GGD
Amsterdam

Informatiebeveiligingsbeleid

GGD Amsterdam

Strategisch beleid voor informatiebeveiliging

Versiebeheer

Versies

Versie	Datum	Auteur	Samenvatting van de wijzigingen
0.1	12-12-2018	5.1,2,e	Initiële versie
0.2	18-12-2018	5.1,2,e	Initiële versie, verduidelijking organisatie en afstemming met privacybeleid
0.3	31-10-2019	5.1,2,e	Concept versie, document gedeeld met direct betrokken functionarissen
0.4	08-05-2020	5.1,2,e	Update concept versie
0.5	06-06-2020	5.1,2,e	Review opmerkingen verwerkt DPGA focusteam, I3 en IV-board
0.6	08-06-2020	5.1,2,e	Review opmerkingen verwerkt CIO-office (CISO en informatiebeveiligingsadviseur)
1.0	09-06-2020	5.1,2,e	Definitieve versie

Goedkeuring

Versie	Datum	Naam	Functie/rol
1.0	16-06-2020	5.1,2,e	Algemeen directeur GGD Amsterdam

Periodieke actualisering

Dit informatiebeveiligingsbeleid GGD Amsterdam treedt in werking na vaststelling directie GGD Amsterdam en vervangt alle voorgaande versies van het informatiebeveiligingsbeleid. Onderhoud en actualisatie van het informatiebeveiligingsbeleid GGD Amsterdam is belegd bij de ISO. Het beleid heeft een looptijd van drie jaar. Jaarlijks toetst de ISO of het beleid moet worden bijgesteld. Aanleidingen voor bijstelling kunnen zijn: herziene stedelijk kader informatiebeveiliging gemeente Amsterdam, voortschrijdend inzicht, gewijzigde wet- en regelgeving, substantiële veranderingen in ontwikkelingen, dreigingen of weerbaarheid, of noodzakelijke (tekstuele) aanpassingen als gevolg van organisatorische of technische wijzigingen.
Minimaal driejaarlijks of zo nodig eerder wordt het informatiebeveiligingsbeleid GGD Amsterdam volledig herzien. Mocht een nieuw beleid GGD Amsterdam binnen deze termijn nog niet zijn vastgesteld, dan blijft het huidige beleid GGD Amsterdam van toepassing.

Voorwoord

Dit document beschrijft het strategisch informatiebeveiligingsbeleid voor de GGD Amsterdam.

In onder meer het Cyber Security Beeld Nederland is een duidelijke trend zichtbaar van toenemende dreigingen en die ook de zorgsector steeds 'harder' kan raken (in de media verschijnen regelmatig berichten over informatiebeveiligingsincidenten die zich bij zorginstellingen hebben voorgedaan). Ook de GGD Amsterdam wordt door de toenemende digitalisering steeds meer afhankelijk van betrouwbare informatie en IT- infrastructurele voorzieningen en dient ten gevolge maatregelen te treffen om uitval in de operationele processen te voorkomen.

Het informatiebeveiligingsbeleid GGD Amsterdam is gebaseerd op de nationale standaard NEN 7510[1] (de Nederlandse norm voor informatiebeveiliging in de zorg). De NEN 7510, gebaseerd op de internationale norm ISO 27001, die kader weergeeft welke maatregelen genomen kunnen worden om op de juiste manier om te kunnen gaan met (persoons/cliënt)gegevens. De maatregelen zorgen ervoor dat de processen rondom informatiebeveiliging gecontroleerd verlopen en ze hebben betrekking op alle mogelijke vormen waarin gegevens van personen zijn vastgelegd.

[1] De GGD Amsterdam heeft besloten om te werken en te voldoen volgends de norm NEN 7510.

Samenvatting

De GGD Amsterdam stelt bij het verlenen van publieke gezondheidszorg de cliënt(veiligheid) centraal en cliënten mogen erop vertrouwen dat de GGD Amsterdam *informatieveilig* werkt. Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend geheel aan activiteiten, methoden, maatregelen en middelen om de informatievoorziening gedurende gehele levenscyclus zeker te stellen.

De kernpunten van informatiebeveiliging zijn:
- Beschikbaarheid: de informatie is (blijvend) toegankelijk en leesbaar.
- Integriteit: de informatie is juist en actueel.
- Vertrouwelijkheid: de informatie is beschermd en alleen toegankelijk voor bevoegden.

Het strategisch informatiebeveiligingsbeleid GGD Amsterdam sluit aan op het stedelijk kader informatiebeveiliging gemeente Amsterdam en is in overeenstemming met relevante (zorg specifieke) wet- en regelgeving. Dit informatiebeveiligingsbeleid is van toepassing op alle processen, onderliggende informatiesystemen, informatie en gegevens die GGD Amsterdam verwerkt en opslaat, het gebruik daarvan door medewerkers en (keten)partners in de breedste zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

De hoofddoelstelling van dit informatiebeveiligingsbeleid is het richting geven aan de wijze waarop informatie van de GGD Amsterdam wordt beveiligd. In het informatiebeveiligingsbeleid worden doelen gesteld, reikwijdte en uitgangspunten weergegeven, kerntaken en verantwoordelijkheden beschreven, de structuur geschetst, en de middelen benoemd waarmee dit beleid wordt vormgegeven.

De nationale norm - NEN 7510 - Informatiebeveiliging in de Zorg, vormt het basisnormenkader voor de zorgsector in Nederland. De GGD Amsterdam gaat volgens deze norm werken. De beheersmaatregelen uit de NEN7510 zijn gebaseerd op de internationale norm ISO 27001.
De werkwijze van de NEN 7510 is gericht op risicomanagement. Dit houdt in dat beslissers op voorhand keuzes maken en continu afwegingen maken om informatie op passende wijze beveiligd te houden in termen van beschikbaarheid, integriteit en vertrouwelijkheid.
Naast dit basisniveau kunnen specifieke beveiligingsmaatregelen vereist zijn; deze zijn veelal vastgelegd in wet- en regelgeving of als resultaat van een risicoafweging. Waar tot nu toe de aandacht vooral uitging naar het doorvoeren van maatregelen om informatie te beveiligen, is de aanpak nu nog méér risk-based, waarbij een standaard niveau het uitgangspunt is en daardoor al veel maatregelen standaard worden getroffen.

De Baseline Informatiebeveiliging Overheid (BIO) vormt het basisnormenkader voor de gehele overheid. De beheersmaatregelen zijn net als de NEN 7510 gebaseerd op de internationale norm ISO 27001 en komen overeen met elkaar.
GGD Amsterdam is een onderdeel van gemeente Amsterdam en zal ook aan de BIO beheersmaatregelen houden. De GGD Amsterdam zal zowel houden aan de zorg specifieke maatregelen/eisen uit de NEN 7510 als de verplichte maatregelen/eisen uit de BIO.

Informatiebeveiliging is een verantwoordelijkheid van alle betrokkenen binnen de GGD Amsterdam, ongeacht de aard en omvang van het proces.

Inhoud

Voorwoord **3**
Samenvatting **4**

1 Inleiding **6**
1.1 Introductie 6
1.2 Stedelijk kader informatiebeveiliging gemeente Amsterdam 6
1.3 Baseline Informatiebeveiliging Overheid (BIO) 7
1.4 Leeswijzer 7

2 Werkveld informatiebeveiliging **8**
2.1 Waarom aandacht voor informatiebeveiliging 8
2.2 Wat betekent informatiebeveiliging 9
2.2.1 Definitie informatiebeveiliging 9
2.2.2 Typen maatregelen 9
2.2.3 Werkingsgebied/scope informatiebeveiliging 11
2.2.4 Raakvlakken 12
2.3 Wat wilt GGD Amsterdam bereiken met informatiebeveiliging 12
2.3.1 Uitgangspunten 12
2.4 Basisniveau 13
2.5 Normenkaders 14

3 Governance **15**
3.1 Functies, rollen, kerntaken en verantwoordelijkheden 15
3.2 Sturing geven aan informatiebeveiliging 18

4 Risicomanagement en controle raamwerk **19**
4.1 Informatierisicomanagement - procesmatige aanpak en continue verbetering 19
4.1.1 Opstellen informatiebeveiligingsbeleid (plan) 20
4.1.2 Opstellen informatiebeveiligingsplan (plan) 20
4.1.3 Uitvoeren risicoanalyse (do) 20
4.1.4 Ontwerpen en implementeren maatregelen (do) 20
4.1.5 Uitvoeren geïmplementeerde maatregelen (check) 20
4.1.6 Toezicht houden op en monitoren uitvoering maatregelen (check) 21
4.1.7 Evalueren en bijstellen geïmplementeerde maatregelen (act) 21
4.1.8 Beoordelen effectiviteit maatregelen (act) 21
4.2 GGD controle raamwerk 22

Bijlage A **23**
Bijlage B **25**

1 Inleiding

1.1 Introductie

De GGD Amsterdam heeft als missie in haar werkgebied de gezondheid van de bevolking te beschermen en actief te bevorderen. Zij wil gezondheidsachterstanden verkleinen en zelfredzaamheid bevorderen om participatie te verbeteren. Deze missie sluit aan bij de wettelijke verplichtingen die de GGD als publieke gezondheidsdienst heeft op basis van de Wet publieke gezondheid. Ten behoeve van de realisatie van deze missie en de daaruit voortvloeiende doelstellingen worden diverse informatiesystemen gebruikt.

De GGD Amsterdam stelt bij het verlenen van publieke gezondheidszorg de cliënt(veiligheid) centraal en cliënten mogen erop vertrouwen dat de GGD Amsterdam *informatieveilig* werkt. Doel van het informatiebeveiligingsbeleid is om op strategisch niveau duidelijkheid te geven over de keuzes die gemaakt zijn ten aanzien van informatiebeveiliging. Het beleid geeft de afdelingen van de GGD Amsterdam een helder beeld van wat er in dat kader van hen wordt verwacht. Het beleid vormt een overkoepelend kader waarbinnen de afdelingen van de GGD Amsterdam -waar nuttig en noodzakelijk- een verdere uitwerking kunnen maken dat is gericht op de specifieke werkzaamheden en systemen van die afdelingen.

Het beleid is in overeenstemming met relevante (zorg specifieke) wet- en regelgeving, evenals de gemeentelijke kaders zoals verwoord in Stedelijk kader informatiebeveiliging gemeente Amsterdam[2].

Tot slot: informatieveilig werken is een iteratief groeiproces dat leidt tot een cultuur waarbij het gedrag wordt gedragen door regels en procedures (we werken hier veilig of we werken hier niet). Daarmee biedt dit beleid een eerste handreiking maar is nadrukkelijk vatbaar voor verbetering en aanscherping conform de gebruikelijke PDCA-cyclus.

1.2 Stedelijk kader informatiebeveiliging gemeente Amsterdam

Het informatiebeveiligingsbeleid GGD Amsterdam sluit aan op het stedelijk kader informatiebeveiliging van de gemeente Amsterdam[2] en het compliance statement van cluster Sociaal met een uitwerking van de kerntaken en verantwoordelijkheden voor informatiebeveiliging.

Een 'afzonderlijk' dan wel 'aanvullend' informatiebeveiligingsbeleid voor de GGD Amsterdam is gerechtvaardigd vanwege het gegeven dat de GGD Amsterdam binnen de Gemeente Amsterdam (zorg)specifieke werkzaamheden uitvoert, die voortvloeien uit onder meer de Wet publieke gezondheid, de Wet op de Geneeskundige Behandel Overeenkomst en de Wet maatschappelijke ondersteuning en voor verschillende afdelingen is specifieke wet- en regelgeving van toepassing. Inherent aan de uitvoering van deze werkzaamheden is dat van cliënten (bijzondere) persoonsgegevens worden verwerkt. Aan deze verwerkingen worden strenge eisen gesteld.

[2] Beleidskader informatiebeveiliging GMT20200402.pdf

De GGD Amsterdam beweegt zich in een complexe publieke (zorg)keten met een groot divers juridisch kader dat wordt gevormd door privacy wet- en regelgeving enerzijds en (zorg)specifieke wet- en regelgeving anderzijds. Dit juridisch kader wordt geduid door de Privacy Officers en de juridisch beleidsadviseurs van de GGD Amsterdam gezamenlijk. Zij treden met elkaar in overleg om de privacy van betrokkenen en de rechtmatigheid van gegevensverwerkingen binnen de GGD Amsterdam te waarborgen. Het privacybeleid van de GGD Amsterdam is hierbij richtinggevend, kader stellend en sluit aan op het stedelijk beleidskader privacy gemeente Amsterdam[3].

1.3 Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) vormt het basisnormenkader voor de gehele overheid, zo ook van toepassing voor de gemeente Amsterdam. De beheersmaatregelen zijn net als de NEN 7510 gebaseerd op de internationale norm ISO 27001.
GGD Amsterdam is een onderdeel van gemeente Amsterdam en zal ook aan de BIO beheersmaatregelen houden. De beheersmaatregelen van de BIO komen overeen met de NEN 7510. In de BIO zijn verplichte maatregelen/eisen voorgeschreven om aan de beheersmaatregelen te voldoen. De GGD Amsterdam zal zowel houden aan de zorg specifieke maatregelen uit de NEN 7510 als de verplichte BIO maatregelen om te voldoen aan de NEN 7510 en de BIO.

1.4 Leeswijzer

Het document is verder als volgt opgebouwd. In hoofdstuk twee wordt de context geschetst waarin de GGD Amsterdam opereert, komt het werkveld van informatiebeveiliging aan de orde en worden de uitgangspunten die aan dit beleid ten grondslag liggen beschreven. In hoofdstuk drie worden de kerntaken en verantwoordelijkheden geschetst en wanneer het beleid wordt geactualiseerd. Hoofdstuk vier beschrijft het proces van risicomanagement met betrekking tot informatiebeveiliging.

[3] stedelijk_kader_verwerken_persoonsgegevens_def_september_2018.pdf

2 Werkveld informatiebeveiliging

In dit hoofdstuk wordt het werkveld waarin de GGD Amsterdam opereert vanuit het perspectief van informatiebeveiliging beschreven. In §2.1 komen relevante ontwikkelingen voor informatie en technologie aan bod. In §2.2 wordt het werkveld geschetst van informatiebeveiliging en in §2.3 wordt het hoofdstuk afgesloten met de doelstellingen die de GGD Amsterdam met informatiebeveiliging wil bereiken, en welke uitgangspunten voor informatiebeveiliging gelden.

De GGD Amsterdam sluit aan op de gemeente Amsterdam brede informatiebeveiliging kaders, processen, procedures en handreikingen. Denk hierbij aan o.a. logische toegangsbeheer processen, dataclassificatie objecten, auditproces/cyclus, projectmanagement (PPM proces en bedrijfsvoering processen (o.a. personeelszaken, huisvesting, facilitair, ICT, etc.).

De kaders/documenten van de gemeente Amsterdam zullen in principe leidend zijn voor GGD Amsterdam. Mocht er maatwerk nodig zijn en/of er is geen gemeente Amsterdam brede document aanwezig, dan zal er advies ingewonden bij de Chief Information Security Officer (CISO).

2.1 Waarom aandacht voor informatiebeveiliging

Voor het realiseren van de (strategische) doelstellingen van de GGD Amsterdam en het uitvoeren van haar werkprocessen zijn gegevens en (digitale) informatiesystemen onmisbaar geworden en niet meer weg te denken uit de organisatie. De omgeving waarin de GGD Amsterdam actief is wordt, door de toenemende digitalisering van cliëntgegevens, inzet van eHealth- toepassingen en apps, uitwisseling van gegevens in de publieke (zorg)keten en mogelijkheden met data-analyse alsook door ontwikkelingen in het publieke (zorg)domein zelf, steeds complexer.

(Technologische) ontwikkelingen volgen elkaar in hoog tempo op en bieden steeds meer mogelijkheden en kunnen voor de GGD Amsterdam als volgt worden samengevat (voor een nadere toelichting hierop wordt verwezen naar bijlage A), toenemende:

- … behoefte aan stuur- en operationele informatie …
- … inzet van informatiesystemen …
- … uitwisseling van gegevens in de keten …
- … eisen vanuit wet- en regelgeving en interne en externe stakeholders …

Aan het gebruiken van informatie en technologie zijn (helaas ook) risico's verbonden die een negatieve invloed kunnen hebben op de werkprocessen van de GGD Amsterdam, en kunnen leiden tot (ernstige) verstoringen. Voorbeelden hiervan zijn:

- Aanval van een hacker, ransomware of een virus-uitbraak op het netwerk van de GGD Amsterdam waardoor applicaties niet kunnen worden gebruikt, hetgeen kan leiden tot het (tijdelijk) sluiten van afdelingen of (tijdelijk) staken van de dienstverlening.
- Op social media kunnen medewerkers en cliënten zich negatief uitlaten over de GGD Amsterdam wat kan leiden tot imagoschade.
- Verlies of diefstal van een tas met bedrijfsgevoelige informatie of een laptop met cliëntbestanden waardoor informatie in handen komt van onbevoegden. In geval van het verlies van cliëntinformatie

kan de privacy in het geding raken en sprake zijn van een datalek en de GGD Amsterdam een boete kan worden opgelegd.
- Medewerkers hun PC of laptop niet vergrendelen waardoor cliëntinformatie door onbevoegden kan worden gelezen.
- Onjuiste of onvolledige informatie wordt gebruikt voor het leveren van publieke gezondheidszorg.

Samenvattend kan worden gesteld dat, naast de vele mogelijkheden die informatietechnologie biedt, het niet betrouwbaar functioneren hiervan en/of het niet kundig omgaan met niet-betrouwbare of vertrouwelijke informatie (grote) consequenties kan hebben en de GGD Amsterdam schade kan berokkenen voor haar cliënten, ketenpartijen, medewerkers, imago en financiële positie. Naast mensen, middelen en financiën is informatie voor de GGD Amsterdam een 'strategisch productiemiddel' geworden en de hiermee gepaard gaande risico's moeten adequaat worden beheerst.

2.2 Wat betekent informatiebeveiliging

2.2.1 Definitie informatiebeveiliging

Informatiebeveiliging wordt gedefinieerd als een samenhangend stelsel van passende preventieve, detectieve, repressieve en correctieve maatregelen gericht op het waarborgen van de betrouwbaarheid van informatie en informatiesystemen, gedurende de gehele levenscyclus.

Kernpunten daarbij zijn:
- Beschikbaarheid (de informatie is (blijvend) toegankelijk en leesbaar): mate waarin informatie op het juiste moment beschikbaar is voor medewerkers. Onder beschikbaarheid valt tevens continuïteit en heeft betrekking op de periode waarbinnen -in geval van een calamiteit- de oorspronkelijke situatie kan worden hersteld.
- Integriteit (de informatie is juist en actueel): mate waarin informatie juist, volledig en/of tijdig is.
- Vertrouwelijkheid (de informatie is beschermd): mate waarin toegang tot informatie beperkt is tot degenen die daartoe bevoegd zijn. Indien sprake is van (bijzondere) persoonsgegevens (van cliënten of medewerkers) wordt gesproken over privacy.
- Controleerbaarheid: mate waarin kan worden vastgesteld in hoeverre informatie betrouwbaar is verwerkt en heeft voldaan aan vigerende wet- en regelgeving (compliance).

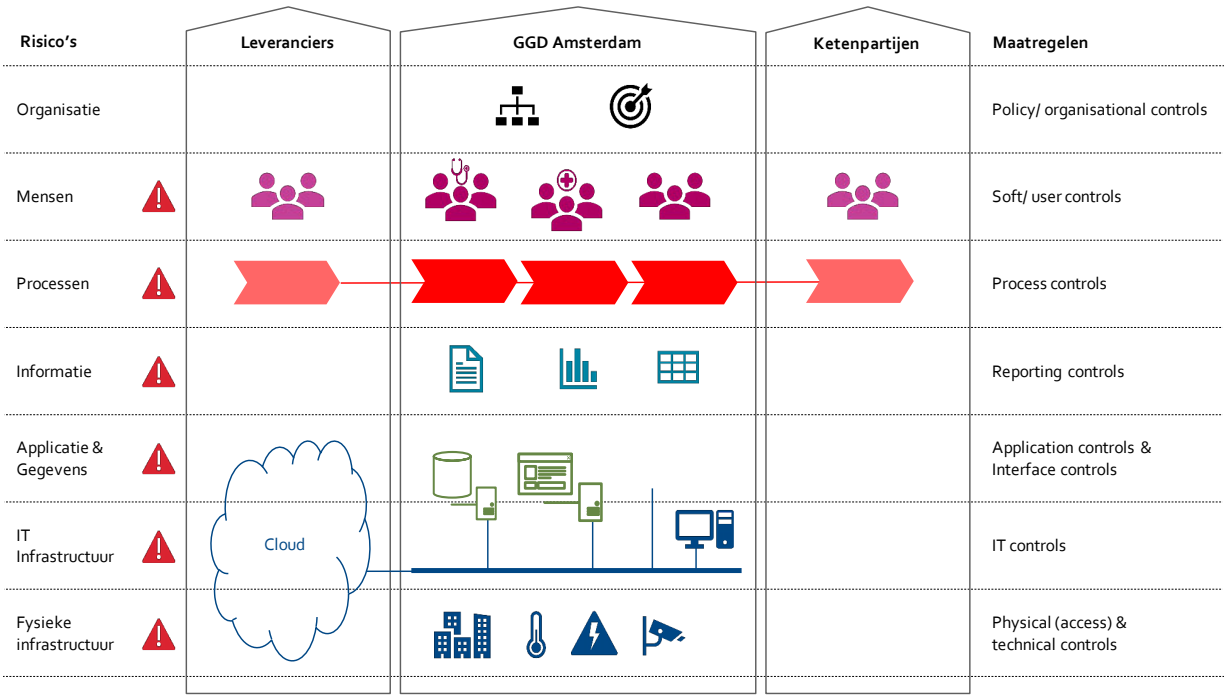
2.2.2 Typen maatregelen

Uit bovenstaande definitie is niet direct af te leiden waar de maatregelen moeten worden getroffen voor het waarborgen van de betrouwbaarheid van informatie en systemen. 'Waar' heeft enerzijds betrekking op de 'levensfase' waarin informatie en/of een systeem zich bevindt en anderzijds op het onderdeel van het systeem. Ter illustratie: een systeem kan zich in de ontwikkelingsfase bevinden en een onderdeel van het systeem kan een smartphone of tablet zijn. Dit betekent dat zowel de fase als het onderdeel bepalend is voor de typen maatregelen die moeten worden getroffen om de betrouwbaarheid te kunnen waarborgen.

Voor de GGD Amsterdam zijn deze maatregelen beschreven in de NEN 7510 en deze norm bestaat uit twee onderdelen:

- Deel 1 : beschrijft het kwaliteitssysteem voor informatiebeveiliging (ook wel het Information Security Management System genoemd). Het ISMS beschrijft het proces (PDCA- cyclus) om de betrouwbaarheid van informatie die door een organisatie wordt verwerkt te waarborgen.
- Deel 2: beschrijft volgens een vaste structuur: beheerscategorie, beheersdoelstelling, beheersmaatregel (de doelstellingen en maatregelen komen overeen met de ISO27001/2) en de zorgspecifieke beheersmaatregel. De uitgangspunten die gelden voor deze maatregelen komen verderop in dit document aan de orde en zijn gebaseerd op de uitgangspunten en hoofdpunten die worden genoemd in het beleidskader gemeente Amsterdam en het huidige beleid van de GGD Amsterdam die specifiek geldt voor beide IT- afdelingen (afdeling Automatisering en ITforCare).

In Figuur 1 zijn de onderdelen opgenomen die binnen de informatievoorziening kunnen worden onderkend en wordt vormgegeven door de informatiesystemen die in gebruik zijn binnen de GGD Amsterdam. Zoals afsluitend is opgemerkt in §2.1 van dit hoofdstuk zijn op alle lagen risico's te onderkennen en moeten deze adequaat worden beheerst door het treffen van passende maatregelen (zoals beschreven in het 2e deel van de NEN 7510) in de verschillende fasen waarin het systeem zich bevindt[4].



Figuur 1: lagen informatievoorziening en soorten maatregelen

- Organisatie (policy & organisational controls): uitgangspunten en beleidsregels die van toepassing zijn en wie waarvoor verantwoordelijk is.

[4] Voor de fasering kan bijvoorbeeld onderscheid gemaakt worden naar strategie, architectuur, ontwikkeling, implementatie (inclusief programma- en projectmanagement), gebruik/beheer en archivering/ verwijdering.

- Mensen (user controls): spelregels die van toepassing zijn om veilig met gegevens om te gaan en maatregelen voor het bevorderen van de awareness van de medewerkers zoals opleiding en voorlichting.
- Processen (process controls): procedures/ werkinstructies die onderdeel uitmaken van de werkprocessen. Voorbeelden hiervan zijn functiescheiding en het 4-ogen principe.
- Informatie (reporting controls): rapportages waarmee de betrouwbaarheid van de informatie kan worden bewaakt en gecontroleerd.
- Applicatie en gegevens (application en interface controls): configuratie-instellingen van een systeem of applicatie en bijbehorende beheerprocessen. Voorbeelden hiervan zijn invoercontroles en autorisatieprofielen.
- IT- infrastructuur (IT controls): configuratie-instellingen van IT-systemen voor het opslaan, bewerken, transporteren en representeren van gegevens en het aanbieden van applicaties en bijbehorende beheerprocessen. Voorbeelden hiervan zijn firewall-rules, wijzigingsbeheer en leveranciersbeheer.
- Fysieke infrastructuur (physical -access- controls): bouwkundige voorzieningen voor stroomvoorziening, klimaatbeheersing, huisvesting en de fysieke beveiliging van de systemen die in de betreffende ruimten staan opgesteld.

Uit Figuur 1 blijkt dat informatiesystemen ook door ketenpartijen/ samenwerkingspartners van de GGD Amsterdam worden gebruikt en door leveranciers worden geleverd/ beheerd. Dit betekent dat de verschillende soorten maatregelen niet alleen van toepassing kunnen zijn voor de GGD Amsterdam, maar ook voor haar ketenpartijen en leveranciers. Tevens betekent dit dat per laag en/of informatiesysteem overzicht en inzicht moet bestaan welke componenten hiervan onderdeel uitmaken en wie welke verantwoordelijkheden/ bevoegdheden hierin heeft ten aanzien aan van informatiebeveiliging. Welk organisatieonderdeel hiervoor verantwoordelijk is en voor welk type maatregelen wordt verder uitgewerkt in hoofdstuk 2.

2.2.3 Werkingsgebied/scope informatiebeveiliging

Het informatiebeveiligingsbeleid is van toepassing op de (geautomatiseerde) informatievoorziening van de GGD Amsterdam, te weten: directie, lijn- en stafafdelingen. Onder informatievoorziening valt (zie ook Figuur 1):

- Processen voor de publieke gezondheidszorg en de bedrijfsvoeringprocessen en de informatie die wordt gebruikt voor de uitvoering en besturing hiervan.
- Applicaties die door de afdelingen van de GGD Amsterdam worden gebruikt, en waarmee gegevens worden verwerkt en de IT- infrastructuur waarop de applicaties worden aangeboden.
- Facilitaire ruimten (MER/ SER) en voorzieningen waarin de centrale IT- infrastructuur staat opgesteld.
- Locaties en gebouwen van de GGD Amsterdam die direct zijn aangesloten op de IT-infrastructuur (primair Nieuwe Achtergracht en Valckenierstraat).
- Applicaties die op de IT- infrastructuur (afdeling Automatisering) van de GGD Amsterdam draaien en door externe organisaties (organisaties buiten de gemeente Amsterdam) of andere organisatieonderdelen van de gemeente Amsterdam worden gebruikt.
- De afdelingen Automatisering en ITforCare zijn ISO27001 gecertificeerd en wordt periodiek getoetst door een externe auditpartij. Voor zover van toepassing leunt het informatiebeveiligingsbeleid van de GGD Amsterdam hierop.

2.2.4 Raakvlakken

Informatiebeveiliging heeft raakvlakken met diverse andere beleidsterreinen, waar onder:

- Informatiebeleid - inrichting en organisatie van de informatiehuishouding/ voorziening.
- Fysiek beveiligingsbeleid - fysieke beveiliging van gebouwen en ruimten, fysieke toegangscontrole en integraal crisisplan.
- Organisatiebeleid - functiehuis, functiescheiding en functieprofielen.
- Personeelsbeleid - screening, opleiding, beoordeling en sanctionering.
- Privacybeleid - vertrouwelijk omgaan met cliënt- en medewerkersgegevens.
- Juridische kwaliteitszorg - beveiligingsclausules in overeenkomsten met derden.

In het informatiebeveiligingsbeleid en het raamwerk worden dan ook verwijzingen opgenomen naar relevante procedures en documenten zoals de gedragscode van de gemeente, gevolgde normen, huisregels, het integraal continuïteitsplan, enzovoort.

2.3 Wat wilt GGD Amsterdam bereiken met informatiebeveiliging

Gelet op de context en de interne en externe ontwikkelingen waarmee de GGD Amsterdam wordt geconfronteerd is het doel van informatiebeveiliging voor de GGD Amsterdam het waarborgen van:

- Beschikbaarheid: de informatie is (blijvend) toegankelijk en leesbaar.
- Integriteit: de informatie is juist en actueel.
- Vertrouwelijkheid: de informatie is beschermd en alleen toegankelijk voor bevoegden.

2.3.1 Uitgangspunten

Bij de toepassing van informatiebeveiliging binnen de GGD Amsterdam worden de uitgangspunten uit het stedelijk kader informatiebeveiliging gemeente Amsterdam[2] en GGD Amsterdam specifieke gehanteerd.

Uitgangspunten gemeente Amsterdam:

1. De aanpak van informatiebeveiliging is risico-gebaseerd.
2. De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement/afdelingsmanager.
3. Elk informatiesysteem heeft een eigenaar die verantwoordelijk is voor de kwaliteitsaspecten van deze systemen en de bijbehorende maatregelen voor informatiebeveiliging op basis van dit beleidskader informatiebeveiliging.
4. Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
5. Toegang tot informatie wordt alleen verstrekt wanneer dit nodig is voor de functie/rol of taak die iemand heeft, volgens het principe 'need to know'.
6. Elke medewerker, vast of tijdelijk en zowel intern als extern, is verplicht gegevens en informatiesystemen waar nodig te beschermen tegen onbevoegde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.
7. Elke medewerker meldt geconstateerde of vermoede inbreuken op de informatievoorziening direct aan het lijnmanagement en aan een daarvoor bestemde servicedesk en/of meldpunt.
8. Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.

Uitgangspunten GGD Amsterdam specifiek:

9. GGD Amsterdam voldoet aan de van toepassing zijnde wet- en regelgeving rondom informatiebeveiliging en sluit aan bij de algemeen geaccepteerde standaard ISO 27001/2 en de daarvan afgeleide Nederlandse standaard voor informatiebeveiliging in de zorg NEN 7510. In dit verband worden tevens genoemd:
    - Wet op de Geneeskundige Behandel Overeenkomst (WGBO)
    - Wet Publieke Gezondheid (WPG)
    - Algemene Verordening Gegevensbescherming (AVG)
    - Archiefwet
    - Wet cliëntenrechten elektronische verwerking van gegevens in de zorg
10. De aanpak van informatiebeveiliging is 'risk based' en 'evidence based' (AVG art. 24): het risicoprofiel van het informatiesysteem (of de informatie) bepaalt welke maatregelen moeten worden getroffen om de risico's te mitigeren en mogelijke rest-risico's te accepteren. Het risicoprofiel wordt bepaald door de informatiesystemen en informatie volgens een gestructureerde methode te classificeren in termen van beschikbaarheid, integriteit en vertrouwelijkheid.
11. Bij de aanname, tijdens het dienstverband en uitdiensttreding van medewerkers wordt aandacht besteed aan de integriteit van medewerkers en het vertrouwelijk omgaan met informatie.
12. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de directie van de GGD Amsterdam een sanctie opleggen conform de bepalingen vastgelegd in de Personeelsregelingen Gemeente Amsterdam (PGA).
13. Bij de ontwikkeling, aanschaf en implementatie (inclusief projectmanagement) van informatiesystemen wordt aandacht besteed aan informatiebeveiliging. Indien de GGD Amsterdam een samenwerking aangaat met externe partijen worden afspraken over informatiebeveiliging een beveiligingsparagraaf schriftelijk vastgelegd en naleving wordt periodiek getoetst door de contracteigenaar.
14. GGD Amsterdam heeft maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
15. Systeemeigenaren van de GGD Amsterdam dienen te beschikken over een actueel continuïteitsplan dat voorziet in de continuering van de processen bij ernstige calamiteiten. Het plan wordt periodiek op werking getoetst en geëvalueerd. Bij het opstellen van continuïteitsplannen wordt alleen rekening gehouden met reële dreigingen (tegen dreigingen als atoom- en natuurrampen worden geen specifieke maatregelen getroffen).

2.4 Basisniveau

Dit informatiebeveiligingsbeleid op basis van de NEN 7510 is een algemene basis binnen de GGD en dekt daarmee grotendeels de beveiligingseisen uit specifieke wetgeving af. Tevens zal de BIO ook als basisniveau dienen.

De Automatiseringsafdeling en ITforCare van de GGD Amsterdam zijn gecertificeerd volgens de ISO27001.

2.5 Normenkaders

De basis voor dit strategisch informatiebeveiligingsbeleid GGD Amsterdam is de (inter)nationale norm NEN-ISO/IEC 27001/2:2017 en de daarvan afgeleide NEN 7510 (de Nederlandse norm voor informatiebeveiliging in de zorg).

- De **NEN-7510** is de Nederlandse norm die van toepassing is op de zorgsector (en daarmee op o.a. gemeentelijke GGD's) en is gebaseerd op de ISO-27001/2. Met de controls ofwel de beheersing van informatiebeveiliging die in de ISO-27001/2 en in de NEN-7510 is beschreven, wordt informatiebeveiliging als continu proces ingericht.
- De **ISO-27001** is een internationaal erkende norm op het gebied van informatiebeveiliging, waar de ISO-27002 als het ware een richtlijn is met maatregelen voor de normen.
- De **Baseline Informatiebeveiliging Overheid (BIO)** is het basisnormenkader voor de gehele overheid, waaronder ook van toepassing binnen de gemeente Amsterdam. De beheersmaatregelen zijn gebaseerd op de bovenstaande ISO-normen.
- De **Algemene verordening gegevensbescherming (AVG)** is een Europese verordening die de regels voor de verwerking van persoonsgegevens door (particuliere) bedrijven, organisaties en overheidsinstanties in de hele Europese Unie standaardiseert.

3 Governance

In dit hoofdstuk wordt de governance van informatiebeveiliging voor de GGD Amsterdam beschreven, één van de onderdelen uit het kwaliteitssysteem van informatiebeveiliging (ook wel het ISMS genoemd). De governance is gebaseerd op het governacemodel van de GGD Amsterdam, het stedelijk kader informatiebeveiliging van de gemeente Amsterdam[2] en de Organisatie van informatiebeveiliging bij de gemeente Amsterdam[5].

In §3.1 worden de functies en rollen voor wat betreft informatiebeveiliging geïntroduceerd. In §3.2 wordt een overzicht gegeven van de overleg- en communicatiestructuren en hoe betrokkenen met elkaar in verbinding staan en onderling informatie delen.

3.1 Functies, rollen, kerntaken en verantwoordelijkheden

De verdeling van taken en verantwoordelijkheden (voor een nadere toelichting hierop wordt verwezen naar bijlage B) is gebaseerd op het zogenaamde 'three lines of defence model'. En beschrijft de organisatorische inrichting van informatiebeveiliging en de verdeling van kerntaken en verantwoordelijkheden op de verschillende organisatorische niveaus van de GGD Amsterdam.

Specifiek voor informatiebeveiliging is onderstaande verdeling van toepassing:

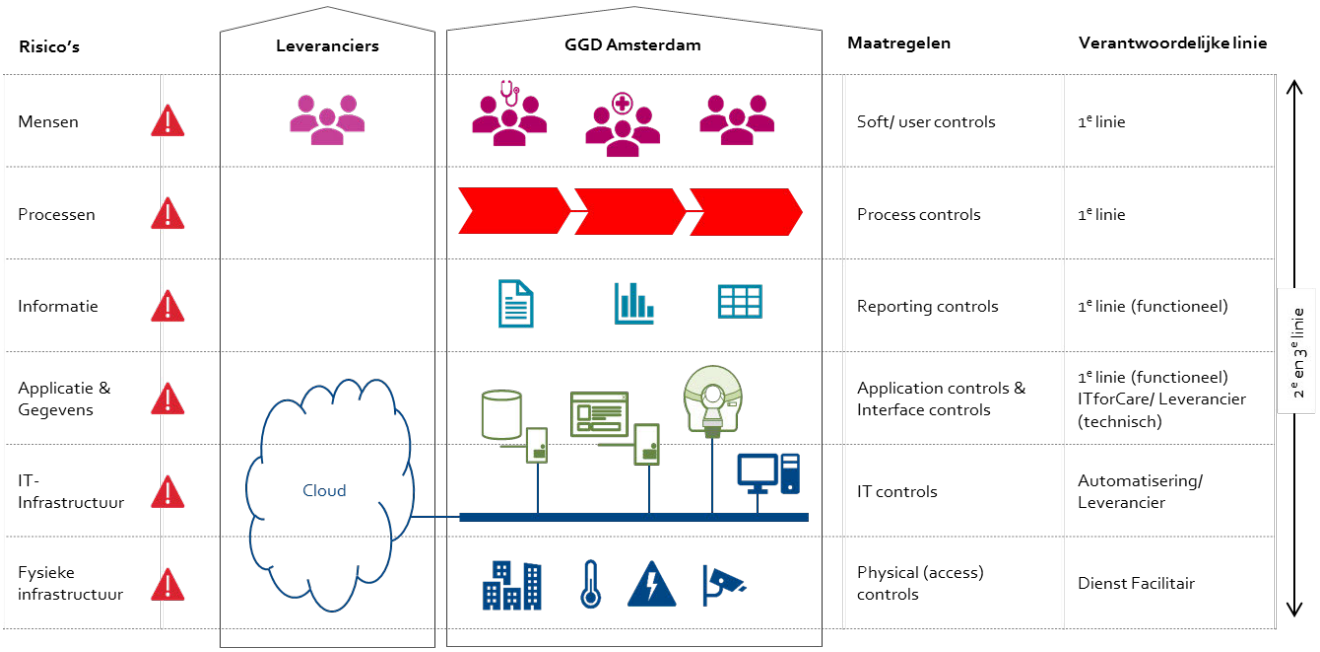
- 1e linie (1st line): **lijnmanagement/afdelingsmanager** van zowel de afdelingen die verantwoordelijk zijn voor de publieke gezondheidszorg als de stafafdelingen die verantwoordelijk zijn voor de ondersteunende (bedrijfsvoering) processen zoals facilitair, personeel, inkoop, financiën en IV/IT. Het lijnmanagement/afdelingsmanager is eigenaar van de informatie en systemen (inclusief de hiermee samenhangende risico's) en verantwoordelijk voor het selecteren, ontwerpen en implementeren van de maatregelen (als resultante van de uitgevoerde risicoanalyse en de classificatie van informatie) en het (laten) bewaken van de effectiviteit van de geïmplementeerde maatregelen. Het lijnmanagement/afdelingsmanager wordt hierbij enerzijds ondersteund door informatiemanagement en functioneel beheer waar informatiebeveiliging een onderdeel van uitmaakt. En anderzijds door de Information Security Officer, de Privacy Officer[6] en de Technical Security Officer (afdeling Automatisering en ITforCare) als specifieke functies voor informatiebeveiliging. In opdracht van het lijnmanagement/afdelingsmanager zijn zij verantwoordelijk voor het ontwikkelen en uitvaardigen ('promoten') van het informatiebeveiligingsbeleid en het inrichten van een effectief kwaliteitssysteem/ ISMS.
- 2e linie (2nd line)[7]: verantwoordelijk voor het bewaken van de voortgang van de implementatie en uitvoering van de maatregelen door de 1e linie. De 2e linie kan naast het zelf monitoren en uitvoeren van controles, gebruik maken van de controles die door de 1e linie worden uitgevoerd. Binnen de gemeente Amsterdam is dit belegd in de 1e linie.
  Binnen de gemeente Amsterdam bestaat de tweede lijn uit medewerkers of afdelingen die een kaderstellende en toetsende rol hebben. Voor informatie betreft dat de Chief Information Officer (CIO), specifiek voor informatiebeveiliging de Chief Information Security Officer (CISO) en de Functionaris Gegevensbescherming (FG) als het gaat om bescherming van persoonsgegevens. De CISO heeft in de

[5] Organisatie van informatiebeveiliging bij de gemeente Amsterdam GMT20200402.pdf
[6] Voor een nadere uitwerking van de privacy functie wordt verwezen naar het stedelijk beleidskader privacy gemeente Amsterdam

gemeente een zelfstandige en onafhankelijke rol en kan zich, indien dit naar zijn oordeel gewenst is, rechtstreeks tot de gemeentesecretaris en/of wethouder ICT wenden voor gevraagd en ongevraagd advies met betrekking tot informatiebeveiliging.

- 3e linie (3rd line): internal en external audit is verantwoordelijk voor het uitvoeren van controles en audits op de effectiviteit van de getroffen maatregelen in opzet, bestaan en/of werking. Naast eigen steekproeven en waarnemingen kan gebruik worden gemaakt van de reeds uitgevoerde controles door de 1e en 2e linie.

Door de soorten maatregelen die zijn geïntroduceerd in § 2.2 te koppelen aan het three lines of defence model van de GGD Amsterdam is onderstaande schematische verdeling van taken en verantwoordelijkheden van toepassing.



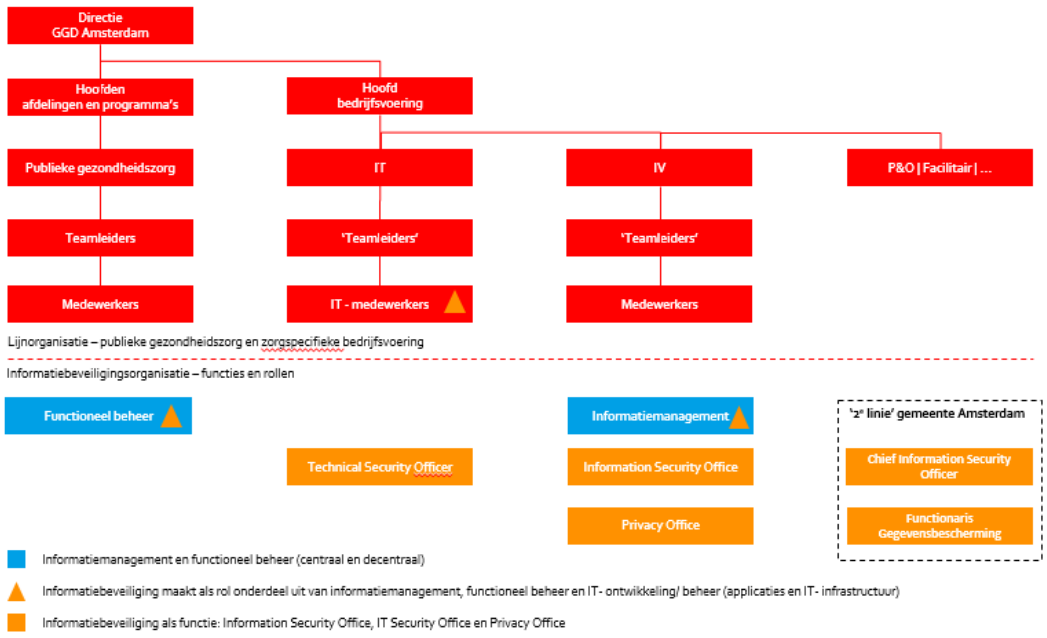
Figuur 2: verdeling informatiebeveiligingsmaatregelen volgens het three-lines-of-defence model

Uit bovenstaand schema blijkt dat informatiebeveiliging de gehele organisatie raakt, alsmede cliënten en externe partijen van de GGD Amsterdam (leveranciers, ketenpartners, toezichthouders, etc.). Voor iedereen die werkzaamheden voor de GGD Amsterdam verricht gelden -in het kader van informatiebeveiliging- dan ook specifieke taken en verantwoordelijkheden. Op basis van de in bovenstaande figuur opgenomen verdeling hiervan, worden hieronder de rollen en bijbehorende verantwoordelijkheden met betrekking tot informatiebeveiliging beschreven.

- 1e linie - **Informatiemanagement en Functioneel beheer**: de kerntaken van informatiemanagement bestaan uit het vormgeven van de strategie, informatiebeleid/planning, portfoliomanagement en architectuur van de informatievoorziening van de GGD Amsterdam. Gelet op de strategische waarde van informatie en zoals ook is verwoord in hoofdstuk 1, maakt informatiebeveiliging integraal onderdeel uit van informatiemanagement en functioneel beheer. Hiervoor is gekozen omdat informatiebeveiliging verankerd dient te zijn in de werkprocessen van de GGD Amsterdam, de informatie om de processen uit te kunnen voeren en te besturen alsmede de applicaties en de gegevens die hiermee worden verwerkt. Informatiemanagement op strategisch/ tactisch niveau en

functioneel beheer op tactisch/ operationeel niveau richten zich -in opdracht van de lijnorganisatie- op het selecteren/ ontwerpen, implementeren, onderhouden en evalueren van de maatregelen die in Figuur 2 worden genoemd voor de informatie- en systemen die door de (staf)afdelingen worden gebruikt.

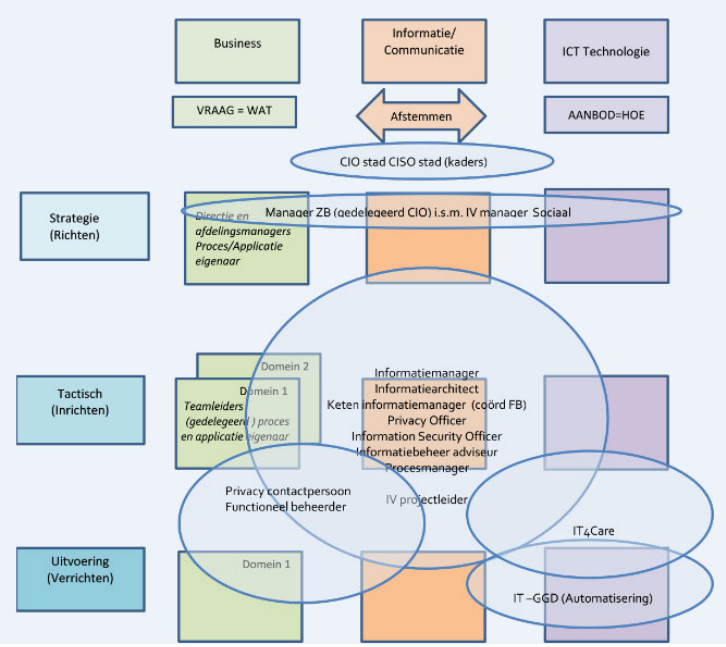
- 1e linie - **Technical Security Officer en Information Security Officer**: gelet op het specialistische en technische karakter van de diensten die door deze afdelingen worden geleverd worden in het kader van informatiebeveiliging naast de Information Security Officer een specifieke functies onderkend, Technical Security Officer (inclusief IT- medewerkers met specialistische security kennis). Deze functies richten zich op het ontwerpen, implementeren, onderhouden en evalueren van de maatregelen die in Figuur 1 worden genoemd voor de informatiesystemen die door de GGD Amsterdam worden gebruikt.
- 1e en 2e linie[7] - **Information Security Officer en Privacy Officer**: beide officers hebben een verbindende rol tussen de GGD Amsterdam en gemeente Amsterdam met betrekking tot het waarborgen van de betrouwbaarheid/ privacy van persoonsgegevens voor de informatie- en systemen die binnen de GGD Amsterdam in gebruik zijn. De officers houden controle op alle lopende projecten en activiteiten voor wat betreft informatiebeveiliging in overeenstemming met van toepassing zijnde wet- en regelgeving. Daarnaast heeft de 2e linie een adviserende rol.
- 2e linie - **Chief Information Security Officer (CISO)** voor informatiebeveiliging en de **Functionaris Gegevensbescherming (FG)** als het gaat om bescherming van persoonsgegevens. De CISO heeft in de gemeente een zelfstandige en onafhankelijke rol en kan zich, indien dit naar zijn oordeel gewenst is, rechtstreeks tot de gemeentesecretaris en/of wethouder ICT wenden voor gevraagd en ongevraagd advies met betrekking tot informatiebeveiliging.
- 3e linie - **Internal en external audit** uitvoeren van controles en audits op de effectiviteit van de getroffen maatregelen in opzet, bestaan en/of werking.



Figuur 3: rolverdeling informatiebeveiliging GGD Amsterdam

[7] GGD Amsterdam: ISO en PO, 1e linie voor o.a. beleid, bewustwording, etc. en in de 2e linie voor o.a. bewaken, toezicht, advies, etc. op de maatregelen. Binnen de gemeente Amsterdam valt dit allemaal binnen de 1e linie.

GGD Amsterdam valt binnen cluster Sociaal. In figuur 4 wordt het Informatievoorziening (IV) model GGD Amsterdam weergegeven in relatie met Informatievoorziening Eenheid (IVE) cluster Sociaal en de CIO-office.



Figuur 4: organisatie Informatievoorziening (IV) GGD Amsterdam – Informatievoorziening Eenheid (IVE) cluster Sociaal

3.2 Sturing geven aan informatiebeveiliging

De kern van (iedere) planning- en controlcyclus (hierna P&C- cyclus) -ook voor informatiebeveiliging- wordt gevormd door het -zoveel als mogelijk- meetbaar maken van de mate waarin de werkstromen die zijn verwoord in hoofdstuk 1 worden gerealiseerd en zo inzicht ontstaat in de mate waarin het niveau van informatiebeveiliging wordt bereikt ('in hoeverre wordt voldaan aan de betrouwbaarheidseisen die de GGD Amsterdam stelt aan haar informatie en systemen'). Met de opname van informatiebeveiliging in de P&C- cyclus van de GGD Amsterdam wordt geborgd dat over informatiebeveiliging periodiek wordt gerapporteerd en verantwoording wordt afgelegd. Daarnaast wordt geborgd dat het niveau van informatiebeveiliging periodiek wordt geëvalueerd zodat op basis van verkregen inzichten kan worden bijgestuurd om zo toe te werken naar continu verbetering.

Planning en rapportages*:

- (Jaar)plan informatiebeveiliging: jaarlijks wordt het plan geëvalueerd en geconcretiseerd voor het komende jaar.
- Het stedelijk dashboard, gemeente Amsterdam: per kwartaal of per 4 maanden (afhankelijk van het stedelijk gemeente Amsterdam proces) een 'forecast' van het lopende (jaar)plan opgesteld en afgezet tegen de afgelopen periode en de (lopende) risico's.
- Operationele rapportage: periodieke operationele rapportages voor de betreffende lijnverantwoordelijke.

* Ook hiervoor geldt het gemeente Amsterdam rapportage proces gevolgd te worden. Voor GGD Amsterdam specifiek operationele rapportagelijnen en verantwoordelijkheden zal in een apart document beschreven worden.

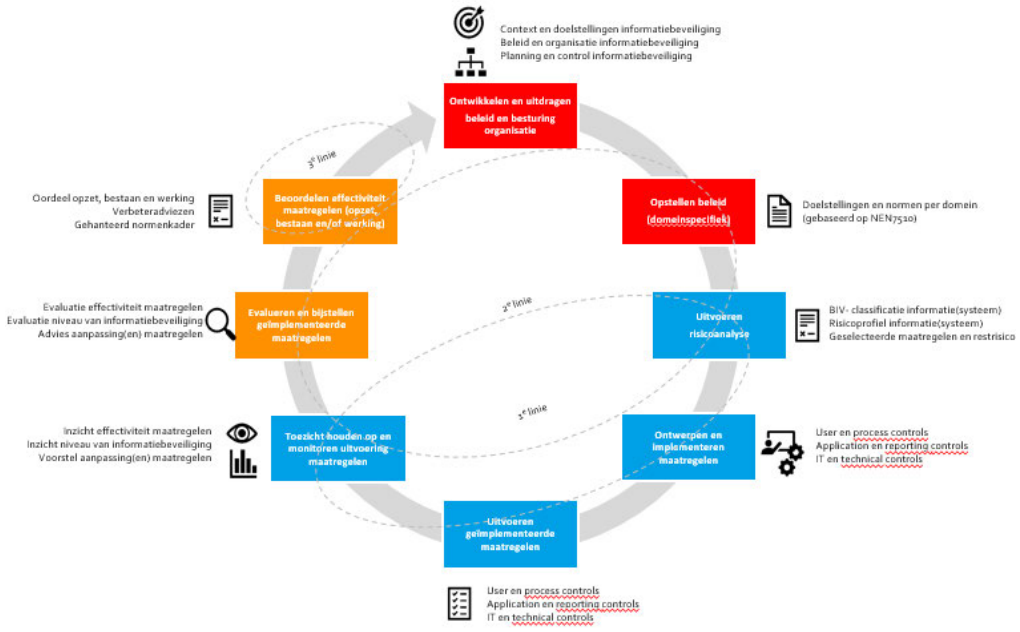
4 Risicomanagement en controle raamwerk

In dit hoofdstuk wordt het proces (informatie)risicomanagement beschreven, één van de pijlers van het kwaliteitssysteem (ISMS) voor informatiebeveiliging van de GGD Amsterdam. In §4.1 wordt het proces risicomanagement toegelicht met betrekking tot de informatievoorziening van de GGD Amsterdam. De resultaten die tijdens het doorlopen van het proces worden verkregen worden opgenomen in het (interne) controle raamwerk wat wordt beschreven in §4.2.

De GGD Amsterdam zal aansluiten op de aanpak risicomanagement en het controle raamwerk van gemeente Amsterdam. De aanpak van de gemeente Amsterdam is uitgewerkt in het implementatie-plan BIO gemeente Amsterdam).

4.1 Informatierisicomanagement - procesmatige aanpak en continue verbetering

Het risicomanagementproces voor informatiebeveiliging biedt een model om risico's adequaat en gestructureerd te beheersen en continu te verbeteren om het gewenste niveau van informatiebeveiliging te bereiken. Dit niveau heeft betrekking op de beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening. Dit proces, ook wel het Information Security Management Systeem (ISMS) genoemd, is vormgegeven in een PDCA-cyclus en de resultaten worden periodiek geëvalueerd en bijgesteld. Hiermee wordt bereikt dat het niveau van informatiebeveiliging periodiek wordt geanalyseerd en -waar nodig- verbeterd. Doordat risicoanalyses integraal onderdeel uitmaken van de procesmatige aanpak, herijkt de GGD Amsterdam eveneens periodiek de GGD- brede, organisatorische, procedurele en technische risico's. De cyclus is weergegeven in onderstaande figuur 4 en bestaat uit 8 stappen. In §4.1.1 t/m §4.1.8 is het onderdeel uit de PCDA-cyclus tussen haakjes "( )"vermeld.



Figuur 5: Informatierisicomanagement als cyclus proces

In de onderstaande paragrafen wordt er naast linies (zie §3.1) ook gesproken over niveaus van lijnorganisatie, zie bijlage B voor uitleg over de verschillende niveaus.

4.1.1 Opstellen informatiebeveiligingsbeleid (plan)

In dit document is het beleid voor informatiebeveiliging beschreven. Het document is vastgesteld door de directie van de GGD Amsterdam. In opdracht van de directie GGD Amsterdam (portefeuillehouder informatiebeveiliging) verzorgt de ISO het beheer en de borging van het beleid binnen de organisatie. Na het vaststellen door de directie GGD Amsterdam, wordt dit gecommuniceerd en dient vanaf dat moment, samen met het Stedelijk kader informatiebeveiliging gemeente Amsterdam, als richtlijn voor de organisatie als geheel.

4.1.2 Opstellen informatiebeveiligingsplan (plan)

In deze stap worden -op basis van de NEN 7510 en de ISO 27001 of de BIO- de algemene eisen, doelen en randvoorwaarden gespecificeerd of bijgesteld op basis van een analyse van de huidige situatie. Deze worden vastgelegd in het informatiebeveiligingspan voor de inhoudelijke onderwerpen zoals de selectie en aanschaf van informatiesystemen, logische en fysieke toegangsbeveiliging en bewustwording. Het plan wordt periodiek geëvalueerd om blijvend te voldoen aan de betrouwbaarheidseisen van alle interne en externe belanghebbenden. Hierbij wordt aandacht besteed aan onder meer: effectiviteit en kosten van de getroffen maatregelen, effect van nieuwe technologieën, wijzigingen in strategische doelstellingen van de GGD Amsterdam en de omgeving waarin GGD Amsterdam acteert, interne en externe ontwikkelingen en wijzigingen in relevante wet- en regelgeving en opgetreden beveiligingsincidenten.

Het (bijgestelde)plan wordt voorbereid door de ISO (in afstemming en de betreffende betrokkenen/stakeholders), met input vanuit de afdelingen en stafafdelingen (1e linie). Het plan wordt ter goedkeuring voorgelegd aan de directie van GGD Amsterdam.

4.1.3 Uitvoeren risicoanalyse (do)

In dit onderdeel wordt op basis van risicoanalyses bepaald welke bedreigingen tot onacceptabele risico's leiden en worden maatregelen geselecteerd (waar onder user controls, process controls en IT controls) waarmee deze risico's kunnen worden gereduceerd tot een voor de organisatie passend en aanvaardbaar betrouwbaarheidsniveau. Dit niveau wordt bepaald door het uitwerken van de inventarisatiesheet, waarin een integrale aanpak voor informatiebeveiliging, privacy en informatiebeheer is opgenomen. Rest-risico's die niet door de geselecteerde maatregelen kunnen worden gemitigeerd worden expliciet gemaakt en door de eigenaar geaccepteerd.

4.1.4 Ontwerpen en implementeren maatregelen (do)

Het ontwerpen en implementeren van de geselecteerde maatregelen vindt plaats in deze stap. Ook het doorvoeren van wijzigingen in de organisatie en -proces vinden in deze stap plaats. Het ontwerpen en implementeren wordt vastgelegd in het informatiebeveiligingsplan en de (jaar)plannen van de afdelingen/lijnorganisatie.

4.1.5 Uitvoeren geïmplementeerde maatregelen (check)

Afhankelijk van het type maatregel en het risicoprofiel worden de geïmplementeerde maatregelen (periodieke controles) uitgevoerd om het vastgestelde niveau van betrouwbaarheid te kunnen

waarborgen. Het uitvoeren van de maatregelen is belegd op het 3e niveau van de lijnorganisatie, inclusief medewerkers met specifieke verantwoordelijkheden.

4.1.6 Toezicht houden op en monitoren uitvoering maatregelen (check)

Deze stap betreft het door het 2e niveau van de lijnorganisatie monitoren of de maatregelen daadwerkelijk worden uitgevoerd en de mate van effectiviteit (self assessments en reviews door de 1e linie). De uitkomsten hiervan worden gerapporteerd aan het eigen management en, na afstemming en goedkeuring door het management, aan de ISO en PO (1e linie).

4.1.7 Evalueren en bijstellen geïmplementeerde maatregelen (act)

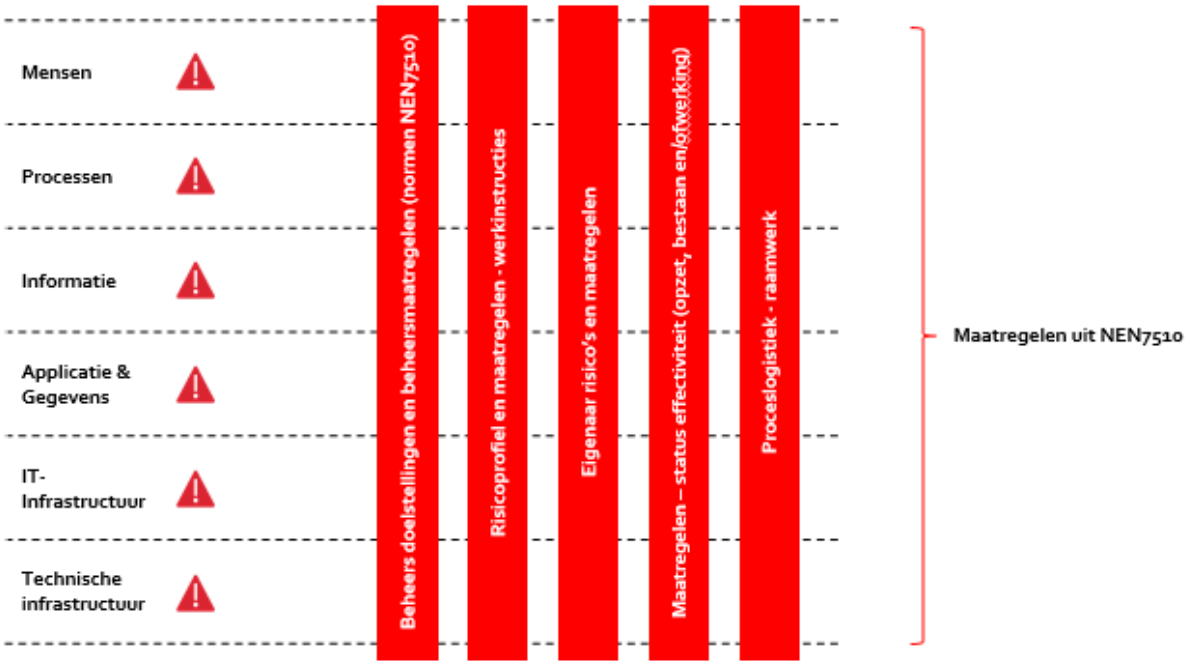
Deze stap betreft het evalueren van de kwaliteit van de maatregelen en de uitvoering hiervan ten opzichte van het beleid en hiervan afgeleiden richtlijnen. De evaluatie wordt uitgevoerd door de ISO (1e linie) en de uitkomsten worden gerapporteerd, na afstemming met de eigenaar, door de ISO aan de directie van GGD Amsterdam, IVE manager(s) en de CISO (indien nodig). De evaluatie wordt tevens gebruikt, indien nodig, om het informatiebeveiligingsplan en/of het beleid aan te passen.

4.1.8 Beoordelen effectiviteit maatregelen (act)

In overleg en afstemming met internal audit worden afspraken gemaakt over het uitvoeren van audits waarbij de (delen van de) informatievoorziening object van onderzoek is. In het auditjaarplan worden de audits opgenomen en gedurende het jaar uitgevoerd. De auditor stelt hiervoor een werkprogramma op en voert op basis van een overeengekomen normenkader de auditwerkzaamheden uit. Op basis van interviews, documentatie-studie en eigen waarneming wordt een oordeel gevormd over de mate waarin de getroffen maatregelen in opzet, bestaan en/of werking voldoen aan de norm. De rapportage wordt afgestemd met betrokkenen en gebruikt om onder meer het beleid aan te passen.

4.2 GGD controle raamwerk

De (tussen)resultaten die worden verkregen met het doorlopen van het risicomanagementproces worden opgenomen in het GGD controle raamwerk, wat in onderstaand figuur is opgenomen:



Figuur 6: opzet GGD controle raamwerk

Het raamwerk wordt gebruikt om onderstaande onderwerpen te documenteren en dient als basis om overzicht en inzicht te hebben in de staat van informatiebeveiliging van de GGD Amsterdam. Het raamwerk bestaat uit:

- Beheerdoelstellingen en (zorgspecifieke) beheersmaatregelen: de algemene uitgangspunten ten aanzien van informatiebeveiliging die zijn opgenomen in de NEN 7510 (en 1-op-1 aansluiten op de ISO27001) en de zorgspecifieke maatregelen als 'add-on'.
- Risicoprofiel: risico's die de GGD Amsterdam in het algemeen loopt (en specifieke risico's voor de informatiesystemen die door de GGD Amsterdam worden gebruikt zijn opgenomen in de inventarisatiesheet).
- Maatregelen werkinstructie: de getroffen maatregelen, algemeen geldend en eventueel gespecificeerd naar afdeling naar aanleiding van de uitkomsten van de risicoanalyse , voorzien van werkinstructies om de effectiviteit (opzet, bestaan en/of werking) te kunnen toetsen.
- Eigenaar: van de risico's en maatregelen en de wijze waarop de taken en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn belegd binnen de organisatie.
- Maatregelen status: de effectiviteit van de getroffen maatregelen in opzet, bestaan en/of werking (gewerkt wordt met stoplichten groen, oranje en rood.
- Proceslogistiek: de wijze waarop wordt toegezien op de naleving van de eisen in de praktijk en de wijze waarop de managementprocedures rondom informatiebeveiliging is ingericht.

Bijlage A

Technologische ontwikkelingen

In deze bijlage worden de ontwikkelingen uit § 2.1 nader toegelicht. Voor het realiseren van de strategische doelstellingen van de GGD Amsterdam en het uitvoeren van de werkprocessen zijn informatiesystemen -inclusief medische systemen en facilitaire systemen- onmisbaar geworden en niet meer weg te denken uit de organisatie.

Afdelingen gebruiken diverse elektronische cliëntdossiers voor (medische) dossiervorming en het verantwoorden/ factureren van de productie, diverse apps en websites voor het geven van voorlichting aan cliënten en diverse medische en facilitaire systemen. Kenmerkend voor al deze systemen is dat ze processen ondersteunen, gegevens verwerken, informatie genereren, door mensen worden gebruikt en (vaak) een technologische component bevatten. De technologische ontwikkelingen volgen elkaar in snel tempo op en bieden steeds meer mogelijkheden.

Toenemende behoefte aan stuur- en operationele informatie
Voor het monitoren van de strategie van de GGD Amsterdam en de werkprocessen is betrouwbare informatie een absolute randvoorwaarde. Maar ook voor het leveren van publieke gezondheidszorg.

Toenemende inzet systemen en omvang/diversiteit gegevens
Niet alleen de 'klassieke' IT-systemen, maar vooral de combinatie met apps en de toepassing van e-health zorgt voor een vergaande digitalisering van de werkprocessen, waarbij de strategische thema's van de GGD Amsterdam een prominente plaats innemen. Met deze systemen worden grote hoeveelheden verzamelingen gestructureerde en ongestructureerde gegevens aangelegd en verwerkt. De nieuwste generatie data-analyse toepassingen maken het mogelijk om patronen te ontdekken en herkennen in deze gegevensverzamelingen. In het kader van onderzoek worden deze analyse-toepassingen steeds belangrijker om bestaande methoden te optimaliseren en nieuwe te ontwikkelen.

Medewerkers en cliënten gaan zich steeds meer als '(zorg)technologie'-consument gedragen. Zij verwachten dat hun smartphone of tablet ook binnen de werkcontext kan worden gebruikt, zowel voor zakelijke als privédoeleinden. Afdelingen of groepen van medewerkers nemen in toenemende mate het initiatief om apps te (laten) ontwikkelen, waarmee eenvoudig en direct aan de brongegevens door een zorgverlener of cliënt kunnen worden geregistreerd, geraadpleegd en uitgewisseld met het elektronisch dossier. De opkomst van 'wearable health' technologie doet hier naar verwachting nog een schepje bovenop.

De onderliggende IT- infrastructuur waarop deze systemen zijn aangesloten dient 'organisch' mee te bewegen voor wat betreft reken- en opslagcapaciteit en dient 'altijd/ overal' via ieder willekeurig device beschikbaar te zijn. Cloudtechnologie en internet-of-things maken snelle opmars in de zorgsector. Niet alleen worden (zeer) hoge betrouwbaarheidseisen gesteld aan deze infrastructurele voorzieningen waarvan 'alle' medewerkers van de GGD Amsterdam afhankelijk zijn. Maar ook -afhankelijk van aard en type van het proces- de systemen die hierop zijn aangesloten en de gegevens die hiermee worden verwerkt.

Toenemende gegevensuitwisseling in (zorg)keten
Door de toenemende samenwerking in de (zorg)keten staan zorgverleners en cliënten (continu) in verbinding met elkaar. Afhankelijk van de zorgbehoefte is de samenstelling -fysiek en virtueel- aan verandering onderhevig. Om kwalitatieve en veilige zorg te kunnen leveren dient informatie altijd en overal voor alle betrokkenen (mits geautoriseerd) beschikbaar te zijn en op maat te worden aangeboden.

Zodanig dat alle betrokkenen, ieder vanuit hun eigen expertise en behoefte, over hetzelfde cliëntbeeld kan beschikken. Het elektronisch dossier wordt een digitaal platform die de zorgconsument verbindt met haar zorgverleners (waar onder apotheker, huisarts, verpleegkundige en artsen). Het platform dient alle betrokkenen in staat te stellen om informatie op een betrouwbare manier te delen en uit te wisselen. Naast het delen van informatie voor het leveren van zorg vragen diverse instanties steeds meer om gegevens te verstrekken die in en rondom het primaire proces worden aangelegd en verwerkt. Voor beide vormen van gegevensuitwisseling geldt dat alle betrokkenen verwachten dat de gegevens betrouwbaar zijn en door hun veilig met deze gegevens wordt omgegaan.

Toenemende wet- en regelgeving
Stakeholders (inclusief externe toezichthouders en wet- en regelgevende instanties) van de GGD Amsterdam vragen steeds meer om transparantie over hoe de kwaliteit en veiligheid van de publieke zorgdienstverlening is geborgd. In dit kader is de GGD Amsterdam gecertificeerd tegen de ISO-norm voor de zorg, en zijn verschillende afdelingen/teams gecertificeerd tegen specifieke ISO/NEN- normen. Mede omdat de GGD Amsterdam op grote schaal (bijzondere) persoonsgegevens verwerkt en voor de werkprocessen betrouwbare informatie randvoorwaardelijk is, is de GGD Amsterdam gehouden aan specifieke wet- en regelgeving waaronder de AVG, WGBO en de NEN 7510.

Waar patiënten en medewerkers -impliciet- verwachten dat hun privacy is gewaarborgd gaan zorgverzekeraars, banken/ verzekeraars en de IGZ/ NzA het voldoen hieraan (steeds meer) verplicht stellen. Niet alleen in opzet, maar afhankelijk van het belang en rol van de informatie en het systeem in het zorgproces, ook steeds meer in bestaan en werking.

De belangrijkste stakeholders voor de GGD Amsterdam zijn:

- Gemeente Amsterdam als opdrachtgever en mede uitvoerende organisatie in de keten van (publieke) gezondheidszorg;
- IGJ en NZa als toezichthoudende instanties;
- RIVM en LCR als opdrachtgever en mede uitvoerende organisaties;
- GGD GHOR Nederland als brancheorganisatie.

In zijn algemeenheid kan worden gesteld dat deze stakeholders eisen stellen aan de dienstverlening van de GGD Amsterdam en het voldoen aan de NEN 7510 (op termijn) randvoorwaardelijk dan wel vanzelfsprekend is.

Bijlage B

Kerntaken en verantwoordelijkheden

In deze bijlage zijn de rollen en kerntaken en verantwoordelijken voor de informatiebeveiligings-organisatie nader uitgewerkt. De specifieke rollen voor informatiebeveiliging zijn gebaseerd op het document beroepsprofielen informatiebeveiliging 2.0, d.d. 1 januari 2017, Platform Informatiebeveiliging), Organisatie van informatiebeveiliging bij de gemeente Amsterdam, de GGD Amsterdam en de compliance statement 6.1.3 waarin de verantwoordelijkheden voor informatiebeveiliging voor het cluster sociaal zijn beschreven. Mocht een functie en/of rol hieronder ontbreken, zie "Organisatie van informatiebeveiliging bij de gemeente Amsterdam GMT20200402.pdf".

Lijnorganisatie – 1e linie

Directie – 1e niveau
De directie van de GGD Amsterdam is integraal eindverantwoordelijk voor het waarborgen van de betrouwbaarheid van de informatie die voor de uitvoering en besturing van de werkprocessen van de GGD Amsterdam wordt gebruikt. Binnen de directie is een portefeuillehouder Informatiebeveiliging aangewezen waarvoor onderstaande kerntaken en verantwoordelijkheden gelden:

- Het vaststellen en uitdragen van het informatiebeveiligingsbeleid en het jaarplan Informatiebeveiliging.
- Het (laten) inrichten en het in stand houden van de planning- en controlcyclus voor informatiebeveiliging.
- Het bewaken en evalueren van het gerealiseerde niveau van informatiebeveiliging.
- Het informeren van het MT over de stand van zaken rondom informatiebeveiliging.
- Het beschikbaar stellen van voldoende middelen (personeel en geld) om uitvoering te kunnen geven aan het jaarplan Informatiebeveiliging.
- Het afstemmen en communiceren met externe partijen en toezichthouders (onder andere IGJ).

Hoofden (staf)afdelingen – 2e niveau
De hoofden van de afdelingen zijn als eigenaar van één of meerdere processen, informatie(stromen), applicaties of gegevens tevens eigenaar van de risico's en hiermee verantwoordelijk voor het waarborgen van de betrouwbaarheid van de gegevens die met de applicatie of het systeem worden verwerkt. Voor de hoofden gelden onderstaande kerntaken en verantwoordelijkheden:

- Het jaarlijks opstellen van het specifieke informatiebeveiligingsplan voor de eigen afdeling en het bewaken van de oplevering van de daarin opgenomen resultaten.
- Als onderdeel van informatiemanagement/ functioneel beheer; beleggen van de rol van Information Security Officer. Deze rol/ functie ie is verantwoordelijk voor de ondersteuning van het management bij het implementeren, uitvoeren en bewaken van het informatiebeveiligingsbeleid in het algemeen en specifieke maatregelen in het bijzonder voor de informatiesystemen waarvan het hoofd eigenaar is.
- Het in overleg met de Information Security Officer vaststellen van het gewenste niveau van informatiebeveiliging van de informatiesystemen waarvan het hoofd eigenaar is.
- Het accepteren van de risico's, die bekend zijn ten tijde van de ontwikkeling van een informatiesysteem, als gevolg van functionele of technische beperkingen en/of het niet (of niet volledig) implementeren van de maatregelen. De (rest)risico's worden door het hoofd expliciet geaccepteerd en gedocumenteerd.

- Het vaststellen en laten beheren (inclusief het toezien op het juist en tijdig implementeren en uitvoeren) van een autorisatiematrix.
- Het vaststellen en laten beheren (inclusief het toezien op het juist en tijdig implementeren en uitvoeren) van een stelsel van maatregelen -in lijn met het informatiebeveiligingsbeleid en de baseline- voor het waarborgen van het vastgestelde niveau van informatiebeveiliging van de informatiesystemen waarvan het hoofd eigenaar is.
- Het rapporteren over de effectiviteit van de getroffen maatregelen binnen de eigen afdeling aan de directie (via en met ondersteuning van de Information Security Officer).

Hoofden (staf)afdelingen - specifieke kerntaken en verantwoordelijkheden – 2e niveau
Voor onderstaande hoofden zijn specifieke kerntaken en verantwoordelijkheden van toepassing:

- Facilitair via ZSB: is verantwoordelijk voor het (laten) selecteren, ontwerpen, implementeren, uitvoeren en controleren van maatregelen voor het waarborgen van het vereiste niveau van informatiebeveiliging van alle (zowel intern- als extern) overeengekomen diensten op de laag fysieke/ technische infrastructuur. Om de inrichting van de maatregelen te borgen, dienen in de gebruikte documenten (onder meer programma van eisen, functioneel en technisch ontwerp, acceptatiecriteria en beheerdocumentatie) paragrafen te worden opgenomen met een overzicht van de (te adresseren) maatregelen.
- Hoofden Automatiseringsafdeling en ITforCare: zijn verantwoordelijk voor het (laten) selecteren, ontwerpen, implementeren, uitvoeren en controleren van maatregelen voor het waarborgen van het vereiste niveau van informatiebeveiliging van alle (zowel intern- als extern) overeengekomen diensten op de lagen IT- infrastructuur en applicatie/ systeem**. Om de inrichting van de maatregelen te borgen, dienen in de gebruikte documenten (onder meer programma van eisen, functioneel en technisch ontwerp, acceptatiecriteria en beheerdocumentatie) paragrafen te worden opgenomen met een overzicht van de (te adresseren) maatregelen.

  ** <u>De eigenaar van de applicatie of systeem is verantwoordelijk voor het waarborgen van de integriteit en vertrouwelijkheid van de gegevens die met het informatiesysteem worden verwerkt.</u>

- P&O via ZSB: is verantwoordelijk voor (laten) selecteren, ontwerpen, implementeren, uitvoeren en controleren van maatregelen met betrekking tot het HR-proces: instroom, doorstroom en uitstroom van interne en externe medewerkers.
- Inkoop via ZSB: is verantwoordelijk voor het toezien op de juiste toepassing van de maatregelen tijdens het inkooptraject van informatiesystemen.
- Lijn- of stafafdelingen met informatiesyste(e)m(en) in eigen beheer: voor informatiesystemen -voor wat betreft de lagen fysieke infrastructuur, technische infrastructuur en applicatie/systeem- die niet in beheer zijn bij de IT- afdeling(en) of bij uitbesteding aan een derde partij is het hoofd van de betreffende lijnafdeling verantwoordelijk.
- Programma-/ Projectmanager: voor de implementatie van nieuwe informatiesystemen (of grote wijzigingen is de projectmanager verantwoordelijk dat het plan van aanpak voorziet in (1) het aspect informatiebeveiliging met in achtneming van het door het lijnmanagement/afdelingsmanager vastgestelde niveau van informatiebeveiliging en (2) rapporteert over de mate waarin de geselecteerde maatregelen worden geïmplementeerd en wordt voldaan aan het vastgelegd.

Teamleider – 3e niveau
Voor de teamleiders gelden onderstaande kerntaken en verantwoordelijkheden:

- Het zich op de hoogte stellen van het informatiebeveiligingsbeleid dat van toepassing is op het functioneren van zijn eigen afdeling. En het toezien op de naleving van het informatiebeveiligingsbeleid binnen het eigen team.

- Het toezien op een juiste en volledige omschrijving in de functieomschrijving van informatiebeveiligingskritische functies (in overleg en afstemming met P&O).
- Wanneer een medewerker (intern of extern) het beleid niet naleeft; het afhandelen van de overtreding volgens het geldende sanctiebeleid. In het geval van een overtreding door een externe medewerker neemt de teamleider contact op met de leverancier (eventueel via degene die normaal de contacten met de externe partij onderhoudt).
- In geval sprake is van een informatiebeveiligingsincident; het (laten) afhandelen hiervan volgens het stedelijke Incidentmanagementprocedure "Informatiebeveiligingsincidenten en datalekken proces" en aangevuld door het "incidentbeheer – informatiebeveiligingsincidenten" GGD Amsterdam.
- Het (laten) toekennen van toegangsrechten en autorisaties aan medewerkers binnen het eigen team (conform de door het management vastgestelde autorisatiematrix). En het periodiek (laten) controleren van de toegekende toegangsrechten en autorisaties aan medewerkers binnen het eigen team.
- Het juist en tijdig (laten) selecteren/ontwerpen, implementeren en uitvoeren van een stelsel van maatregelen -in lijn met het informatiebeveiligingsbeleid en de baseline- voor het waarborgen van het vastgestelde niveau van informatiebeveiliging van de informatiesystemen binnen het eigen team.
- Het (laten) controleren van de effectiviteit van de werking van de getroffen maatregelen en het (laten) rapporteren hierover aan het hoofd van de eigen afdeling (via en met ondersteuning van informatiemanagement, functioneel beheer en Information Security Officer).
- Het leveren van een actieve bijdrage aan informatiebeveiliging door:
  - Geven van het goede voorbeeld.
  - Medewerkers op hun verantwoordelijkheden te wijzen en hierop aan te spreken.
  - Beantwoorden van vragen van medewerkers.
  - Als aanspreekpunt binnen het eigen team te fungeren voor het melden en (laten) afhandelen van incidenten.
  - Informatiebeveiliging periodiek aan de orde te stellen in het werkoverleg en bij plannings-/ functionerings-/ en beoordelingsgesprekken in het kader van de HRM- cyclus.
  - Leveren van een bijdrage aan het realiseren van het informatiebeveiligingsplan.
- Bij indiensttreding; informeren van nieuwe medewerkers (intern en extern) over informatiebeveiliging binnen de GGD Amsterdam in het algemeen en over de voor hem/haar van toepassing zijnde richtlijnen in het bijzonder, inclusief de daaraan gerelateerde individuele verantwoordelijkheden.
- Bij beëindiging van het dienstverband of de inzet van externen, of het doorstromen van medewerkers; het toezien en controleren op het inleveren van alle GGD Amsterdam- eigendommen die de medewerker ter beschikking zijn gesteld (zoals toegangspas/ druppel, laptop, mobiele telefoon, etc.) en het intrekken van toegangsrechten en autorisaties.

Medewerkers – 4e niveau
Voor zowel interne als externe medewerkers gelden onderstaande kerntaken en verantwoordelijkheden:

- Het op de hoogte laten stellen van het beleid dat de GGD Amsterdam van toepassing heeft verklaard op de eigen afdeling en/of de eigen functie (bijvoorbeeld specifieke procedures en werkinstructies gericht op de eigen werkprocessen).
- Het raadplegen van de teamleider voor specifieke vragen en nadere toelichting over informatiebeveiliging. Dit geldt ook wanneer het beleid een belemmering of beletsel opleveren voor het uitvoeren van de werkzaamheden en in dergelijke zo'n geval mag de gebruiker niet zelfstandig, op eigen initiatief afwijken van de voorgeschreven procedures en richtlijnen.
- Het naleven van het beleid en het respecteren van de maatregelen die zijn getroffen en het nalaten om deze maatregelen uit te testen of bewust te omzeilen.

- Leveren van een actieve bijdrage aan informatiebeveiliging, onder andere door het direct melden van incidenten aan de daarvoor ingerichte organisatorische eenheden of, wanneer het om vertrouwelijke incidenten gaat, aan zijn/haar teamleider of hoofd van de afdeling.
- Bij beëindiging; het inleveren van alle beschikbaar gestelde <organisatie>- middelen (toegangspas, laptop, etc) bij zijn/haar operationeel leidinggevende.

Arts of verpleegkundige

- Gelden in het kader van de WGBO of wet BIG nog specifieke taken en verantwoordelijkheden, naast de verantwoordelijkheid dat de arts -als hoofdbehandelaar- de integriteit en vertrouwelijkheid/ privacy van de informatie die is opgenomen in het dossier waarborgt.

Informatiebeveiligingsorganisatie – 1e linie (en ISO, PO 2e linie)

Technical Security Officer – 2e niveau
Technical Security Officer heeft betrekking op het ontwikkelen, ontwerpen en implementeren van IT maatregelen voor het waarborgen van de betrouwbaarheid van de applicaties, IT- infrastructuur en fysieke/ technische infrastructuur, evenals bijbehorende IT- beheerprocessen. Vanuit de IT security office worden de security specialisten (in ieder geval functioneel) aangestuurd. Opmerking: voor beide IT-afdelingen is de IT security office ingericht.

De kerntaken en verantwoordelijkheden van de Technical Security Officer zijn:

- Het vertalen van het informatiebeveiligingsbeleid naar IT maatregelen ten behoeve van de levenscyclus van informatiesystemen op het gebied van architectuur, eisen, richtlijnen, procedures, methoden en technieken.
- Het classificeren van de IT- infrastructuur in termen van beschikbaarheid, integriteit en vertrouwelijkheid (BIV- classificatie), het uitvoeren van en ondersteunen bij risicoanalyses en het adviseren, het selecteren van mitigerende maatregelen en het adviseren over restrisico's.
- Het implementeren, (laten) uitvoeren en toezien op de naleving van de geselecteerde maatregelen (inclusief continuïteit).
- Het zorgdragen voor een adequate registratie, analyse en rapportage van informatiebeveiligingsincidenten.
- Het initiëren, adviseren/ managen, ondersteunen bij van informatiebeveiligingsprojecten.
- Het afstemmen van projecten en activiteiten met andere beveiligingsdomeinen, waaronder privacy en fysieke beveiliging.
- Het rapporteren over de effectiviteit van de getroffen maatregelen (inclusief IT assessments, testen, reviews en audits) en het presenteren van verbetervoorstellen aan het hoofd van de eigen stafafdeling en Information Security Officer.
- Het functioneel inhoudelijk aansturen van de IT medewerkers die verantwoordelijk zijn voor IT security.

Information Security Officer – 2e niveau
De Information Security Officer heeft een sleutelrol met betrekking tot het waarborgen van de betrouwbaarheid van de informatiesystemen die binnen de GGD Amsterdam in gebruik zijn. De office houdt toezicht op alle lopende projecten en activiteiten in verband met de ontwikkeling, implementatie, het beheer van en de naleving van het beleid (en hiervan afgeleide procedures en richtlijnen) met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid van informatie, in overeenstemming met van toepassing zijnde wet- en regelgeving.

De Information Security Officer is verantwoordelijk voor de aansturing en bewaking van GGD- brede projecten voor de betrouwbaarheid van informatie en het onderhouden van interne en externe contacten op dit terrein (inclusief het inrichten en beheren van het GGD Amsterdam controle raamwerk). Tevens is

de office verantwoordelijk voor het coördineren en communiceren van de activiteiten binnen de lijnorganisatie van de GGD Amsterdam voor wat betreft informatiebeveiliging.

De kerntaken en verantwoordelijkheden van de Information Security Officer zijn:

- Het opstellen van en het toezien op het naleven van het informatiebeveiligingsbeleid, op basis van interne en externe ontwikkelingen. Het (laten) vertalen van het beleid naar architectuur, richtlijnen, eisen, procedures, methoden en technieken (inclusief het monitoren en borgen van de kwaliteit van risicoanalyses, ontwerpen en oplossingen). Het beleid heeft onder meer betrekking op logische en fysieke toegangsbeveiliging, het selecteren en aanschaffen van nieuwe systemen, het uitvoeren van risicoanalyses en het classificeren van informatie- en systemen.
- Het ontwerpen en inrichten van de organisatie voor informatiebeveiliging en de daarvoor benodigde expertise (inclusief calamiteitenorganisatie).
- Het opstellen van het informatiebeveiligingsplan, waarbij input wordt verkregen vanuit de 1e lijn. Het zorgdragen voor een projectportfolio voor informatiebeveiliging en het initiëren/ coördineren dan wel managen van GGD- brede projecten.
- Het inrichten van het <organisatie> controle raamwerk en bijbehorende IT-platform waarmee het proces van informatierisicomanagement wordt ondersteund. En het functioneel beheren van het IT-platform.
- Het afstemmen van informatiebeveiliging met andere domeinen, waaronder privacy, fysieke beveiliging en continuïteitsmanagement.
- Het initiëren en laten uitvoeren van risicoanalyses (inclusief systeemclassificaties). En het coördineren en bewaken van de voortgang van het selecteren en implementeren van maatregelen voor het waarborgen van het vastgestelde niveau van informatiebeveiliging.
- Het stimuleren en monitoren van het beveiligingsbewustzijn bij management (hoofden en teamleiders) en medewerkers door communicatie en voorlichting en het (laten) opstellen, uitvoeren en onderhouden van een communicatieplan.
- Het implementeren, (laten) uitvoeren en toezien op de naleving van de geselecteerde maatregelen (mede op basis van acties in het informatiebeveiligingsplan).
- Het zorgdragen voor een adequate registratie, analyse en rapportage van informatiebeveiligingsincidenten, samen met de IT security office.
- Het monitoren (inclusief borgen van de kwaliteit) op basis van assessments, testen, reviews en audits in hoeverre de GGD Amsterdam compliant is met het informatiebeveiligingsbeleid en vigerende wet- en regelgeving.
- Het coördineren van ernstige incidenten en het verzamelen van informatie over potentiële incidenten, beveiligingslekken en de rapportage hierover.
- Het (laten) rapporteren over de status van informatiebeveiliging aan de portefeuillehouder en het MT.
- Het (ongevraagd) adviseren van de directie en het lijnmanagement/afdelingsmanager (1e linie) over informatiebeveiliging.

Informatiemanagement – 1e /2e niveau
De kerntaken van informatiemanagement bestaan uit het vormgeven van de strategie, beleid, projectportfolio en architectuur van de informatievoorziening voor de GGD Amsterdam als geheel.

Informatiebeveiliging maakt integraal onderdeel uit van informatiemanagement, waarvoor naast die van Information Security Officer onderstaande kerntaken en verantwoordelijkheden gelden:

- Het functioneel/ inhoudelijk aansturen van de medewerkers die onderdeel uitmaken van functioneel beheer, en specifiek op het gebied van informatiebeveiliging.

- Het opstellen en beheren van specifieke richtlijnen en procedures voor informatiebeveiliging binnen een afdeling of team.

Functioneel beheer – 3e niveau
Na acceptatie en implementatie van het informatiesysteem ligt de verantwoordelijkheid van het gebruik bij de eigenaar (lijnmanagement/afdelingsmanager). Het gebruik kan geconcentreerd zijn binnen één afdeling (of slechts enkele medewerkers) maar kan ook verspreid zijn over de hele organisatie. De kern van functioneel beheer bestaat uit het optimaal laten gebruiken van informatiesystemen en aan te laten sluiten bij de werkprocessen.

Specifiek voor informatiebeveiliging gelden onderstaande kerntaken en verantwoordelijkheden:
- Beheren van gegevens die door het systeem worden verwerkt en gegevensuitwisseling met andere applicaties en derden. En het uitvoeren/ controleren van de hierbij behorende maatregelen gericht op het waarborgen van de integriteit van de gegevens.
- Beheren van de autorisaties van de applicatie/ systemen. En het uitvoeren/ controleren van de hierbij behorende maatregelen gericht op het waarborgen van de vertrouwelijkheid van de gegevens.

IT medewerkers (die operationeel verantwoordelijk zijn voor IT security) – 3e niveau
IT medewerkers met security in beschikken over diepgaande kennis op specifieke technische onderwerpen dan wel domeinen (onder meer firewalls, netwerk, besturingssystemen, etc.). Gelet op het specifieke en specialistische karakter kan deze functie zijn uitbesteed.

Voor deze specialisten gelden onderstaande kerntaken en verantwoordelijkheden
- Heeft diepgaande technische security kennis (op één of meerdere domeinen) en volgt relevante ontwikkelingen op dit vakgebied. Het opleiden en begeleiden van collega's in de technische beveiliging van systemen maakt hier onderdeel vanuit.
- Het kennisnemen van actuele dreigingen en dreigingstrends, het bepalen van de mogelijke impact hiervan op de organisatie en het geven van technisch advies.
- Het opstellen van technische ontwerpen en –oplossingen en het implementeren van security-by-design en privacy-by-design in informatiesystemen.
- Het realiseren van technische maatregelen en updates in systemen en de technische infrastructuur.
- Het selecteren en implementeren van security tooling.
- Het realiseren en monitoren van technische assessments, -tests, -reviews en –audits
- Het testen van het incident/response en continuïteitsplan.
- Het rapporteren aan IT security office over de effectiviteit van de werking van de technische maatregelen en het uitwerken van verbetervoorstellen aan IT security office.

Privacy Officer
Voor de kerntaken en verantwoordelijkheden van de Privacy Office wordt verwezen naar het privacybeleid van de GGD Amsterdam en Organisatie van informatiebeveiliging bij de gemeente Amsterdam.

Informatiebeheer (adviseurs)
- Advisering over de inrichting van het informatiebeheer voor nieuwe en bestaande informatiesystemen en projecten.
- Toetsen van het informatiebeheer aan de geldende wet- en regelgeving en IB-kaders en te adviseren c.q. hulp te bieden bij het implementeren daarvan.