en risico's hun intrede deden, waarvoor weer nieuwe passende maatregelen (zowel organisatorische als technische) ontwikkeld en geïmplementeerd moesten worden.

In deze situaties werden niet enkel de regels en beleid als uitgangspunt genomen maar meer de aangediende realiteit. Vanuit volwassen vakmanschap is gewerkt om de nieuwe realiteit te interpreteren naar, voor de gemeente, waarde toevoegende activiteiten rondom informatieveiligheid. Deze getoonde veerkracht is een basis onder het nieuwe Rotterdamse werken.

De arena rondom digitale aanvallen wordt niet alleen groter en intensiever, maar ook complexer. Het is daarom onmogelijk om incidenten helemaal te voorkomen. Wat we wél kunnen doen is weerbaarder worden, weten wat we moeten doen wanneer een incident de gemeente treft. Goed voorbereid zijn en klaar staan, dat is de veerkracht van informatieveiligheid Rotterdam en is gedefinieerd als de activiteiten die nodig zijn om netwerk- en informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen (kunnen) worden door (digitale) dreigingen, te beschermen.

Goed voorbereid zijn betekent voor de eigenaren van de informatiesystemen en -processen continue op de hoogte zijn van de actuele risico's om de juiste maatregelen te treffen ter vermindering/voorkoming/verzekeren van deze risico's. Dit impliceert een risicobereidheidsprofiel. De eigenaren worden hierin ondersteund en geadviseerd door meerdere disciplines, waaronder functionarissen informatiebeveiliging, immers informatiebeveiliging is "maar" één van de kwaliteitsaspecten in informatievoorziening.

Het verder digitaliseren van processen staat hoog op de agenda, de informatiesystemen worden steeds beter, sneller en preciezer. Deze komen steeds meer met elkaar samen, raken met elkaar vervlochten en vormen zo één geheel. Nieuwe technologieën worden uitgetest en bij succes ingevlochten. Het datagedreven werken neemt een snelle vlucht. Gegevens over alles wat mensen en organisaties doen worden steeds vaker opgeslagen en gebruikt. Zo krijgt iedereen te maken met meer digitalisering en technologie.

De eigenaren van de informatiesystemen moeten op een andere manier aangesproken en betrokken worden vanuit informatiebeveiliging. Niet vanuit een centraal beleid en plan waarin de doelen en oplossingen bedacht en geïmplementeerd zijn, maar door samenwerking aan integrale veiligheid welke het clusterbelang optimaal ondersteunt.

In de nieuwe werkelijkheid blijven de eigenaren van informatiesystemen verantwoordelijk voor de resultaten, de uitvoering, nakoming van regels en de effectiviteit ten aanzien van informatiebeveiliging. Zij worden hierin ondersteund door de functionarissen informatieveiligheid met ontwikkeling van beleid, kaders en processen. De eigenaren worden geadviseerd inzake dreigingen, risico's en te nemen maatregelen, waarbij waarde-creatie,

veerkracht, heuristiek, leren/ervaren en door-ontwikkelen de uitgangspunten zijn. De inspiratie voor deze samenwerking heeft een relatie met het vermogen om de toekomst te voorzien.

De eigenaren van informatiesystemen kunnen daarmee een voortrekkersrol pakken en leiderschap tonen om vanuit hun proces / informatiesysteem de integrale veiligheid te borgen. De complementaire benadering van het thema behoeft een nieuwe uitwerking van beleidsvoornemens voor informatiebeveiliging.

De directie(s) en de bestuurder(s) kunnen op basis van deze beleidsvoornemens en de risicobereidheid haar verantwoordelijkheid nemen rondom informatiebeveiliging door inzicht in de dreigingen, risico's en maatregelen.

Met dit informatiebeveiligingsbeleid heeft gemeente Rotterdam het concern brede informatiebeveiligingsbeleid beschreven voor de jaren 2021-2023. Dit beleid sluit aan bij het 'Concern Integraal Beveiligingsbeleid', de kadernota 'Sturen en Verantwoorden Rotterdam 2020' en de VNG resolutie 'Digitale Veiligheid: kerntaak voor de gemeenten' (feb. 2021).

2. Aanleiding/context

Dit concern informatiebeveiligingsbeleid 2021-2023 is **richtinggevend en kaderstellend** voor informatieveiligheid en wordt aangevuld met onderwerp specifieke documenten voor informatiebeveiliging op tactisch niveau, waaronder de Regeling ICT- en informatiegebruik, het Meerjarenplan Informatiebeveiliging en uitgewerkt op operationeel niveau in processen en werkinstructies.

2.1 Leeswijzer

Hoofdstuk 2 bevat de uitgangspunten en strategische principes van informatiebeveiliging binnen de gemeente. Hoofdstuk 3 zet de kern van het strategisch beleid uiteen inclusief het raakvlak met andere domeinen. Hoofdstuk 4 beschrijft hoe de taken en verantwoordelijkheden ten aanzien van informatiebeveiliging in gemeente Rotterdam belegd zijn.

2.2 Wat is informatiebeveiliging

Informatiebeveiliging is de verzamelnaam van processen en maatregelen, die ingericht zijn om de *betrouwbaarheid* van gemeentelijke processen, informatiesystemen en de daarin opgeslagen gegevens (zowel digitaal als analoog, tekst, video, geluid) en de organisatie te beschermen tegen al dan niet opzettelijk onheil. Dit betreft:

- Beschikbaarheid (B)/ continuïteit: het zorg dragen voor het beschikbaar zijn van informatie en informatie-verwerkende bedrijfsmiddelen op de juiste tijd en plaats voor de gebruikers;
- Integriteit (I)/ juistheid: het waarborgen van de correctheid, volledigheid, tijdigheid en controleerbaarheid van informatie en informatieverwerking;
- Vertrouwelijkheid (V)/ exclusiviteit: het beschermen van informatie tegen kennisname en mutatie door onbevoegden. Informatie is alleen toegankelijk voor degenen die hiertoe geautoriseerd zijn.

Deze indeling van informatiebeveiliging naar *betrouwbaarheid* wordt kortweg BIV genoemd.

Informatieveiligheid borgt beveiligingsmaatregelen tegen bedreigingen ter voorkoming en vermindering van:

- Onwenselijk verlies van informatie, zowel tijdelijk als permanent;
- Onwenselijke corruptie van informatie, zowel bewust als onbewust;
- Onwenselijke onthulling van informatie, bewust of onbewust.

De Baseline Informatiebeveiliging Overheid (de BIO) omschrijft deze beveiligingsmaatregelen op vier niveaus. Per gedefinieerd bedrijfsbelang zal het juiste niveau passende maatregelen een adequate bescherming bieden. Rotterdam zal standaard voldoen aan Basis Beveiliging Niveau (BBN) 2. Indien de te beschermen belangen een hogere BBN (2+ of 3) eist, wordt via een risicoanalyse bepaald welke passende maatregelen aanvullend getroffen moeten worden.

2.3 Scope

Het concern informatiebeveiligingsbeleid is van toepassing op **alle informatie van de gemeente**, waarvan de gemeente eigenaar, leverancier en/of afnemer is, en worden verwerkt door de processen en onderliggende informatiesystemen van de gemeente, (keten)partners, samenwerkingsverbanden en/of diensten. Het is ook van toepassing op de informatie en dienstverlening welke door externe partijen worden uitgevoerd namens gemeente Rotterdam.

Het concern informatiebeveiligingsbeleid is van toepassing voor alle processen van de gemeente en borgt daarmee de informatievoorziening gedurende de **hele levenscyclus van**

informatie-systemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT en informatie. Het heeft ook betrekking op het bestuur, management, alle medewerkers, bezoekers en externe relaties.

Dit informatiebeveiligingsbeleid is **locatie-onafhankelijk** en omvat alle locaties die onder de verantwoordelijkheid vallen van gemeente Rotterdam. De doelstellingen en bestuurlijke principes voor informatiebeveiliging die de gemeente stelt zijn ook van toepassing op momenten wanneer medewerkers zich met informatie van de organisatie buiten deze locaties bevinden. Denk hierbij bijvoorbeeld aan de ambulante medewerkers en het (massaal) thuiswerken.

Het concern informatiebeveiligingsbeleid is een **algemene basis** en dekt tevens **aanvullende beveiligingseisen** uit wetgeving af zoals voor de gemeentelijke basisregistraties, BRP, PNIK en SUWI.

Er zijn **meerdere domeinen** waar informatiebeveiliging raakvlakken mee heeft. Informatiebeveiliging houdt zich bezig met het beveiligen van **alle** (gevoelige) gegevens die binnen de gemeente worden verwerkt. Dit maakt dat het domein privacy, waarbij privacygevoelige gegevens dienen te worden beschermd met passende organisatorisch en technische beveiligingsmaatregelen, raakvlakken heeft met het domein van informatiebeveiliging. Domeinen naast privacy waar ook raakvlakken mee zijn, zijn beschreven in paragraaf 3.6. De beleidsmatige aspecten (wat mag wel en wat mag niet) van deze domeinen vallen buiten de scope van dit concern informatiebeveiligingsbeleid. Waar deze domeinen inhoudelijk betrekking hebben op de informatiebeveiligingscomponent (hoe beschermen we informatie) valt dit binnen de scope van het concern informatiebeveiligings-beleid.

2.4 Dreigingslandschap gemeente Rotterdam

Gemeente Rotterdam heeft te maken met een alsmaar veranderend dreigingslandschap. De arena rondom digitale aanvallen wordt niet alleen groter en intensiever, maar ook complexer. Actoren spelen daarop in en maken misbruik van de actualiteit, zoals de verkiezingen in een land of bij de pandemie. De steeds verdergaande digitalisering leidt tot een verdere vergroting van de aanvalsmogelijkheden. De groep actoren die beschikt over geavanceerde aanvalscapaciteiten groeit. De digitale dreiging is permanent, actoren blijven digitale middelen inzetten voor spionage, verstoring en sabotage om eigen doelen (bijvoorbeeld wraak, geldelijk gewin of ideologie) te bereiken. Digitale incidenten kunnen leiden tot maatschappij-ontwrichtende schade, waar ook gemeente Rotterdam waakzaam en weerbaar voor moet zijn, inclusief de impact die digitale incidenten kunnen hebben op de gemeentelijke organisatie.

Het is onmogelijk om incidenten helemaal te voorkomen. Wat we wél kunnen doen is weerbaarder worden, weten wat we moeten doen wanneer een digitale incident de gemeente treft zodat de negatieve gevolgen zo klein mogelijk worden gehouden. Goed voorbereid zijn en klaar staan, dat is de veerkracht van gemeente Rotterdam op het gebied van informatiebeveiliging. Deze veerkracht en weerbaarheid is gedefinieerd als de activiteiten die nodig zijn om netwerk- en (keten-)informatiesystemen, de gebruikers van dergelijke systemen, en andere personen die getroffen (kunnen) worden door cyberdreigingen, te beschermen. Om voorbereid te zijn, onderhoudt gemeente Rotterdam een dreigingsbeeld als continue monitor.

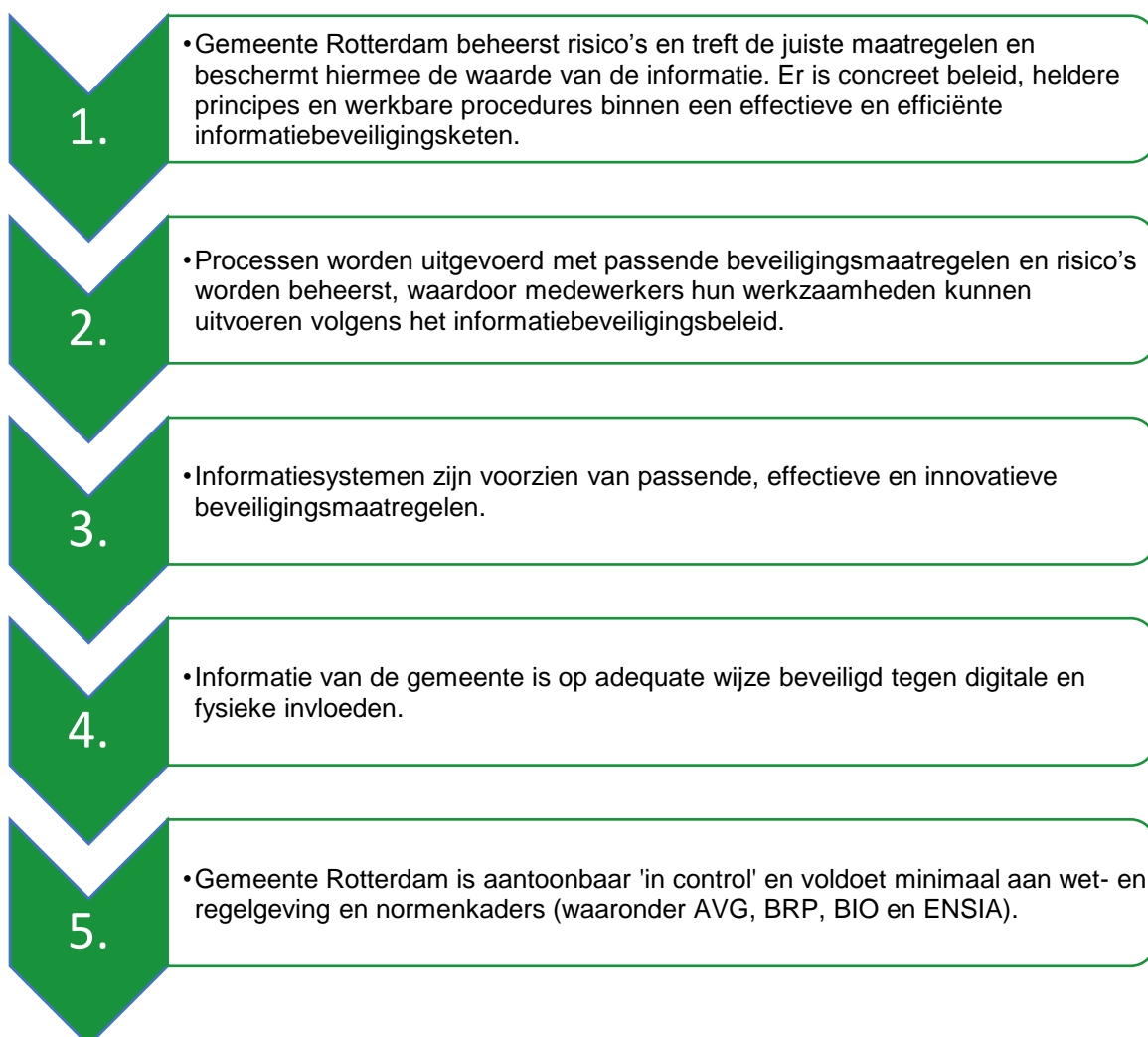
Het onderkennen en kunnen herkennen van dreigingen is randvoorwaardelijk voor een snelle en accurate respons. Om goede risicoafwegingen te kunnen maken en te kunnen prioriteren in de te treffen maatregelen, moet duidelijk zijn wat de meest relevante dreigingen zijn. Het Dreigingsbeeld Informatiebeveiliging Gemeente Rotterdam 2021-2023 biedt hier inzicht in. Vanuit het perspectief van nationale veiligheid liggen de dreigingen vooral op het vlak van (voorbereidingen voor) sabotage en spionage door statelijke actoren. Ook (grootschalige) uitval van digitale diensten, processen of systemen vormt een dreiging. Verder is er de dreiging

die uitgaat van criminele actoren die het te doen is om economisch gewin. De dreigingen die een risico vormen voor de nationale veiligheid zien we ook terug op lokaal niveau. De dreiging van binnenuit levert echter het grootste risico op voor gemeente Rotterdam, zowel onbedoeld (door menselijke en/of technische fouten) als opzettelijk (medewerkers met kwade bedoelingen).

Het dreigingsbeeld en de onderliggende dreigingsanalyses die de gemeente hier periodiek op uitvoert, vormt het kloppend hart van het gemeentelijke informatiebeveiligingsproces. En stelt de gemeente beter in staat om haar kennis, aandacht en geld aan de belangrijkste dreigingen en kwetsbaarheden te besteden.

2.5 Doelstellingen Concern Informatiebeveiligingsbeleid

Het concern informatiebeveiligingsbeleid beschrijft de vijf doelstellingen op het gebied van informatiebeveiliging waarmee gemeente Rotterdam zorgt voor geformaliseerde en gestructureerde uitvoering van informatiebeveiliging waarbij de beheersing aantoonbaar is. Deze vijf doelstellingen zijn:



Deze doelstellingen zijn leidend voor het Meerjarenplan Informatiebeveiliging, waarin een overzicht en prioritering van alle trajecten en activiteiten tot en met 2023 is uitgewerkt langs de indeling van 'beleid', 'uitvoering' en 'control'. Het meerjarenplan ondersteunt hiermee de gemeente Rotterdam in de verantwoordelijkheid op het gebied van informatiebeveiliging.

2.6 Doelgroepen

Het concern informatiebeveiligingsbeleid is bedoeld voor iedereen in en rond de gemeentelijke organisatie. In onderstaande tabel zijn de verschillende doelgroepen samengebracht, inclusief de relevantie, en verwijzing naar onderliggende bronnen, van diezelfde doelgroep naar het thema van informatiebeveiliging.

Doelgroep	Relevantie
College van B en W	Integrale verantwoordelijkheid om de gemeentelijke informatiehuishouding veilig te organiseren (1)
Gemeentesecretaris	Eindverantwoordelijk voor beveiligingsbeleid en voor de uitvoering van de organisatie brede vraagstukken ten aanzien van de informatiebeveiliging (2)
Proceseigenaren	Verantwoordelijk voor de beveiliging van het betreffende proces, data, en/of informatiesysteem (2)
Directeuren, afdelingshoofden, teamleiders, projectmanagers en projectleiders	Als eerste lijn verantwoordelijk voor realiseren van de organisatiedoelen, doelmatige inzet van middelen en weloverwogen omgaan met de risico's die de gemeente loopt (3)
Informatiebeveiligings-functionarissen	Als tweede lijn de adviestaat voor informatiebeveiliging aan de eerste lijn (3) Verstrekken van concern brede kaders, methodieken en formats (3) Vaststellen dat de concern brede kaders, methodieken en formats worden toegepast (3)
Financial Audit en Concern Auditing	Vaststellen gezamenlijke functionering eerste en tweede lijn om doelstelling te realiseren (doelmatig en doeltreffend) (3)
Dienstenleveranciers	Organisaties in de markt waaraan de gemeentesecretaris of proceseigenaar een (deel van) de beveiligingstaak in- of uitbesteedt (2)
Medewerkers	Toepassen van de regels en procedures aangaande informatiebeveiliging (2)

Legenda bronnen informatieveiligheid:

(1) VNG resolutie "informatieveiligheid"

(2) BIO, versie 2020

(3) Kadernota 'Sturen en Verantwoorden Rotterdam 2020'

2.7 Besluitvorming

Het concern informatiebeveiligingsbeleid is vastgesteld door het college van B en W voor de periode 2021-2023. Hiermee komt het oude informatiebeveiligingsbeleid (van 2018) te vervallen.

Jaarlijks wordt in het ENSIA-verantwoordingsproces, het informatiebeveiligingsbeleid getoetst op effectiviteit en actualiteit. Uiterlijk 2023 zal het informatiebeveiligingsbeleid, waar nodig, worden aangepast en opnieuw ter vaststelling worden aangeboden. Indien een nieuw informatiebeveiligingsbeleid nog niet is vastgesteld, dan blijft het huidige informatiebeveiligingsbeleid tot dat moment van toepassing.

3 Uitgangspunten voor informatiebeveiliging

Dit hoofdstuk beschrijft de uitgangspunten voor informatiebeveiliging die gelden binnen gemeente Rotterdam. De uitgangspunten bestaan uit de strategische doelen die de gemeente zichzelf heeft gesteld en de bestuurlijke principes die de gemeente hanteert om deze doelen te realiseren. Informatiebeveiliging is een thema wat niet op zichzelf staat. De verschillende domeinen waarmee informatiebeveiliging een relatie heeft zijn toegelicht evenals de cruciale rol van een informatieveilige cultuur en informatiebeveiliging bewustwording.

3.1 Strategische doelen informatiebeveiliging

Het concern informatiebeveiligingsbeleid streeft de volgende strategisch doelen na:

1. Het managen van de informatiebeveiliging.
2. Adequate bescherming van informatie en bedrijfsmiddelen.
3. Het minimaliseren van risico's van menselijk gedrag.
4. Het voorkomen van ongeautoriseerde toegang.
5. Het garanderen van correcte en veilige informatievoorzieningen.
6. Het beheersen van de toegang tot informatiesystemen.
7. Het waarborgen van veilige informatiesystemen.
8. Het adequaat reageren op incidenten.
9. Het beschermen van kritieke bedrijfsprocessen.
10. Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
11. Het waarborgen van de naleving van dit beleid.

3.2 Bestuurlijke principes informatiebeveiliging

Het concern informatiebeveiligingsbeleid sluit aan bij de tien bestuurlijke principes¹ die de gemeente Rotterdam toepast, welke de bestuurlijke aanvulling is op het normenkader BIO en gaat over de waarden die de bestuurders hanteren en uitdragen.

Deze principes zijn 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 ervan en de hieruit voortvloeiende werkwijze van de gemeente.

Als aanvulling op deze tien bestuurlijke principes, onderkent gemeente Rotterdam, de volgende vier bestuurlijke principes voor informatiebeveiliging.

1. De **samenwerking** tussen de informatiebeveiligingsorganisatie en de domeinen waar raakvlakken mee zijn, is cruciaal voor het borgen van een betrouwbare en open omgeving binnen de gemeente.
2. Een belangrijk uitgangspunt van informatiebeveiliging is het principe **security-by-design**. Door security-by-design toe te passen ontwikkelt en implementeert gemeente Rotterdam in een zo vroeg mogelijk stadium passende informatiebeveiligingsmaatregelen. De gemeente schenkt bij het ontwikkelen en implementeren van nieuwe processen, applicaties en innovaties (bijvoorbeeld AI, algoritmes en chatbots) aandacht aan bestaande en toekomstige dreigingen en het benoemen en mitigeren van de beveiligingsrisico's. Bij het toepassen van dit uitgangspunt maakt gemeente Rotterdam gebruik van interne en externe standaarden.
3. Bij het toepassen van deze bestuurlijke principes moet altijd worden gezocht naar een goede **balans** tussen informatieveiligheid, gebruiksvriendelijkheid (werkbaarheid) en kosten. Aangezien niet alle risicovolle situaties volledig af te dekken zijn met

¹ https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/01/De-10-bestuurlijke-principes-voor-Informatiebeveiliging_20190109.pdf

beveiligingsmaatregelen, legt gemeente Rotterdam de gemaakte keuzes vast ten behoeve van verantwoording en evaluatie.

4. De gemeente Rotterdam werkt zowel **norm- als risico-gebaseerd**. De proceseigenaar, gemandateerd door de concerndirecteur, is verantwoordelijk voor de beveiliging van het betreffende proces, data, en/of informatiesysteem. Het is daarom aan de proceseigenaar om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de proceseigenaar acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming.

3.3 Wet- en regelgeving

De juridische grondslag van het concern informatiebeveiligingsbeleid is terug te vinden in wet- en regelgeving. Wetten en regelingen die van toepassing zijn (niet limitatief): Wet Openbaarheid van Bestuur (WOB), Algemene Verordening Gegevensbescherming (AVG), Wet Computercriminaliteit II, Comptabiliteitswet, Archiefwet, Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007), Wet SUWI, Wet GBA en wet BRP.

Naleving van regels vergt steeds meer externe verantwoording, bijvoorbeeld voor gebruik van DigiD², SUWI³ en BRP⁴. Aanvullend op dit informatiebeveiligingsbeleid kunnen daarom specifieke regels gelden, bijvoorbeeld op grond van de Archiefwet, de wet BRP of SUWI. Rotterdam sluit aan bij de landelijk ingevoerde ENSIA.

Voor alle categorieën informatie is de bewaartermijn bepaald in overeenstemming met wet- en regelgeving, contractuele verplichtingen en bedrijfsmatige eisen.

Bij het (laten) vervaardigen en installeren van programmatuur wordt er voor gezorgd dat de intellectuele eigendomsrechten die daar op rusten niet worden geschonden.

3.4 Normen en standaarden

De ontwikkelingen in de informatietechnologie gaan steeds sneller en de wetgeving rondom de bescherming van persoonsgegevens is aangescherpt. Een breed erkende internationale norm om informatie(systemen) adequaat te beveiligen is vastgelegd in de ISO27001/2. Voor de Nederlandse overheid is deze norm vertaald naar een zogenaamde Baseline Informatiebeveiliging Overheid (BIO⁵) met daarin de regels waaraan alle overheidslagen dienen te voldoen. Door middel van een zelfevaluatie (ENSIA) verantwoorden gemeenten zich over deze norm.

De gemeente past de normen en standaarden toe die als aanvulling op de ISO27001/2 en de BIO dienen, zoals de wereldwijde beveiligingsstandaard IEC 62443 voor industriële controlesystemen (ICS) en veilig software ontwikkelen (SSD, NPR5326 en IEC25010) en voor veilige en toegankelijke websites ontwikkelen. Ook past gemeente Rotterdam standaarden en producten toe welke ontwikkeld zijn door de Informatiebeveiligingsdienst voor gemeenten (IBD) en het Nationaal Cyber Security Centrum (NCSC).

3.5 Strategisch risicomanagement

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" (Bron: Concern Integraal Beveiligingsbeleid Rotterdam).

Strategisch risicomanagement is het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van informatiebeveiliging risico's

² DigiD: Naam van het systeem waarmee Nederlandse overheden op internet iemand identiteit verifiëren

³ SUWI: Wet Structuur Uitvoeringsorganisatie Werk en Inkomen

⁴ BRP: Basisregistratie Personen

⁵ Zie Staatscourant 2019, nr 26526: <https://zoek.officielebekendmakingen.nl/stcrt-2019-26526.html>

en benutten van kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes.

Gemeente Rotterdam beschikt over een strategisch risicomanagement proces. Binnen dit proces werken de doelgroepen (zie paragraaf 2.6) samen bij het maken van een weloverwogen keuze en goede balans tussen risico's, maatregelen en dreigingen.

3.6 Overige domeinen

De bestuurlijke principes (zie paragraaf 3.2) hanteert de gemeente Rotterdam ten aanzien van het informatiebeveiliging-domein. Daarnaast onderkent de gemeente Rotterdam de raakvlakken en/of afhankelijkheid met de volgende domeinen waarop informatiebeveiliging een positieve impact heeft. Per domein is een korte toelichting gegeven hoe de gemeente de samenhang met het andere domein ziet vanuit strategisch perspectief:

- **Privacy:** De verantwoordelijke voor het verwerken van persoonsgevoelige informatie dient te voldoen aan de wettelijke verplichtingen zoals de AVG. Hierbij richt privacy zich specifiek op de risico's die impact hebben voor individuen, voor mensen, voor burgers; om hierbij de rechten en vrijheden van natuurlijke personen te waarborgen.
Gemeente Rotterdam is als verwerkingsverantwoordelijke verplicht om passende organisatorische en technische beveiligingsmaatregelen te treffen, in lijn met de artikelen 5, 24 en 25 en 32 van de AVG. Daarnaast moet gemeente Rotterdam kunnen laten zien dat de juiste organisatorische en technische maatregelen zijn genomen om de persoonsgegevens te beveiligen.
Om veilig persoonsgegevens te verwerken maakt gemeente Rotterdam onder andere gebruik van privacy-by-design en beveiligingsmaatregelen zoals het autoriseren van toegang, het loggen van applicatie-gebruik en het risico-bewustzijn van de medewerkers. Daarnaast heeft gemeente Rotterdam de werkprocessen waarin persoonsgegevens worden verwerkt, vastgelegd in een verwerkingsregister.
- **Informatiebeheer:** De verantwoordelijke voor het verwerken, opslaan en verwijderen van informatie past de kaders en richtlijnen van informatiebeheer toe. Om dit veilig te doen is informatiebeheer afhankelijk van de beveiligingsmaatregelen die hiervoor ontwikkeld zijn. Denk hierbij aan het versiebeheer, het maken en terug zetten van backups, het veilig archiveren van maatregelen en het toepassen van de wettelijke bewaartermijnen.
- **Architectuur:** De verantwoordelijke van een proces hanteert architectuur principes om de voorgestelde aanpassingen te toetsen tegen de bestaande principes, richtlijnen en modellen van de gemeente. Hiermee borgt architectuur dat veranderingen in lijn met de gemeentelijke afspraken getoetst en beschreven zijn. Zo ook op het gebied van informatiebeveiliging. Informatiebeveiligingsarchitectuur is hiermee de set van samenhangende modellen en principes die efficiënt en flexibel richting geeft aan het implementeren van het concern informatiebeveiligingsbeleid, zodat de gemeente de juiste beveiligingsmaatregelen treft en onderhoud.
- **Fysieke veiligheid:** De verantwoordelijke van het pand of de ruimte verschaft alleen geautoriseerde toegang tot panden of ruimtes waar gevoelige informatie fysiek of digitaal aanwezig is. De verantwoordelijke van het pand of de ruimte neemt maatregelen op basis van risicoafweging tot het beschermen van de aanwezige informatie conform de eisen uit het concern informatiebeveiligingsbeleid.
- **Personele veiligheid:** De verantwoordelijke zorgt ervoor dat medewerkers veilig hun taak kunnen uitvoeren. De verantwoordelijke zorgt ook voor het borgen van de betrouwbaarheid en integriteit van de medewerkers, zodat bewust foutief menselijk handelen zoveel mogelijk wordt voorkomen.

- **Business continuity management (BCM):** De verantwoordelijke van een proces draagt zorg voor het tijdige herstel van de werking van zijn proces in geval van een onderbreking als gevolg van een incident of calamiteit. Waar het gaat over de continuïteit van informatievoorziening worden de maatregelen genomen conform het concern informatiebeveiligingsbeleid.
- **Softwareontwikkeling:** De verantwoordelijke van een proces hanteert bij het ontwikkelen, het testen en het onderhouden van software, de normen en standaarden om te komen tot blijvend veilige software.
- **ICT beheer:** De verantwoordelijke voor een proces draagt zorg voor de het veilig beheer van applicaties, systemen en informatie. Het veilige beheer omvat een ruim scala aan on-premise systemen en onderdelen (zoals koppelingen) met de (externe) cloudoplossingen.
- **ICS/OT en IOT:** De verantwoordelijke van een proces houdt rekening met additionele veiligheidseisen die gesteld worden aan zogeheten Operational Technology (OT). Dit is een overkoepelende term voor onder andere Industrial Control Systems (ICS), Supervisory control and data acquisition systemen (SCADA), Programmable Logic Controllers (PLC), (Industrial) Internet of Things toepassingen (IIoT/IoT) en sensoren. Hieronder vallen bijvoorbeeld systemen voor het bedienen van bruggen, sluizen, gemalen, tunnels, verkeerslichten, camera's, parkeergarages, liften, toegangspoorten, (straat)verlichting en sensoren die enkel gebruikt worden voor dataverzameling. De gevolgen van een incident m.b.t. OT kunnen eerder levensbedreigend en/of maatschappij verstorend/ontwrichtend zijn dan van een incident m.b.t. kantoorautomatisering.
- **Cyber Resilience:** De verantwoordelijke van een proces draagt zorg voor de cyber resilience ervan. Digitalisering en nieuwe technologieën bieden grote maatschappelijke en economische kansen. Tegelijkertijd zorgen deze ontwikkelingen ook voor dreigingen en kwetsbaarheden. Nieuwe technieken, diensten en aanbieders maken dat de maatschappelijke afhankelijkheid van internet en ICT-middelen steeds groter wordt en dat de fysieke en digitale wereld steeds meer verweven raken. Gemeente Rotterdam krijgt naast fysieke crises ook te maken met digitale crises of crises met een digitale component. Bij cyber resilience, oftewel digitale weerbaarheid, gaat het om de veerkracht van een organisatie en haar digitale systemen en processen. Cyber resilience wordt uitgedrukt in de snelheid en effectiviteit waarmee een organisatie zich weet te herstellen na een incident⁶. Waar het gaat over de weerbaarheid van het proces worden de maatregelen genomen conform het concern informatiebeveiligingsbeleid.

Het concern informatiebeveiligingsbeleid van gemeente Rotterdam is eveneens van toepassing binnen al deze domeinen.

3.7 Verhogen Digitale Weerbaarheid

Informatieveiligheid is een zaak van alle medewerkers. Zij zijn cruciaal om de digitale weerbaarheid van de gemeente te verhogen. Om dit te ondersteunen zijn de aandachtspunten:

De mens centraal

De toegenomen afhankelijkheid van internet in het maatschappelijke en zakelijke verkeer, de voortschrijdende digitalisering van de dienstverlening, het toegenomen gebruik van sociale netwerken en de opslag van informatie in de cloud, creëren nieuwe beveiligingsrisico's voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. De mens is een belangrijke schakel in het grotere geheel van informatiebeveiliging. De mate waarin medewerkers zich bewust zijn van de dreigingen die aan het cyberlandschap en de gemeentelijke processen, informatiesystemen en informatie verbonden zijn en veilig gedrag vertonen, bepaalt de sterkte en zwakte van deze schakel.

⁶ <https://www.nctv.nl/actueel/nieuws/2019/10/01/cybersecurity-woordenboek-maakt-lastige-terminologie-begrijpelijk>

Attitude en gedrag

De meeste inbreuken op de vertrouwelijkheid en integriteit van de gegevens worden veroorzaakt door onbewust verkeerd handelen. Om het risico op dit onbewust en ongewenst verkeerd handelen te bestrijden, zet de gemeente in op het creëren van een goede veiligheidscultuur; een cultuur waar medewerkers risico's en bedreigingen meewegen als onderdeel van hun dagelijkse routine. Om een goede veiligheidscultuur binnen de gemeente op te bouwen, is een structurele cultuurverandering nodig. Een verandering waarbij het juiste gedrag wordt bevorderd en er een open cultuur ontstaat waarin men elkaar aanspreekt op fout en goed gedrag. Het uiteindelijke doel is om een informatieveilige en privacy-veilige cultuur te bouwen die in het DNA van gemeente Rotterdam verankerd is. Dit is niet gemakkelijk te realiseren, aangezien het een langdurig proces is waarvoor een integrale aanpak en veel deskundige inzet nodig zijn.

Informatiebeveiliging cultuur

Organisatorische en technische maatregelen om informatie te beveiligen werken alleen als bestuur, management en medewerkers de noodzakelijke houding en gedrag vertonen. Gedrag heeft te maken met iets ongrijpbaars als de 'organisatiecultuur'. Een gestructureerde aanpak maakt het ongrijpbare toch hanteerbaar. Maar het vereist wel een voortdurend proces, dat zijn basis vindt in een duidelijke strategie en een verdere uitwerking in een concreet stappenplan. Het voorbeeldgedrag door het management is daarbij van wezenlijk belang, van boven naar beneden.

Informatiebeveiliging is van iedereen, medewerkers zijn zich bewust van de waarde en de gevoeligheid van de informatie. Het management ondersteunt continue het veilig werken en het daarbij horende gedrag om gezamenlijk de kans op een datalek, hack of incident te voorkomen. Veilig werken wordt beloond, medewerkers schromen zich niet om onveilige situaties te bespreken of te melden, de middelen om veilig te werken zijn beschikbaar sluiten aan bij de behoefte van de medewerkers om veilig te werken.

Het veilig werken wordt rondom deze middelen en het gedrag structureel ondersteund door gedragsregels, continue doorlopende bewustwordingscampagnes, e-learning en berichten over actuele en nieuwe dreigingen.

Crisis oefeningen

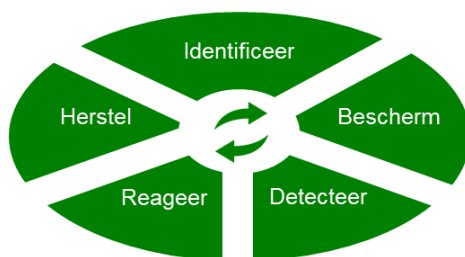
Crisisoefeningen zijn een goede manier om met digitale dreigingen en weerbaarheid van de organisatie aan de slag te gaan. Hierbij leren we gezamenlijk, doen we ervaringen op en zijn we uiteindelijk beter voorbereid op potentiële ontwrichting bij een incident. Door met regelmaat te oefenen en het ervaren van een crisis, verhogen we de digitale weerbaarheid. Goed voorbereid zijn als gemeente is dan ook van cruciaal belang, om digitale ontwrichting te voorkomen en om alle digitale dienstverlening veilig en bereikbaar te houden.

4 Organisatie van informatiebeveiliging

Dit hoofdstuk beschrijft hoe de taken en verantwoordelijkheden ten aanzien van informatiebeveiliging in gemeente Rotterdam belegd zijn. Binnen deze methodiek is het managementsysteem voor informatiebeveiliging leidend. De beschreven taken en verantwoordelijkheden sluiten aan bij het 'Concern Integraal Beveiligingsbeleid' en het binnen de gemeente bekende Three Lines-model. In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO, DISO's, Security Management, Security Operations Center (SOC) e.a.) ondersteunt, adviseert, coördineert, monitort en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

4.1 Managementsysteem

Binnen gemeente Rotterdam is informatiebeveiliging ingericht als een continu verbeterproces en sluit aan op de bestuurlijke P&C cyclus. Dit managementsysteem van informatiebeveiliging, in het vakgebied ook wel Information Security Management System (ISMS) genoemd, bestaat uit een vijftal stappen: Identificeer, Bescherm, Detecteer, Reageer en Herstel.



Titel: Gemeente Rotterdam - Informatieveiligheid is een continu proces

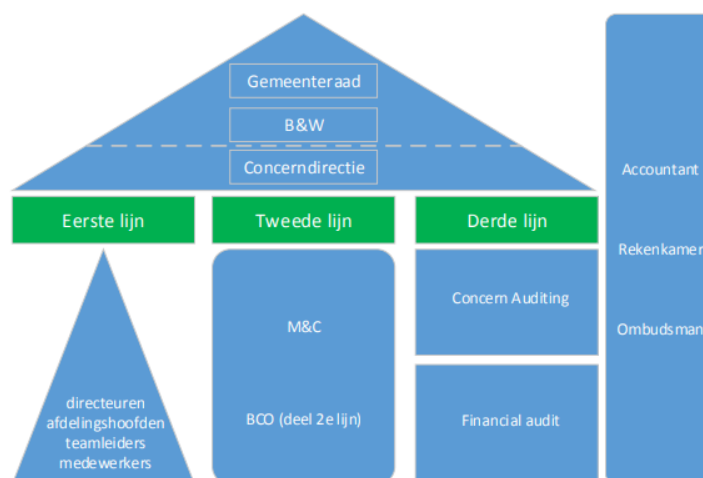
Met het doorlopen van de stappen Identificeer en Bescherm verlaagt de gemeente de kans van het optreden van een incident of kwetsbaarheid. De stappen Detecteer, Reageer en Herstel stelt de gemeente in staat de impact bij het optreden van een incident of kwetsbaarheid te verlagen.

Met dit management systeem werkt de gemeente aan de best mogelijk invulling van en maatregelen voor een *betrouwbare* informatievoorziening. Het concern brede ISMS ondersteunt het college van B en W en de concerndirectie in het maximaal 'in control' zijn van de informatieveiligheid.

Door periodieke controle en verantwoording, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het concern informatiebeveiligingsbeleid vormt samen met het Meerjarenplan Informatiebeveiliging het fundament onder een betrouwbare informatievoorziening. In het Meerjarenplan Informatiebeveiliging wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van externe ontwikkelingen in wet- en regelgeving, dreigingen, op basis van interne eisen aan vernieuwing van digitalisering, bevindingen naar aanleiding van uitgevoerde risicoanalyses en uit registraties in het incidentenregister.

4.2 Verschillende rollen en verantwoordelijkheden

De verschillende rollen en verantwoordelijkheden ten aanzien van informatiebeveiliging zijn conform het Three-Lines model⁷ beschreven en geïmplementeerd binnen de gemeente.



Bron: Kadernota Sturen en Verantwoorden Rotterdam 2020

De first line (hierna: de eerste lijn) wordt gevormd door alle functionarissen die hiërarchisch of functioneel andere medewerkers aansturen en namens hen verantwoording afleggen. De eerste lijn, de concerndirectie en het management binnen de clusters zijn verantwoordelijk voor de resultaten, de uitvoering, nakoming van regels en de effectiviteit ten aanzien van informatiebeveiliging.

De second line (hierna: de tweede lijn) wordt gevormd door functionarissen die, onafhankelijk zijn van de eerste lijn. De tweede lijn, de informatieveiligheid-gebaseerde functies binnen de gehele informatiebeveiligingsketen zijn verantwoordelijk voor het stellen van kaders en regels. Alsmede voor advisering inzake informatieveiligheid en voor het op een objectieve wijze voeren van toezicht op en rapporteren over de uitvoering, het management, de beheersing en de verslaglegging van informatiebeveiligingsrisico's.

De third line (hierna: de derde lijn) wordt gevormd door de Functionaris Gegevensbescherming (FG) en de afdelingen Financial Audit en Concurrence Auditing. De derde lijn, is de onafhankelijk rol binnen de gemeente die verantwoordelijk is voor het geven van een onafhankelijk oordeel over de mate van functioneren van de interne informatiebeveiligingsmaatregelen. De derde lijn heeft verder een coördinerende rol richting de externe auditor en de toezichthouders.

4.3 Controle en verantwoording

Dit concern informatiebeveiligingsbeleid is een verantwoordelijkheid van het bestuur van gemeente Rotterdam. De bestuurders en concerndirecteuren van gemeente Rotterdam zullen volgens de strategische principes voor informatiebeveiliging en het concern brede management systeem richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De concerndirectie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan de bestuurlijke portefeuillehouders. De concerndirectie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit concern informatiebeveiligingsbeleid.

⁷ Kadernota 'Sturen en Verantwoorden Rotterdam 2020'

De gemeente verantwoordt zich jaarlijks over informatiebeveiliging middels de ENSIA-systematiek, gebaseerd op de normen die gelden voor de overheid, de BIO. De aangestelde ENSIA-coördinator zorgt ervoor dat de informatie die nodig is voor het beantwoorden van de audit-vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke proceseigenaren. De proceseigenaren leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten. Op basis van ENSIA vindt enerzijds de verantwoording aan de gemeenteraad plaats via een collegeverklaring informatiebeveiliging. Anderzijds vindt verantwoording plaats richting de toezichthouders van de ministeries inzake informatiebeveiliging van de BRP, SUWI, DigiD, BAG, ed..



Bron: VNG-realizatie; ENSIA

Middels deze verantwoording worden het college van B en W van gemeente Rotterdam en de gemeenteraad geïnformeerd. De betrokkenheid van het Gemeentebestuur is essentieel, en laat zien dat de gemeente Rotterdam informatiebeveiliging serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

4.4 Afwijkingen van bestaand beleid en regelgeving

De implementatie van maatregelen kost in veel gevallen geld en/of tijd van de medewerkers en de gemeente. Omdat dit schaarse middelen zijn, kan het voorkomen dat bepaalde en dus benodigde beveiligingsmaatregelen niet of onvoldoende (tijdig) kunnen worden geïmplementeerd.

Afwijkingen van het concern informatiebeveiligingsbeleid en informatiebeveiligingsmaatregelen worden door de proceseigenaar inclusief een advies van de informatiebeveiligingsfunctionaris ter beoordeling voorgelegd aan de desbetreffende cluster directeur en bij cluster overstijgende impact aan de concerndirectie. De toegestane afwijkingen zullen aan een termijn van maximaal één jaar zijn gebonden. Voor het verstrijken van deze termijn dient de herbeoordeling plaats te vinden en ter beoordeling worden voorgelegd aan de cluster en/of concerndirectie.

Het desbetreffende cluster zorgt ervoor dat de besluitvorming rond deze afwijkingen goed gedocumenteerd wordt en steeds voor audits toegankelijk is. De informatiebeveiligingsfunctionaris bewaakt het totaaloverzicht en ziet er op toe dat de termijnen zorgvuldig bewaakt en gehandhaafd worden.

Bijlage A: Relevante documenten en bronnen

Relevante documenten en bronnen	Vindplaats	URL
Algemene Verordening Gegevensbescherming (AVG)	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	https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/
Collegetargets 2018-2022	Website gemeente Rotterdam	https://www.rotterdam.nl/bestuur-organisatie/collegetargets-2018-2022/
Concern Informatiebeheerbeleid Rotterdam	Intranet gemeente Rotterdam	Wet- en regelgeving - RIO (rotterdam.nl)
Concern Integraal Beveiligingsbeleid Rotterdam		
Kadernota 'Sturen en Verantwoorden Rotterdam 2020'	Intranet gemeente Rotterdam	Kaders, beleid en richtlijnen - RIO (rotterdam.nl)
VNG resolutie 'Digitale Veiligheid: kerntaak voor de gemeenten'	Website VNG	https://vng.nl/nieuws/meer-prioriteit-voor-beveiliging-digitale-systemen-gemeenten
Regeling ICT- en informatiegebruik	Website Bestuurlijk Informatiesysteem Rotterdam	https://www.bis.rotterdam.nl/dossiers/43022
Meerjarenplan Informatiebeveiliging		
Informatiebeveiligingsbeleid (2018)	Website Raadsinformatie gemeente Rotterdam	https://rotterdam.raadsinformatie.nl/document/6124517/1#search='informatiebeveiligingsbeleid'
De 10 bestuurlijke principes voor informatiebeveiliging	Website VNG	https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor-20190109.pdf
ISO 27001 en 27002	Website NEN	https://www.nen.nl/ict/cyber-privacy/informatiebeveiliging
IEC 62443	Website NEN	https://www.nen.nl/
IEC25010	Website NEN	https://www.nen.nl/
NPR5326	Website NEN	https://www.nen.nl/
Verwerkingsregister gemeente Rotterdam	Website gemeente Rotterdam	https://www.rotterdam.nl/bestuur-organisatie/verwerkingsregister/
VNG-realisatie; ENSIA	Website VNG	https://www.vngrealisatie.nl/ensia