senzer

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 799

15 september 2021

Officiële uitgave van de gemeenschappelijke regeling Werkbedrijf Atlant De Peel

Informatiebeveiligingsbeleid Senzer 2021-2023

Inhoud:
Het informatiebeveiligingsbeleid Senzer 2021 - 2023 is opgesteld aan de hand van de operationele Baseline Informatiebeveiliging Overheid (BIO) vervaardigd door de Informatiebeveiligingsdienst voor gemeenten (IBD).
Inhoud
1. Inleiding
1.1. Leeswijzer
1.2 Wat is informatiebeveiliging?
1.3 Ambitie en visie van Senzer op het gebied van informatieveiligheid

2. Strategisch beleid
2.1. Doel
2.1.1. Baseline Informatieveiligheid Overheid
2.1.2. Algemene Verordening Gegevensbescherming
2.1.2.1. Uitgangspunten uitvoering AVG binnen Senzer
2.1.3. De 10 principes van informatiebeveiliging
2.1.4. Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten
2.1.5. Informatie uit incidenten en inbreuken op beveiliging
2.2. Plaats van het strategisch beleid
2.3. Scope informatiebeveiliging
2.4. Uitgangspunten
2.4.1. Doelen
2.4.2. Belangrijkste uitgangspunten
2.4.3. Invulling van de uitgangspunten
2.4.4. Randvoorwaarden
3. Organisatie, taken & verantwoordelijkheden
3.1. Aansturing: Directieteam/CIO
3.2. Uitvoering: Proces- en systeemeigenaren
3.3. Uitvoering: Managers en teamleiders
3.4. Coördinatie/ondersteuning: CISO – FG – SO Suwinet
3.5. Controle: Interne Controle
3.6. Verantwoording: Directie
BIJLAGEN:
1. Kader BIO
2. 10 principes van informatiebeveiliging
3. Taken/verantwoordelijkheden proces- en systeemeigenaren
4. Voorlopige (taak)profielen CISO, FG en SO Suwinet

1. Inleiding
Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2021 tot en met 2023 en vervangt het in december 2019 vastgestelde "Informatiebeveiligingsbeleid Senzer 2020 – 2022". Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.
Met dit Informatiebeveiligingsbeleid 2021 - 2023 zet Senzer een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen Senzer te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (Kader BIO, zie bijlage 1).
Het vorig vastgestelde Informatiebeveiligingsbeleid 2020 - 2022 wordt tussentijds aangepast in verband met de onderstaande onderwerpen, waarvan het belang dermate groot is dat zij dienen te worden opgenomen in het strategische informatiebeveiligingsbeleid:
-Uitgangspunten toepassing Algemene Verordening Gegevensbescherming.
-Taken en verantwoordelijkheden proces- en systeemeigenaren.
-Voorlopige positionering en (taak)profielen CISO, FG en SO Suwinet

1.1 Leeswijzer
In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatiebeveiligingsplan worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is

geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.
1.2 Wat is informatiebeveiliging?
Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Kernpunten daarbij zijn beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van Senzer en borgt daarmee de informatievoorziening gedurende de hele levenscyclus van informatiesystemen, ongeacht de toegepaste technologie en ongeacht het karakter van de informatie. Het beperkt zich niet alleen tot de ICT, maar heeft ook betrekking op fysieke beveiliging en gedrag van mensen. Het heeft betrekking op alle medewerkers, burgers, gasten, bezoekers en externe relaties.

2. Strategisch beleid
2.1 Doel
Het doel van deze beleidsnota is het presenteren van het Informatiebeveiligingsbeleid Senzer 2020 - 2022. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan.
Het informatiebeveiligingsbeleid is gebaseerd op gegevens die staan vermeld of voortkomen uit de bronnen in de hierna beschreven paragrafen 2.1.1. tot en met 2.1.5.
2.1.1 De BIO (zie bijlage 1)
De interbestuurlijke werkgroep Normatiek1 heeft in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van de NEN-normen vanuit de NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen. Op grond van de met de gemeenten afgesloten Verwerkersovereenkomsten, afgesloten op basis van de Gemeenschappelijke Regeling WADP/Mandaatbesluit Samenwerking WADP (punt II sub C), geldt het BIO ook voor Senzer. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. De inhoud en structuur van deze nota zijn afgestemd op die van de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.
De werkwijze van de BIO is gericht op risicomanagement. Dat wil zeggen dat het management nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.
2.1.2 Algemene Verordening Gegevensbescherming
Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van Senzer en de relevante landelijke en Europese wet- en regelgeving, waarbij met name ook de Algemene Verordening Gegevensbescherming (AVG). De AVG regelt in artikel 32 welke maatregelen organisaties moeten treffen in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen. Voor wat betreft Senzer is daarnaast uitgegaan van de verwerking van persoonsgegevens, zoals bedoeld in artikel 9 en 10 van de AVG. Deze maatregelen dienen deel uit te maken van het informatiebeveiligingsbeleid van Senzer.
2.1.2.1 Uitgangspunten uitvoering AVG binnen Senzer
Senzer maakt gebruik van diverse informatiesystemen waarin persoonsgegevens worden verwerkt. In dit Informatieveiligheidsbeleid Senzer is vastgelegd dat voor ieder informatiesysteem een systeemeigenaar dient te worden aangewezen en dat de systeemeigenaar eindverantwoordelijk is voor de verwerking van de persoonsgegevens binnen zijn informatiesysteem. Teneinde te voorkomen dat systeemeigenaren te verschillend omgaan met de te maken keuzes in het kader van het verwerken van persoonsgegevens in de informatiesystemen is het belangrijk dat door de uitgangspunten worden geformuleerd die door Senzer worden gehanteerd. Daardoor kan worden bereikt dat organisatiebreed in principe op dezelfde wijze wordt omgegaan met de verwerking van persoonsgegevens, waarbij maatwerk binnen de verschillende informatiesystemen mogelijk moet blijven. Het maatwerk heeft dan met name betrekking hebben op de volgende onderwerpen:
-Welke persoonsgegevens worden er verwerkt in de verschillende informatiesystemen.
-Het toebedelen van toegangsrechten voor informatiesystemen en tot welk niveau.
Ten behoeve van de bovengenoemde punten zullen uitgangspunten moeten worden geformuleerd, die recht doen aan de AVG, de BIO als mede de praktische uitvoering, zowel kijkende naar de technische als de bedrijfsvoeringsmatige (on)mogelijkheden en de daarbij behorende risico's. Hieronder volgt een opsomming van de binnen Senzer gehanteerde uitgangspunten:

1. Bij de verwerking van persoonsgegevens wordt de privacywetgeving en andere van belang zijnde wetgeving (denk o.a. aan de archiefwetgeving en de daarin vermelde bewaartermijnen) niet overtreden.
2. Persoonsgegevens worden alleen verwerkt ten behoeve van een specifiek doel, waarbij het doel duidelijk omschreven is en de persoonsgegevens niet langer worden verwerkt dan noodzakelijk.

3. De verwerking van persoonsgegevens beperkt zich tot die gegevens die noodzakelijk zijn voor het te bereiken doel.
4. Er worden maatregelen getroffen om persoonsgegevens die onjuist of volledig zijn te wissen of te rectificeren.
5. Persoonsgegevens worden, bij voorkeur geautomatiseerd, verwijderd zodra deze niet langer nodig zijn voor het oorspronkelijke doel waarvoor ze zijn verzameld.
6. De informatiesystemen worden tijdig voorzien van de benodigde beveiligingsupdates en beveiligingsupdates worden gearchiveerd.
7. Persoonsgegevens moeten worden verwerkt op een dusdanige manier dat een passende technische of organisatorische beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging" (integriteit en vertrouwelijkheid).
8. Toegangsrechten tot een informatiesysteem en de zich daarin bevindende persoonsgegevens worden alleen gegeven aan medewerkers die de betreffende persoonsgegevens nodig hebben om hun opgedragen werkzaamheden te kunnen uitvoeren. Daarbij wordt ook gekeken tot welk niveau/onderdeel binnen dat informatiesysteem de toegangsrechten worden verleend als er sprake is van verschillende niveaus/onderdelen binnen dat informatiesysteem. Om vorenstaande te realiseren worden onderstaande acties uitgevoerd:
   a.Voor elk informatiesysteem wordt door de systeemeigenaar een autorisatieprocedure en –matrix vastgesteld.
   b.Toegangsrechten worden toegekend, aangepast en verwijderd volgens de vastgestelde autorisatieprocedure en op basis van de vastgestelde autorisatiematrix.
   c.1 x per 3 jaar, of tussentijds indien daartoe aanleiding bestaat, worden vastgestelde autorisatieprocedures en -matrixen geëvalueerd.
   d.Periodieke controle van alle verleende toegangsrechten (conform de termijnen gesteld in het BIO).

De onderdelen a tot en met c en e worden ter advisering besproken met de CISO2 en de FG3. De onderdelen d wordt na verrichting gearchiveerd en teruggekoppeld aan de CISO.
2 Chief Information Security Officer
3 Functionaris Gegevensbescherming

2.1.3 De 10 principes voor informatiebeveiliging (zie bijlage 2)
De 10 principes voor informatiebeveiliging zijn een aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:
1. Management bevordert een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. De directie controleert en evalueert.

De principes gaan vooral over de rol van het management bij het borgen van informatiebeveiliging binnen Senzer. Deze principes ondersteunen het management bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de processen van Senzer, dan kan dit directe gevolgen hebben voor de deelnemende gemeenten, medewerkers, klanten en partners. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de managementtafel.

2.1.4 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten
Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten geeft een actueel zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.1.5 Informatie uit incidenten en inbreuken op beveiliging
Senzer kent naast het hierboven genoemde dreigingsbeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd (Topdesk). Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.2 Plaats van het strategisch beleid
Dit Informatiebeveiligingsbeleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid

zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven "Informatiebeveiligingsplan Senzer".

2.3 Scope informatiebeveiliging

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van Senzer, de deelnemende gemeenten en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur. Dit Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de SUWI. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI). Deze worden in aanvullende documenten geformuleerd. Bewust wordt in dit beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.4 Uitgangspunten

Het management speelt een cruciale rol bij het uitvoeren van dit Informatiebeveiligingsbeleid. Het management maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor Senzer heeft, de risico's die Senzer hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Op basis hiervan zet het management dit beleid voor informatiebeveiliging op, draagt dit uit naar de organisatie en ondersteunt en bewaakt de uitvoering ervan.

Het gehele management geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor geheel Senzer. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen).

2.4.1 Doelen

De doelen van het informatiebeveiligingsbeleid zijn:

1. Het managen van de informatiebeveiliging.
2. Adequate bescherming van 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.

2.4.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

1. Alle informatie en informatiesystemen zijn van belang voor Senzer, bepaalde informatie is van vitaal en kritiek belang. De Algemeen directeur is eindverantwoordelijke voor de informatiebeveiliging.
2. De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Senzer hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
3. Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatiebreed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
4. Informatiebeveiliging is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging.
5. Senzer stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
6. Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
7. Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.4.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

1. De Algemeen directeur stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
2. De Algemeen directeur stelt jaarlijks het informatiebeveiligingsplan vast.
3. De directie is verantwoordelijk voor het vragen om informatie bij de managers en ziet erop toe dat de managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
4. De CIO is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
5. De CISO, FG en SO Suwinet ondersteunen vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteren, periodiek, in principe per kwartaal en tussentijds indien noodzakelijk, hierover rechtstreeks aan de directie.
6. Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportages van de CISO, FG en SO Suwinet. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
7. De managers/teamleiders zijn in de lijn verantwoordelijk voor de uitvoering van de informatiebeveiliging met betrekking tot de processen en/of systemen waarvoor zij (mede) verantwoordelijk zijn.
8. Per proces of informatiesysteem wordt een proces- respectievelijk systeemeigenaar aangewezen, die eindverantwoordelijk is voor de aan hem/haar toegewezen processen en informatiesystemen. De proces- en systeemeigenaar is geen afzonderlijke functie, maar is een taak/rol die wordt uitgevoerd binnen een bepaalde functie. De specifieke taken en verantwoordelijkheden van de proces- respectievelijk systeemeigenaar zijn beschreven en zijn als bijlage 3 bij dit informatiebeveiligingsbeleid gevoegd.
9. Systeemeigenaren dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
10. Alle medewerkers van Senzer worden getraind in het gebruik van beveiligingsprocedures.
11. Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
12. De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Systeemeigenaren voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.4.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

1. De informatiebeveiliging maakt deel uit van afspraken met ketenpartners.
2. Kennis en bewustzijn van informatiebeveiliging en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
3. Jaarlijks wordt een informatiebeveiligingsplan opgesteld door de CISO, gebaseerd op:
    1. het dreigingsbeeld gemeenten van de IBD;
    2. Informatie uit incidenten en inbreuken op beveiliging;
    3. De door de managers/teamleiders en/of proces-/systeemeigenaren ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn.

3. Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het management verantwoordelijk voor de eigen processen/informatiesystemen. De tweede lijn (CISO voor wat betreft de algehele informatiebeveiliging en daarnaast de SO Suwinet en de FG met betrekking tot hun specifieke onderdelen respectievelijk Suwinet en AVG) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Zij voeren deze taken uit vanuit een onafhankelijke positie en kunnen daarbij, indien noodzakelijk, rechtstreeks schakelen met de directie en/of bestuur. In de derde lijn wordt het geheel door een (interne) auditor (denk bij interne auditor aan Interne Controle vallend onder de Concerncontroller) van een

objectief oordeel voorzien met mogelijkheden tot verbetering. Deels kan de FG ook nog onder de derde lijn worden gebracht gezien de taak gericht op controle van een juiste omgang met persoonsgegevens, echter grotendeels zal de FG kunnen worden geschaard onder de tweede lijn.

3.1 Aansturing: directieteam/CIO

De directie zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een manager/teamleider. De directie zorgt dat de managers/teamleiders zich verantwoorden over de beveiliging van de informatie die onder hen berust.
De directie stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directie draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO.
De directie autoriseert de benodigde procedures en uitvoeringsmaatregelen, tenzij dit is gemandateerd naar het overige management. Het onderwerp informatiebeveiliging wordt binnen Senzer gezien als een integraal onderdeel van risicomanagement.
De CIO maakt deel uit van het MT Senzer en geeft namens de directie van Senzer op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.

3.2 Uitvoering: Proces- en systeemeigenaren

Aan alle processen, systemen, data, applicaties wordt één verantwoordelijk eigenaar toegewezen, die eindverantwoordelijk is voor een proces of een informatiesysteem. De proces- en systeemeigenaar is een manager, teamleider of een ander daartoe aangewezen functionaris op grond van specifieke kennis. Zij rapporteren aan de directie (via de CIO/CISO) over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten (denk aan bijvoorbeeld: verslag van halfjaarlijkse controle autorisaties informatiesystemen).
De specifieke taken en verantwoordelijkheden van de proces- respectievelijk systeemeigenaar zijn beschreven en zijn als bijlage 3 bij dit informatiebeveiligingsbeleid gevoegd.

3.3 Uitvoering: Managers en teamleiders

Informatiebeveiliging valt onder de verantwoordelijkheden van alle managers en teamleiders. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. De verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel.
Taken van de managers/teamleiders in het kader van informatiebeveiliging zijn:

-Het leveren van input voor wijzigingen op maatregelen en procedures.
-Het binnen de eigen afdeling/team uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
-Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
-Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.
-Het delen van input uit bovenstaande punten met de proces- en/of systeemeigenaren die verantwoordelijk zijn voor het gerelateerde proces(sen) en/of informatiesystemen.

3.4 Coördinatie/ondersteuning: CISO - FG - SO Suwinet

De CISO, FG en SO Suwinet ondersteunen, adviseren (gevraagd en ongevraagd), coördineren en bewaken of de uitvoering zijn verantwoordelijkheden ook daadwerkelijk neemt. Zij hebben periodiek overleg met de CIO. Zij doen vorenstaande met betrekking tot:

-CISO: Algehele informatiebeveiliging m.u.v. de deelgebieden van de FG en SO Suwinet.
-FG: Algemene Verordening Gegevensbescherming.
-SO Suwinet: Suwinet-Inkijk.
De taken van de CISO, FG en SO Suwinet bestaan binnen hun eigen (deel)gebied onder andere uit:

-Het voorbereiden en opstellen van beleid.
-Het ondersteunen/adviseren van het management en proces- en systeemeigenaren bij het uitvoeren van verplichting met betrekking tot informatiebeveiliging.
-Het archiveren en/of van publiceren van beleidstukken met betrekking informatiebeveiliging en verantwoordingsrapportages van managers.
-Het opstellen van kwartaalverslagen met betrekking tot informatiebeveiliging. Het kwartaalverslag betreft een coproductie van de CISO, FG en SO Suwinet en wordt via de CIO aangeboden aan het MT Senzer.
-Het laten uitvoeren van interne en externe audits.
Een voorlopig (taak)profiel van zowel de CISO, FG respectievelijk SO Suwinet is als bijlage 4 bij dit beleid gevoegd en zal gelden tot het moment dat de huidige doorontwikkeling van de organisatie Senzer is afgerond. Die doorontwikkeling zal vermoedelijk worden geëffectueerd per 01-01-2022. Dan zal ook het definitieve profiel en positie in de organisatie van de CISO, FG respectievelijk SO Suwinet worden vastgesteld. De CISO, FG respectievelijk SO Suwinet behoeft geen zelfstandige functie zijn, maar kan een rol zijn binnen een bestaande functie.

3.5 Controle: Interne Controle

De interne controle op de uitvoering van de processen en de verwerking van gegevens in de informatiesystemen vindt plaats op 2 niveaus:

1.In de uitvoering door controlemechanismen in te bouwen in de processen en in het kader van integriteit en vertrouwelijkheid van gegevens zorg te dragen voor vastgestelde autorisatieprocedures- en matrixen ten behoeve van de informatiesystemen alsmede het monitoring op de juiste toepassing daarvan. De verantwoordelijkheid hiervoor ligt bij de proces- respectievelijk systeemeigenaar.
2.Het team Interne Controle voert jaarlijks een interne audit uit op de juiste werking van informatiebeveiligingsactiviteiten, waarbij met name aandacht wordt besteed aan die processen en informatiesystemen die risicovol zijn (denk aan bijvoorbeeld: het proces van verstrekken van toegangsrechten volgens de vastgestelde procedures met betrekking tot kernapplicaties, zoals SSD en Szeebra). Interne Controle geeft daarbij een objectief oordeel voorzien met mogelijkheden tot verbetering.
Interne Controle behoeft geen interne audit te verrichten met betrekking tot informatiebeveiligingsactiviteiten aangaande Suwinet-aansluiting en Digid-aansluiting.
Bij genoemde aansluitingen vindt jaarlijks al een verplichte externe audit plaats, welke middels een interne audit worden voorbereid door de CISO.

3.6 Verantwoording: Directie

Dit strategisch informatiebeveiligingsbeleid is een verantwoordelijkheid van de directie van Senzer en zij zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.
De directie is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan het Dagelijks bestuur van Senzer. De directie rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.
Vastgesteld te Helmond op 22 februari 2021.
De Algemeen directeur Senzer,
A.E.W. van Limpt
Bijlagen zijn op te vragen