

# Informatiebeveiligingsbeleid Senzer 2024

# Inhoudsopgave

Inhoudsopgave .....	2
1. Inleiding .....	3
2. BIO-normen .....	4
3. Organisatie .....	5
3.1 Aansturing: directieteam/CIO .....	5
3.2 Uitvoering: Proces- en systeemeigenaren .....	5
3.3 Uitvoering: Managers en teamleiders.....	5
3.4 Coördinatie/ondersteuning: CISO - FG - SO Suwinet .....	6
3.5 Controle: Interne Controle .....	6
3.6 Verantwoording: Directie .....	7
4. Autorisatiebeleid .....	8
5. Antivirusbeleid.....	9
6. Backup- en restore beleid .....	10
7. Classificatiebeleid .....	12
8. Clear desk en clear screen beleid .....	15
9. Cryptografiebeleid.....	16
10. Fysieke toegangsbeleid .....	17
11. Logging beleid.....	18
12. Veilig Personeelsbeleid.....	21
13. Privacy beleid .....	23
14. Hybride werken beleid .....	24
15. Cloud beveiliging beleid .....	25
16. Leveranciersbeleid.....	26
17. Netwerkbeleid .....	27
18. Wachtwoord beleid.....	28
19. Update en patch beleid .....	30
20. Gebruikersaccount beleid .....	31
21. Externe communicatiebeleid.....	32
Bijlage 1: BIO verantwoording.....	33
Bijlage 2: Inkoop Eisen ten aanzien van informatiebeveiliging.....	41
Bijlage 3: Functieprofielen.....	43
Vaststellen beleid in het DT.....	46

# 1. Inleiding

Dit document beschrijft het informatiebeveiligingsbeleid dat van toepassing is op alle medewerkers, processen en systemen van onze organisatie. Het doel van dit beleid is om de vertrouwelijkheid, integriteit en beschikbaarheid van onze informatie te waarborgen en te beschermen tegen ongeautoriseerde toegang, wijziging, openbaarmaking of vernietiging. Dit beleid is gebaseerd op eerdere reeds bestaande beleidsstukken, de Baseline Informatiebeveiliging Overheid (BIO), handreikingen vanuit de InformatieBeveiligingsDienst (IBD), aansluiting op de visie en strategie digitalisering, bijbehorende digitale spelregels en eigen inzichten.

Het naleven van dit beleid is een verantwoordelijkheid van iedereen die betrokken is bij het verwerken van informatie binnen onze organisatie.

Dit beleid biedt kaders voor de organisatie en van hieruit kunnen de verantwoordelijken procedures opstellen, die medewerkers dienen te volgen.

Het is van belang te erkennen dat bepaalde aspecten van dit beleid nog niet volledig zijn geïmplementeerd binnen onze organisatie. We streven ernaar dat na dit initiële jaar het beleid volledig en uniform binnen de gehele organisatie van kracht zal zijn.

Dit document kan, indien nodig, worden aangevuld of uitgebreid wanneer blijkt dat, mogelijk door (toekomstige) ontwikkelingen, het beschrevene in dit document niet toereikend (genoeg) is.

## Vervanging voorgaande beleidsstukken

Bij vaststelling van dit beleidsstuk komen de voorgaande beleidsstukken te vervallen en zal dit informatiebeveiligingsbeleid gelden:

- Autorisatiebeleid Senzer, d.d. 2019-06-03
- Back- up en recoverymanagement Senzer 2021-2024
- Dataclassificatiebeleid Senzer 2020-2022, d.d. 2019-12-09
- Informatiebeveiligingsbeleid Senzer 2021-2023
- Patchmanagement Senzer 2021-2024
- Privacybeleid Senzer
- Toegangsbeleid Senzer, d.d. 2019-06-03
- Wachtwoordbeleid Senzer 2023\_getekend

## 2. BIO-normen

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen in Nederland, waaronder het Rijk, gemeenten, provincies en waterschappen.

De BIO heeft tot doel de informatieveiligheid te versterken door betere afstemming binnen ketens van overheden en andere partijen. Het biedt uniforme beveiligingsnormen voor de overheid en vermindert administratieve lasten voor zowel afnemers als leveranciers.

De BIO is gebaseerd op internationaal erkende en actuele ISO-normen, met name de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017. Deze normen vormen ook de basis voor informatiebeveiliging binnen de overheid.

Naast de ISO-standaarden geeft de BIO specifieke overheidsmaatregelen voor beveiligingscontroles. Deze maatregelen zijn gericht op de unieke behoeften en dreigingen waarmee overheidsorganisaties te maken hebben.

Zie [Bijlage 1](#) voor een verantwoording welke Bio-normen zijn afgedekt door dit beleid.

### NIS2

De NIS2 (Network and Information Systems Directive 2) is een Europese richtlijn die zich richt op de beveiliging van netwerken en informatiesystemen. Deze richtlijn is van toepassing op vitale dienstverleners en digitale dienstverleners binnen de Europese Unie. De NIS2 legt een zorgplicht op aan vitale dienstverleners om passende maatregelen te nemen om hun netwerken en informatiesystemen te beschermen tegen cyberdreigingen en wordt rechtstreeks omgezet in nationale wetgeving van EU-lidstaten, inclusief Nederland. Senzer zal zich ook moeten gaan conformeren aan de NIS2.

## 3. Organisatie

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 DT 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

Voor het goed kunnen uitvoeren van alle vraagstukken op het gebied van informatiebeveiliging is het noodzakelijk dat het eigenaarschap van de vraagstukken helder is belegd. Het ontbreekt binnen de organisatie nog aan formele afspraken en vastlegging van proces- en systeemeigenaarschap. Hier wordt evenwel aan gewerkt. Voor het adresseren van vraagstukken uit dit informatiebeveiligingsbeleid sluiten we daar zoveel mogelijk op aan, dan wel vallen we terug op lijnverantwoordelijkheden.

### 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 en uitvoeren van het beveiligingsbeleid, de daaraan gerelateerde procedures.
- Het vroegtijdig signaleren van de 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.
- Het classificeren van vertrouwelijkheid in het kader van te publiceren stukken mbt de Woo.

### **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.

Een (taak)profiel van zowel de CISO, FG en de SO Suwinet is in bijlage 3 te vinden. 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 informatiebeveiligingsbeleid is een verantwoordelijkheid van de directie van Senzer en zij zullen volgens dit beleid 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 beleid.

## 4. Autorisatiebeleid

Dit autorisatiebeleid is van toepassing op informatiesystemen waarvan Senzer de eigenaar is. Ook als informatiesystemen niet binnen Senzer draaien is dit autorisatiebeleid van toepassing. Senzer maakt, indien mogelijk, gebruik van bestaande (landelijke) voorzieningen voor authenticatie. Voor elk bedrijfsproces, informatiesysteem, gegevensverzameling is een verantwoordelijk proceseigenaar benoemd. Wanneer er meerdere systemen en/ of verzamelingen worden gebruikt binnen meerdere bedrijfsprocessen wordt één verantwoordelijk proceseigenaar aangewezen.

### Beleidsregels en uitgangspunten

- Iedere verantwoordelijke systeemeigenaar is verplicht tot het uitvoeren van een risicoanalyse voor de informatiesystemen waarvoor hij/ zij verantwoordelijk is. Deze wordt overlegd aan de CISO.
- Vanuit Senzer is er een autorisatieprocedure opgezet. De applicatie wordt toegevoegd aan deze procedure. Dit gebeurt in overleg met de systeemeigenaar.
- De autorisaties die uitgegeven worden gebeuren op een 'need-to-know' en 'least privilege' basis. Dit betekent dat de medewerker alleen maar toegang krijgt tot gegevens die hij/ zij nodig heeft voor de uitoefening van het werk en dat hij/ zij alleen de noodzakelijke machtigingen krijgt.
- Het uitgeven van autorisaties gebeurt op een basis van de rol binnen de organisatie (Role Based Access Control: RBAC). Wanneer een rol/ functie van een medewerker verandert, behoren zijn/ haar rechten ook te wijzigen. Deze autorisaties worden zo min mogelijk los uitgegeven om het 'zwerven' van rechten te voorkomen.
- Er dient per functie binnen de organisatie een beschrijving te zijn van de autorisaties die bij die functie horen. De inventarisatie ligt bij HR (in overleg met IT). De autorisaties worden naar aanleiding van deze beschrijving ingericht te zijn. Uitzonderingen hierop worden door de leidinggevende aangevraagd. De CISO dient hierop goedkeuring te geven.
- Controle op de autorisaties per functie dient eens per half jaar gedaan te worden door de systeem/proceseigenaar. Deze controle wordt na afronding ter beschikking gesteld aan de CISO ter inzage.
- Het autorisatiebeleid moet duidelijk gecommuniceerd en gehandhaafd worden. Dit betekent dat alle gebruikers op de hoogte zijn van het autorisatiebeleid, en dat ze zich eraan houden. Mogelijke overtredingen en incidenten omtrent het autorisatiebeleid worden via het beveiligingsincident proces aangemeld.
- Het autorisatiebeleid moet ondersteund worden door passende technische maatregelen. Dit betekent dat er gebruik gemaakt wordt van sterke authenticatie- en autorisatiemechanismen, zoals wachtwoorden, tokens, biometrie of multifactorauthenticatie. Ook moet er een logging- en monitoringssysteem zijn om het gebruik van de informatie en systemen te registreren en te controleren. Zie hiervoor het loggingbeleid.

## 5. Antivirusbeleid

Antivirussoftware is een essentieel onderdeel van de informatiebeveiliging voor Senzer. Het beschermt de systemen en gegevens tegen malware, zoals virussen, wormen, ransomware en spyware. Malware kan leiden tot verstoring van de bedrijfsvoering, verlies of beschadiging van gegevens, schending van de privacy of zelfs aantasting van de integriteit van de organisatie.

### Beleidsregels en uitgangspunten

- Binnen Senzer dient er op alle systemen een antivirus oplossing geïnstalleerd te zijn.
- De antivirus dient realtime bescherming te bieden.
- Er dienen regelmatig updates van de virusdatabase te worden gedaan. Deze dienen volgens de patchprocedure opgepakt te worden.
- Binnen de antivirus dient logging ingeschakeld te zijn.
- Alerts welke de antivirus genereert dienen te worden doorgestuurd naar IT en/ of SOC/SIEM-provider voor verdere analyse, opvolging of rapportage.
- Het team IT is belast met de uitvoering van dit beleid.

## 6. Backup- en restore beleid

Een manier om de beschikbaarheid van bedrijfskritische informatie te waarborgen is het maken en terugzetten van backups. Dit houdt in dat er regelmatig kopieën worden gemaakt van de informatie, de systemen en applicaties waar deze op draaien, en de systeemconfiguraties (zoals machine-instellingen en Active Directory). Dit is cruciaal voor het herstellen van informatie die beschadigd, verloren of vernietigd is door een calamiteit of een uitwijkscenario. Een effectieve backupstrategie zorgt voor een passend schema dat de kans op een succesvolle restore vergroot.

### Beleidsregels en uitgangspunten

- Er worden reserve kopieën gemaakt van alle essentiële bedrijfsgegevens, programmatuur en system states.
- Backups volgen de voorschriften in lijn met de wettelijke bewaartermijn (Archiefwet/AVG).
- Bij ketensystemen dient het backup mechanisme de data-integriteit van de informatieketen te waarborgen.
- De backups dienen dagelijks gecontroleerd te worden en herstelprocedures worden ten minste 1x per jaar, of na een grote wijziging ingepland en getest om de betrouwbaarheid ervan vast te stellen. De uitkomsten hiervan worden vastgelegd en op verzoek beschikbaar te worden gesteld.
- Het team IT is belast met het uitvoeren van dit beleid.
- Dataverlies moet worden beperkt tot maximaal 24 uur.
- De hersteltijd in geval van incidenten bedraagt maximaal 16 werkuren in 85% van de gevallen.
- Minstens drie versies van een backup moet worden bewaard namelijk:
  - Een online backup on-site
  - Een online backup off-site (deze dient binnen de EU opgeslagen te zijn)
  - Een offline backup
- Er dient minimaal één volledige online backup te worden opgeslagen in een veilige, off-site locatie. Deze locatie dient te zijn goedgekeurd door de CISO.
- Vereiste backup documentatie omvat de identificatie van alle belangrijke gegevens, programma's, documentatie en support items die nodig zijn om essentiële taken tijdens een herstelperiode te voeren. Documentatie van het restoreproces omvat procedures voor het hertel van single-system of applicatiestoringen, alsmede voor een totale datacenter ramp scenario (in geval van uitwijk), indien van toepassing.
- De IT-procedures omtrent backup en restore worden minimaal jaarlijks getest. De uitkomst hiervan wordt vastgelegd. Hier moet ook rekening gehouden worden met nieuwe technologie, veranderingen in het bedrijf en de migratie van toepassingen naar alternatieve platforms (bijvoorbeeld cloud). Deze procedures worden aangepast aan deze veranderingen. De uitkomsten hiervan worden vastgelegd en op verzoek beschikbaar te worden gesteld.
- Restore procedures moeten minimaal op jaarbasis worden getest:
  - Er wordt een jaarlijkse planning opgemaakt door IT van de te verrichten testen aangaande de herstelprocedures van systemen en data. De jaarplanning wordt besproken met de betrokken systeemeigenaren en de CISO en uiterlijk vastgesteld in de maand december voorafgaan aan het testjaar.
  - Van de uit te voeren testen aangaande de herstelprocedure wordt een logboek bijgehouden door IT.

- Het logboek dient 2 jaar bewaard te worden.
- Na afloop van de testprocedure wordt een overleg ingepland met de betrokken systeemeigenaar en de CISO teneinde de testprocedure te evalueren. Daarbij wordt ook het logboek van de backup procedure besproken. Van de evaluatie wordt een verslag gemaakt, die ter beschikking wordt gesteld aan de betrokken systeemeigenaar en de CISO.
- De CISO neemt in zijn kwartaalverslag informatieveiligheid een passage op met betrekking tot het backup- en recoverymanagement.

### Backup cyclus en bewaartermijn

Soort backup	Wanneer gemaakt	Bewaartermijn
Dagbackup	Iedere werkdag (op een vast moment op de dag)	1 week
Weekbackup	Iedere week (op een vaste dag in de week)	4 weken of een maand
4-wekelijkse backup	Iedere 4 weken of op de laatste dag van de maand	12 weken of een kwartaal
Kwartaalbackup	Om de 16 weken of op de laatste dag van het kwartaal	Een jaar

## 7. Classificatiebeleid

Het beschermingsniveau van data wordt uitgedrukt in de classificatieniveaus Beschikbaarheid, Integriteit, en Vertrouwelijkheid van informatie.

Dataclassificatie is een eenvoudige en praktische vorm van risicoanalyse waarbij de waarde van informatie wordt bepaald. Een risicoanalyse helpt bij het identificeren van risico's en hun omvang. Op basis daarvan kunnen passende beveiligingsmaatregelen worden genomen om de risico's te minimaliseren.

Classificatie is vooral nuttig bij het vertalen van risico's naar concrete maatregelen. Het classificatiebeleid van Senzer is van toepassing op alle gegevens, informatiesystemen en gerelateerde processen, zelfs als deze zich buiten het computernetwerk van Senzer bevinden, bijvoorbeeld bij externe partners.

### Beleidsregels en uitgangspunten

- De directie, meer concreet de CIO, is primair verantwoordelijk voor de invoering en handhaving van het beleid dataclassificatie.
- De managers/teamleiders zijn verantwoordelijk voor de correcte naleving van dit beleid door hun medewerkers en rapporteren onmiddellijk een onbedoelde of opzettelijke schending van dit beleid, met name inbreuken die een relatie hebben met de Algemene Verordening Gegevensbescherming. Dit gebeurt via de beveiligingsincident procedure.
- De Chief Information Security Officer (CISO) is eigenaar van het proces dataclassificatie en hierdoor verantwoordelijk voor het voorbereiden, opstellen en controleren van het beleid dataclassificatie. De CISO coördineert de implementatie van het beleid en faciliteert de uitvoering van de dataclassificatie.
- De medewerker is verantwoordelijk om de geclassificeerde data te behandelen in lijn van dit beleid en onmiddellijk een onbedoelde of opzettelijke schending van dit beleid te melden bij de teamleider en via de beveiligingsincident procedure, met name inbreuken die een relatie hebben met de Algemene Verordening Gegevensbescherming.
- De verantwoordelijk proceseigenaar bepaalt het vereiste beschermingsniveau (classificatie). Indien sprake is van wettelijke eisen wordt dit expliciet aangegeven. De verantwoordelijk proceseigenaar bepaalt tevens wie toegang krijgt tot welke gegevens.
- Er wordt gestreefd naar een zo 'laag' mogelijk classificatieniveau; te hoge classificatie leidt namelijk tot onnodige kosten. Bovendien dient data in beginsel voor zoveel mogelijk mensen beschikbaar zijn in het kader van een transparante overheid.
- Het object van classificatie is data. De classificatie die door het soort data bepaald wordt geldt ook voor het hogere niveau van informatiesystemen (of informatieservices), dat wil zeggen dat als een systeem geheime informatie verwerkt het hele systeem als geheim wordt aangemerkt tenzij voor dat hogere niveau maatregelen genomen zijn binnen het informatiesysteem.
- Alle classificaties van alle bedrijfskritische systemen zijn centraal vastgelegd en dienen tweejaarlijks gecontroleerd te worden door de CISO.
- In alle gevallen kan de eigenaar van de gegevens zich voor het classificeren laten ondersteunen door beveiligingsspecialisten, zoals de CISO.
- Nadat het classificatieniveau is vastgesteld dient de proceseigenaar dit vast te leggen in een classificatierapport.

- Het classificatierapport wordt door de verantwoordelijk proceseigenaar vastgesteld, tenzij er sprake is van een kernapplicaties (SSD, Szeebra, Mercash, Navision- Financieel, Suwinet, Snelbalie en Verzuimexpert) of de verantwoordelijk proceseigenaar het noodzakelijk vindt dat de dataclassificatie om moverende redenen door het DT Senzer dient te worden vastgesteld.
- Tegelijkertijd met het opmaken van het Dataclassificatierapport wordt tevens, indien noodzakelijk als er nadere (beveiligings)maatregelen dienen te worden uitgevoerd, een plan van aanpak opgemaakt. In dat plan van aanpak worden de te nemen maatregelen benoemd, wie daarvoor verantwoordelijk is, de tijdsplanning en eventuele daaraan verbonden kosten.
- Na vaststelling van het Dataclassificatierapport en het eventuele plan van aanpak worden beiden verstrekt aan de CISO ten behoeve van een centrale registratie en monitoring van de te nemen (beveiligings)maatregelen.

## Bepalen classificatie

Er wordt binnen classificatie met 4 niveaus gewerkt: 0, BBN1, BBN2, BBN3 (= BBN2 met aanvullende risicoanalyse)


	0	BBN1	BBN2	BBN3
<b>Beschikbaarheid</b>	<u>Niet nodig:</u> De gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn. Schending van beschikbaarheid heeft geen gevolgschade.	<u>Belangrijk:</u> De informatie of service mag incidenteel uitvallen, het bedrijfsproces staat incidentele uitval toe. De continuïteit zal op redelijke termijn moeten worden hervat. Schending van beschikbaarheid kan enige (in)directe schade toebrengen	<u>Noodzakelijk:</u> De informatie of service mag bijna nooit uitvallen, het bedrijfsproces staat nauwelijks uitval toe. De continuïteit zal snel moeten worden hervat. Schending van beschikbaarheid kan serieuze (in)directe schade toebrengen.	<u>Essentieel:</u> De informatie of service mag alleen in zeer uitzonderlijke situaties uitvallen, bijvoorbeeld als gevolg van een calamiteit, het bedrijfskritische bedrijfsproces staat eigenlijk geen uitval toe. De continuïteit zal zeer snel moeten worden hervat. Schending van beschikbaarheid kan (zeer) grote schade toebrengen.
<b>Integriteit</b>	<u>Niet zeker:</u> Deze informatie mag worden veranderd. Geen extra bescherming van integriteit noodzakelijk. Schending van integriteit heeft geen gevolgschade.	<u>Beschermd:</u> Het bedrijfsproces dat gebruik maakt van deze informatie staat enkele (integriteits-) fouten toe. Een basisniveau van beveiliging is noodzakelijk. Schending van integriteit kan enige (in-)directe schade toebrengen	<u>Hoog:</u> Het bedrijfsproces dat gebruik maakt van deze informatie staat zeer weinig (integriteits-)fouten toe. Bescherming van integriteit is absoluut noodzakelijk. Schending van integriteit kan serieuze (in)directe schade toebrengen.	<u>Absoluut:</u> Het bedrijfsproces dat gebruik maakt van deze informatie staat geen (integriteits-) fouten toe. Schending van integriteit kan (zeer) grote schade toebrengen
<b>Vertrouwelijkheid</b>	<u>Openbaar:</u> Alle informatie die algemeen toegankelijk is voor iedereen. Er is geen schending van vertrouwelijkheid mogelijk.	<u>Bedrijfsvertrouwelijk:</u> Informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.	<u>Vertrouwelijk:</u> Informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. <sup>3</sup> De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.	<u>Geheim</u> Dit betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen. Weerstand tegen statelijke actoren noodzakelijk.

Aangezien de niveaus BBN3 met name betrekking hebben op zeer vertrouwelijke informatie die staatsaangelegenheden kunnen raken, zal de classificatie BBN3 binnen Senzer niet voor komen.

## 8. Clear desk en clear screen beleid

Het clear desk en clear screen beleid is ervoor bedoeld dat er geen personen toegang hebben tot gevoelige informatie waar ze niet bij zouden mogen.

### Beleidsregels en uitgangspunten

- Zorg ervoor dat activa (zoals laptops, mobiele telefoons) worden afgesloten wanneer ze niet nodig zijn.
- Laat computers uitgelogd of beveiligd met een schermvergrendelingsmechanisme wanneer ze niet worden gebruikt.
- Werk zo veel mogelijk digitaal. Een papierloze cultuur wordt aangemoedigd. Ben terughoudend met het printen van informatie.
- Zorg dat er geen (gevoelige)informatie op whiteboards blijft staan.
- Laat vergaderruimtes leeg/ informatieloos achter.
- Papieren die niet meer nodig zijn worden verwijderd of gearhiveerd volgens de geldende procedures.
- Na 15 minuten van inactiviteit wordt de computer automatisch vergrendeld.
- Dossiers worden na werktijd bewaard in een afgesloten kast. Mocht de werkkamer kunnen worden afgesloten, dan kan worden volstaan met het afsluiten van de kamer mits de documenten niet door het raam alsnog te lezen zijn. Dit geldt ook als je de werkruimte verlaat om te gaan lunchen of voor een overleg.
- Mobile devices (laptop, notebook, tablet of mobiele telefoon) worden, indien deze na werktijd niet worden meegenomen door de gebruiker, bewaard in een afgesloten kast.
- Laptops en mobiele telefoons worden niet achtergelaten worden in de auto. Dit geldt ook wanneer de apparatuur in de auto uit het zicht kan worden opgeborgen.
- Als de werkplek wordt verlaten dient deze vergrendeld te worden (  + L)
- Bovenstaande beleidsregels en uitgangspunten gelden voor alle Senzer informatie ongeacht de locatie. Wanneer je thuiswerkt, gelden deze regels ook.
- Spreek collega's erop aan wanneer er niet aan deze punten voldaan wordt.
- Zorg dat gevoelige informatie niet zichtbaar is voor anderen.

## 9. Cryptografiebeleid

Cryptografie is de wetenschap en kunst van het versleutelen en ontsleutelen van informatie, zodat alleen de bedoelde ontvangers deze kunnen lezen en begrijpen. Cryptografie is nodig om de vertrouwelijkheid, integriteit en authenticiteit van informatie te beschermen, zowel 'at rest' (in rust) als 'in transit' (tijdens het versturen). Dit beleid helpt ons om de risico's te verminderen die gepaard gaan met het verlies, de diefstal of het misbruik van gevoelige informatie, en om te voldoen aan de wettelijke en regelgevende vereisten op het gebied van informatiebeveiliging.

### Beleidsregels en uitgangspunten

- De mate van encryptie wordt bepaald naar aanleiding van de classificatie van de data (zie [5.1 classificatiebeleid](#)).
- Versleuteling vindt plaats conform 'best practices', waarbij geldt dat de vereiste encryptie sterker is naarmate gegevens gevoeliger zijn. Hiervoor wordt gebruik gemaakt van het [forum standaardisatie](#) op basis van 'pas toe of leg uit'.
- Waar nodig kan overleg met CISO plaatsvinden of de encryptie voldoende is.
- Intern dataverkeer ('machine to machine') wordt conform classificatie beveiligd met certificaten.
- Het beheer van beveiligingscertificaten vindt centraal plaats op verantwoordelijkheid van IT.
- Het gebruik van HTTPS is verplicht waar van toepassing.
- Authenticatiemiddelen worden altijd versleuteld. Zowel 'in transit' als 'at rest'.
- Encryptie dient minimaal toegepast te worden op data die verstuurd wordt (zowel binnen het interne netwerk als het internet), als ook op vertrouwelijke data welke opgeslagen is.
- Senzer is bevoegd om beveiligingsinstellingen af te dwingen. Dit heeft betrekking op zowel door Senzer verstrekte middelen, als privé-apparatuur (bring your own device(BYOD)). Dit betreft onder meer versleuteling.
- Om bedrijfsinformatie op mobiele apparaten te beveiligen zijn deze zo ingericht dat geen bedrijfsinformatie wordt opgeslagen ('zero footprint'). Voor het geval dat zero footprint (nog) niet realiseerbaar is, of functioneel onwenselijk is, wordt de toegang tot het apparaat beschermd door middel van een wachtwoord en is apparaatversleuteling geïmplementeerd .
- Om vertrouwelijke en geheime informatie te beschermen is het niet toegestaan om dit type informatie te delen via niet goedgekeurde voorzieningen zoals Whatsapp, als ook sociale netwerken en clouddiensten (Dropbox, Gmail, et cetera.). Dit vanwege het lage beschermingsniveau, veelal alleen naam en wachtwoord, en het ontbreken van versleuteling.
- Voor Clouddiensten (bijvoorbeeld toepassingen in SaaS, O365) geldt dat versleuteling geregeld is op een manier die recht doet aan de beschermingseisen.
- Er is, door IT, een proces in gebruik welke zorgt voor een gedegen management van het beheer, vervangen, updaten, archiveren en verwijderen van encryptiesleutels en certificaten.
- Minimaal jaarlijks wordt er een scan gedaan binnen het netwerk om te kijken of er geen oude (niet veilige) encryptie en communicatieprotocollen worden gebruikt. De uitkomsten van deze scan worden gedeeld met de CISO.

## 10. Fysieke toegangsbeleid

Het doel van het fysieke toegangsbeleid is te voorkomen dat onbevoegden toegang krijgen tot ruimtes of systemen met informatie waar zij geen kennis van behoren te nemen danwel dat informatie kan worden aangepast.

### Beleidsregels en uitgangspunten

- Binnen Senzer zijn barrières aangebracht om ruimten te beschermen waar zich IT-voorzieningen dan wel persoonsgegevens en/ of gevoelige informatie bevinden.
- Er is een zoneringsplan met daarin opgenomen de volgende zones: Openbaar, wachtruimten en spreekkamers, werkruimten, IT-ruimte/beveiligde ruimte, fysieke archief en een off-site backup locatie.
- Toegang tot gebouwen of beveiligingszones is alleen mogelijk na autorisatie. Autorisatie wordt verleend conform de vastgestelde procedure.
- Voor toegang tot speciale ruimtes is doelbinding vereist (denk aan serverruimte en archief ruimten). Toegang tot deze ruimtes wordt middels logging vastgelegd en periodiek gecontroleerd door afdeling Services & Ondersteuning/ Facilitair.
- Er is cameratoezicht op toegangswegen en beveiligde ruimtes.
- Gebouwen bieden voldoende weerstand bij gewelddadige aanvallen zoals inbraak en vandalisme, hierbij wordt ook rekening gehouden met de omgeving.
- Er zijn alarmknoppen geplaatst in ruimtes waar bezoekers in contact komen met medewerkers van Senzer (zoals receptieruimtes, wachtruimtes, spreekkamers, enz).
- De kwaliteit van de toegangsmiddelen hoort in overeenstemming te zijn met de zonering.
- Gedurende sluitingstijden is er een inbraak alarm gekoppeld aan een alarmcentrale. Hierbij wordt gebruik gemaakt van enkel persoonlijke codes. Er wordt geen gebruik gemaakt van een generieke code.
- Medewerkers/ bezoekers zonder autorisatie mogen alleen onder begeleiding van bevoegd personeel en als er een noodzaak is, toegang krijgen tot de beveiligde omgeving.
- Zonder expliciete toestemming mogen in beveiligde ruimtes geen opnames (beeld en/of geluid) worden gemaakt.
- Toegangsmiddelen vallen onder de verantwoordelijkheid van Facilitaire Diensten.
- Niet uitgegeven toegangsmiddelen worden beveiligd opgeborgen.
- De huisregels voor toegangsbeleid worden bekend gesteld aan al het personeel en de bezoekers.
- Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, zijn beheerst en afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.
- Bij uitdiensttreding van een medewerker dient de uitdienstprocedure gevolgd te worden en alle toegangsmiddelen dienen onmiddellijk gedeactiveerd te worden én ingeleverd te worden om daarna, indien nodig, vernietigd te worden.

# 11. Logging beleid

Logging houdt in dat er bijgehouden wordt wie, wat en wanneer doet met de systemen en gegevens. Dit is nodig om de veiligheid, integriteit en beschikbaarheid van onze informatie te waarborgen. Met dit beleid lossen we een aantal problemen op, zoals het voorkomen en detecteren van ongeautoriseerde toegang en het aantonen van naleving van wet- en regelgeving.

## Beleidsregels en uitgangspunten

- Een logregel bevat minimaal (afhankelijk van de mogelijkheden):
  - Een tot een natuurlijk persoon herleidbare gebruikersnaam of ID
  - De gebeurtenis
  - Waar mogelijk de identiteit van het werkstation of de locatie:
  - Host naam
  - Operating System (OS)
  - Naam van de toepassing
  - IP-adres(sen)
  - Locatie(s)
  - Het object waarop de handeling werd uitgevoerd
  - Het resultaat van de handeling
  - De datum en het tijdstip van de gebeurtenis
- In een logregel worden in geen geval gevoelige gegevens opgenomen.
- Alle ongeautoriseerde toegangspogingen zijn beveiligingsincidenten en vereisen directe opvolging via het beveiligingsincidenten proces.
- De volgende gebeurtenissen dienen gelogd te worden:
  - Gebruik van technische beheerfuncties
  - Gebruik van functionele beheerfuncties
  - Handelingen van beveiligingsbeheer
  - Beveiligingsincidenten
  - Verstoringen in het productieproces
  - Handelingen van gebruikers
  - Online transacties
- Naast het reguliere loggen wat door systemen en netwerken zelf wordt verzorgd, dienen de activiteiten van beheerders op uitgebreidere wijze gelogd te worden.
- Logbestanden dienen te worden beschermd tegen modificatie, inzien door onbevoegden en verwijdering. De volgende beleidsregels zijn hierop van toepassing:
  - Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk, integriteit en onbevoegde toegang.
  - Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in de nieuw aangelegde log.
  - Het raadplegen van logbestanden is enkel voorbehouden aan geautoriseerde gebruikers. Hierbij is de toegang beperkt tot leesrechten.
  - Logbestanden worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.
  - De instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden zal daarbij altijd het 'vier ogen'-principe toegepast worden. Dit wordt ook geregistreerd en op verzoek ter beschikking gesteld.

- De beschikbaarheid van loginformatie is gewaarborgd binnen de termijn waarin loganalyse noodzakelijk wordt geacht, met een minimum van drie maanden, conform de wensen van de systeemeigenaar. Bij een (vermoedelijk) informatiebeveiligingsincident is de bewaartermijn minimaal drie jaar.
- Het goed functioneren van de logging wordt continu gemonitord voor essentiële systemen.
- Controle op opslag van de logs: het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijvoorbeeld: een logserver die niet bereikbaar is). Bij elke dienst, proces of systeem moet worden bekeken of logging moet worden ingesteld en met welk doel.
- Voor de bewaartermijn wordt gekeken naar de integriteit en de vertrouwelijkheid van informatie (zie hiervoor het classificatiebeleid)

#### Integriteit

Niveau	Monitoring
Niet zeker	Geen
Beschermd	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of -service. Monitoring-gegevens bewaren voor periode van een half jaar.
Hoog	<b>Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of -service. Monitoring-gegevens bewaren voor periode van maximaal twee jaar of langer bij een vermoed beveiligingsincident.</b>
Absoluut	Vastleggen authenticatie (correct en foutief) en tijdstip. Vastleggen relevante input en output van een IT-systeem of -service. Monitoring-gegevens bewaren voor periode van minimaal drie jaar bij een vermeend beveiligingsincident. Vastleggen oude staat van te wijzigen gegevens.

#### Vertrouwelijkheid

Niveau	Monitoring
Openbaar	Geen
Bedrijfs-vertrouwelijk	Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van een half jaar.
Vertrouwelijk	<b>Vastleggen herhaaldelijk foutieve authenticatie en tijdstip. Monitoring-gegevens bewaren voor periode van twee jaar.</b>
Geheim	Zijn in aanvulling op de BIO beschikbaar als BBN2+, gerelateerd aan BIO BBN3.

- De klokken van alle relevante informatiesystemen van Senzer behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron. Bovenstaande beleidsregels en uitgangspunten gelden op alle systemen en services van Senzer, zowel intern als in de cloud.

## 12. Veilig Personeelsbeleid

Dit personeelsbeleid heeft als doel dat alle medewerkers zich bewust zijn van hun rol en verantwoordelijkheid in het beschermen van onze informatie. Dit beleid geeft richtlijnen en regels voor het veilig omgaan met informatie in alle fasen van de informatielevenscyclus, van creatie tot vernietiging. Het doel van dit beleid is om het risico op informatieverlies, -diefstal, -misbruik of -beschadiging te verminderen en om de continuïteit en reputatie van Senzer te waarborgen.

### Beleidsregels en uitgangspunten

Binnen het personeelsbeleid worden er verschillende fasen onderscheiden. Bij elke fase zijn de beleidsregels en uitgangspunten uitgewerkt.

- Voorafgaand aan het dienstverband
  - De kandidaat dient te worden gescreend op uitvoering van de functie binnen Senzer. Afhankelijk van de inhoud van de werkzaamheden kan de zwaarte van deze screening worden aangepast. Onder de screening wordt onder andere verstaan: het nakijken van de identificatie van de kandidaat, het valideren van CV (diploma's, certificaten, etc), het nagaan van referenties, het overleggen van een VOG, etc.  
[14 - VOG Beleid compleet.pdf \(sharepoint.com\)](#)
- Aanvang dienstverband
  - De nieuwe collega dient op de hoogte gebracht te worden van de huisregels, het beleid en de procedures omtrent informatiebeveiliging binnen Senzer.
  - Binnen drie maanden na de start van het dienstverband dient de e-learning informatieveiligheid succesvol te zijn doorlopen. Hierop wordt maandelijks op gerapporteerd. Dit rapport is indien nodig op te vragen door de CISO.
- Tijdens het dienstverband
  - Regelmatig worden activiteiten uitgevoerd die het beveiligingsbewustzijn bevorderen en op peil houden. Dit kan zijn door een training, artikelen op het intranet of dmv een bewustwordingscampagne. De CISO is hiervoor verantwoordelijk.
  - Er dienen beveiligingsopleidingen beschikbaar te zijn die aansluiten op de rol, kennis en verantwoordelijkheid van de medewerker.
  - Bij nieuwe versies van programmatuur of apparatuur dient de functioneel beheerder te beoordelen of aanvullende training op het gebied van informatiebeveiliging aan de medewerkers noodzakelijk is. Dit dient een onderdeel te zijn van de acceptatieprocedure
- Beëindiging of wijziging van dienstverband
  - Bij uitdiensttreding of functiewijziging van een medewerker zal door de leidinggevende moeten worden nagegaan of de rechten van toegang tot gebouw, apparatuur en informatie op de juiste wijze zijn ingetrokken of gewijzigd.
  - De vertrekkende medewerker zal bij uitdiensttreding moeten worden gewezen op eventuele resterende verplichtingen op het gebied van informatiebeveiliging, zoals een blijvende verplichting tot geheimhouding.
  - Er is een uit-dienst-procedure opgesteld waarbij zorg gedragen wordt dat rechten ingetrokken worden (zowel op systemen/ applicaties als de toegangspas, Senzer eigendommen weer worden ingeleverd (Bijvoorbeeld, laptop, telefoon, toegangspas, sleutels en bedrijfskleding)

- Er wordt een overzicht bijgehouden van de medewerkers die uit dienst zijn gegaan, met daarbij een overzicht van de stappen die zijn gezet. Hiervoor kan een checklist gebruikt worden. De CISO heeft inzicht in deze rapportage.
- Er is een formele en gecommuniceerde disciplinaire procedure actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.
- Elke gebruiker, zowel individueel als binnen de organisatie, is verantwoordelijk voor het verstandig en verantwoord gebruik van computer- en netwerkbronnen.

## 13. Privacy beleid

Senzer werkt met persoonsgegevens van burgers, medewerkers en (keten)partners om wettelijke taken goed uit te voeren. Iedereen moet erop kunnen vertrouwen dat Senzer zorgvuldig en veilig met persoonsgegevens omgaat. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid introduceren steeds nieuwe risico's als het gaat om bescherming van gegevens en privacy. Senzer is zich hier van bewust en zorgt dat de privacy geborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

### Beleidsregels en uitgangspunten

- Senzer is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Hiervoor gelden onder andere de volgende wettelijke kaders:
  - Algemene Verordening Gegevensbescherming (AVG);
  - Uitvoeringswet Algemene Verordening Gegevensbescherming.
- Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.
- Senzer zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt. Persoonsgegevens worden alleen met een rechtvaardige grondslag verwerkt.
- Alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel worden verwerkt. Er wordt streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
- Persoonsgegevens worden niet langer bewaard dan nodig is. Het bewaren van persoonsgegevens kan nodig zijn om de (gemeentelijke) taken goed uit te kunnen oefenen of om wettelijke verplichtingen te kunnen naleven. Voor het bepalen van bewaartermijnen wordt altijd een DIV-adviseur geraadpleegd en vormt de vigerende Selectielijst de grondslag. Overleg tussen FG en DIV kan daarbij nodig zijn.
- Persoonsgegevens worden alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld. Daarbij wordt er gezorgd voor passende beveiliging van persoonsgegevens.
- In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, worden afspraken gemaakt over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. Deze afspraken worden jaarlijks gecontroleerd. Een verslag van deze controle wordt gedeeld met de CISO en FG.
- Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt.
- De inbreuk op de belangen van de betrokkene mag niet onevenredig zijn in verhouding tot het te dienen doel van de verwerking.
- Alle rechten van betrokkenen worden gehonoreerd.

## 14. Hybride werken beleid

De laatste jaren heeft, vooral door de coronapandemie, het telewerken (ook wel thuiswerken genoemd) een enorme ontwikkeling gekend. Er is in meerdere mate overgegaan naar cloud gebaseerd werken. Hierdoor is het plaats-, apparaat- en tijdonafhankelijk werken een norm geworden en ook een ambitie en focus vanuit ons organisatieplan. Het onderscheid tussen op kantoor en thuis werken wordt daardoor ook drastisch verminderd.

### Beleidsregels en uitgangspunten

- Medewerkers worden bewust gemaakt van de thuiswerkregels omtrent informatieveiligheid.
- Alle beschreven beleidsregels en uitgangspunten gelden ook voor het werken op afstand, hierbij geldt met name het "Clear desk en clear screen" en het "Cryptografie" beleid.
- Medewerkers van Senzer moeten altijd werken met de apparatuur die door Senzer is geleverd, zoals laptops, tablets of smartphones. Als het niet mogelijk is om met de Senzer-apparatuur te werken, bijvoorbeeld door een storing, een noodsituatie of een andere omstandigheid, mogen medewerkers gebruik maken van hun eigen privé-apparatuur.
- Senzer is bevoegd om beveiligingsinstellingen af te dwingen. Dit heeft betrekking op zowel door Senzer verstrekte apparatuur, als privé-apparatuur wanneer deze wordt ingezet om toegang te verkrijgen tot de data en netwerken van Senzer.
- Medewerkers moeten zich registreren en akkoord gaan met de beleidsregels en gedragsregels die Senzer heeft vastgesteld.
- Medewerkers zijn zelf verantwoordelijk voor het veilig opstellen van een veilige netwerkverbinding. Denk hierbij aan een veilig thuisnetwerk.
- Senzer is bevoegd om te bepalen welke applicaties en netwerken toegestaan zijn op de mobiele apparaten, zowel Senzer verstrekte apparatuur, als privé-apparatuur en hoe deze applicaties toegang krijgen tot de data en netwerken van Senzer.
- Senzer is bevoegd om het mobiele apparaat, zowel Senzer verstrekte apparatuur, als privé-apparatuur wanneer deze wordt ingezet om toegang te verkrijgen tot de data en netwerken van Senzer (selectief) te wissen.
- De mobiele apparaten zijn voorzien van een sterk wachtwoord of een andere vorm van authenticatie, zoals een pincode, vingerafdruk of gezichtsherkenning. Het wachtwoord of de pincode moet regelmatig veranderd worden.
- De mobiele apparaten moeten versleuteld zijn, zodat de gegevens niet leesbaar zijn als het apparaat kwijt of gestolen wordt. De versleuteling moet ook gelden voor de gegevens die via het mobiele apparaat worden verzonden of ontvangen.
- De mobiele apparaten moeten voorzien zijn van de laatste beveiligingsupdates en patches.
- De mobiele apparaten mogen niet geroot of gejaillbreakt zijn, omdat dit de beveiliging en de werking van de technische beveiliging van Senzer kan omzeilen. Toegang tot data en netwerken van Senzer wordt bij een dergelijke detectie per direct ontzegt vanaf het betreffende mobiele apparaat.
- De mobiele apparaten moeten in geval van verlies, diefstal, defect of einde dienstverband zo snel mogelijk gemeld worden bij de afdeling IT.

## 15. Cloud beveiliging beleid

Tegenwoordig is het normaal om te werken 'in de cloud'. Dit brengt een hoop voordelen met zich mee. Helaas kleven er ook risico's aan het werken in de cloud. Daarom is het van belang om mogelijke risico's vooraf goed in kaart te brengen.

### Beleidsregels en uitgangspunten

- Alle eisen die in het informatiebeveiligingsbeleid worden benoemd gelden ook voor de cloud. Denk vooral aan het gebruik van MFA, backups, toegangscontrole, updates, enz
- Opslag in de cloud gebeurt uitsluitend in datacenters gevestigd in Europa, daar waar persoonsgegevens verwerkt worden.
- Toegang tot de diensten in de cloud worden gebaseerd op het principe van de minste privileges.
- Alle gegevens (zowel 'in transit' als 'in rest') worden versleuteld op een manier passend bij de gevoeligheid van de gegevens en conform de industrie best-practices.
- Alle cloudomgevingen worden gescheiden van andere klanten van de cloudproviders/ datacenters.
- Er mag alleen gebruik gemaakt worden van cloud leveranciers waar van tevoren een gedegen risico analyse is uitgevoerd (zie [leveranciersbeleid](#))

## 16. Leveranciersbeleid

Om een goed beeld te hebben en te houden op onze leveranciers en te toetsen op de naleving van ons beleid, is het noodzakelijk om ook beleid op te stellen op leveranciers.

### Beleidsregels en uitgangspunten

- Voorafgaand aan het afsluiten van een contract is er een risico analyse gedaan en zijn er afspraken gemaakt omtrent informatieveiligheid. In geval van verwerking van persoonsgegevens dient er een verwerkersovereenkomst opgesteld te zijn. Een DPIA kan onderdeel zijn van het voortraject.
- Voorafgaand aan het afsluiten van een contract zijn er afspraken vastgelegd omtrent de inkoop-eisen ten aanzien van informatiebeveiliging. (zie bijlage 2)
- Voorafgaand aan het afsluiten van een contract dient er een exit-strategie opgesteld te worden.
- Leverancier dient zich minimaal te houden aan de overeengekomen BIO-kaders én het beleid van Senzer en kan dit aantonen.
- In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.
- Door het aangaan van een contract met Senzer zegt de leverancier toe dat er mogelijk een terugkerende externe audit plaatsvindt waarmee leverancier aantoont dat hij voldoet aan de overeengekomen kaders waaraan de dienstverlening moet voldoen. Een audit is niet nodig wanneer leverancier door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.
- Minimaal jaarlijks wordt de leverancier gemonitord, beoordeeld en indien nodig geaudit op de afgesproken prestatie-indicatoren. Wanneer blijkt dat leverancier niet voldoet, wordt dit met leverancier besproken en een plan opgesteld. Wanneer het daaropvolgende jaar nog geen verbetering is opgetreden, dient er op zoek te worden gegaan naar een andere leverancier. Van deze monitoring en de uitkomst hiervan wordt een verslag gemaakt welke gedeeld wordt met de CISO.
- Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.
- Incidenten omtrent de dienstverlening of de informatiebeveiliging van Senzer gegevens worden altijd doorgegeven aan Senzer.
- De leverancier houdt de dienst gescheiden van andere klanten.
- Indien de leverancier gegevens van Senzer opslaat voor verwerking, dient dit te gebeuren binnen de EU.
- Wanneer leveranciers op het moment van verschijnen van dit beleid nog niet voldoen aan dit beleid, geldt er een periode van 4 jaar om alsnog aan dit beleid te voldoen. Dit kan betekenen dat er nieuwe contracten afgesloten moeten worden.

## 17. Netwerkbeleid

Het is van belang om in het gebruik en de inrichting van het netwerk een aantal beleidsregels en uitgangspunten op te stellen om op een veilige manier van het netwerk gebruik te kunnen (blijven) maken.

### Beleidsregels en uitgangspunten

- Toegang tot het netwerk van Senzer wordt beperkt tot geautoriseerde gebruikers en apparaten. Indien externen gebruik willen maken van de wifi dient hier een apart netwerk voor ter beschikking gesteld te worden, zodat dit verkeer niet via het netwerk van Senzer verloopt.
- Gebruikers mogen geen handelingen verrichten die de functionaliteit en werking van het Senzer netwerk uitbreidt of aanpast. Denk hierbij aan het aansluiten van apparatuur zoals een router of switch, het installeren van software om een (draadloos)netwerk te verzenden, enz.
- Gebruikers mogen geen beveiligingsprogramma's of hulpprogramma's downloaden, installeren of uitvoeren die zwakke punten in de beveiliging van een systeem onthullen. Er mogen bijvoorbeeld geen wachtwoordkrakende programma's, packet sniffers, netwerkscanners of poortscanners gedraaid worden terwijl ze op enigerlei wijze zijn verbonden met de Senzer netwerkinfrastructuur. Alleen de afdeling IT is gemachtigd om deze acties uit te voeren.
- Het opnieuw configureren van apparatuur van een thuisgebruiker voor split-tunneling of dual homing is te allen tijde niet toegestaan.
- Alle hosts die zijn verbonden met de interne netwerken van Senzer via externe toegangstechnologieën, moeten gebruikmaken van up-to-date antivirussoftware die van toepassing is op dat apparaat of platform. Het netwerk wordt opgedeeld in segmenten. Per segment worden beveiligingsinstellingen doorgevoerd, passend bij de aanwezig systemen en informatie van dat segment. Toegang tot netwerksegmenten moet worden beperkt tot geautoriseerde gebruikers en apparaten. Dit omvat het gebruik van firewallregels, toegangscontroles en authenticatiemechanismen.
- Senzer maakt gebruik van een SIEM/SOC-oplossing om de veiligheid van het netwerk en onze systemen en informatie te waarborgen. De SIEM/SOC-oplossing verzamelt en analyseert loggegevens van onze systemen en netwerken om verdachte activiteiten te detecteren en te alarmeren. In geval van een beveiligingsincident zal de SOC snel reageren conform het geldende incident-response proces om het incident te beperken, te onderzoeken en op te lossen. Senzer zorgt ervoor dat de SIEM/SOC-oplossing up-to-date is en regelmatig wordt geëvalueerd om de effectiviteit te waarborgen.
- Om de vertrouwelijkheid, integriteit en authenticiteit van informatie die over het netwerk wordt verzonden te waarborgen, is het van cruciaal belang dat alle gevoelige gegevens worden versleuteld tijdens de verzending. Dit wordt bereikt door het toepassen van robuuste cryptografische technieken, zoals beschreven in ons cryptografiebeleid. Het ontsleutelen van informatie mag alleen worden uitgevoerd door geautoriseerde partijen met de juiste sleutels en toestemmingen.

## 18. Wachtwoord beleid

Wachtwoorden zorgen ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot informatie van Senzer. Een gemakkelijk wachtwoord evenals onduidelijke of niet gevolgde wachtwoord procedures zijn een bedreiging voor de vertrouwelijkheid en integriteit van informatie van Senzer, maar uiteindelijk ook voor het imago van Senzer. Alle gebruikers van informatiesystemen dienen goede wachtwoorden te kiezen en zijn verantwoordelijk voor de geheimhouding van hun wachtwoorden en inloggegevens.

Het doel van dit wachtwoordbeleid is drieledig:

- Het vaststellen van regels waar wachtwoorden en wachtwoordprocedures aan moeten voldoen.
- Het vaststellen van de bescherming van de wachtwoorden.
- Het vaststellen van de wijzigingscriteria voor wachtwoorden.

### Beleidsregels en uitgangspunten

- Standaard wachtwoorden, die in systemen zitten, worden voor ingebruikname gewijzigd.
- Wachtwoorden worden altijd versleuteld bewaard of verstuurd.
- Bij nieuwe applicaties of dienstverlening is het gebruik van MFA verplicht.
- Als er, bij een reeds bestaand systeem of dienst, geen gebruik wordt gemaakt van twee-factor authenticatie, is de wachtwoordlengte minimaal 14 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 7. Het account wordt daarna minimaal 15 minuten geblokkeerd. Indien er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker een verzoek indient deze lock-out op te heffen of het wachtwoord te resetten volgens de geldende procedure.
- In situaties waar, bij een reeds bestaand systeem of dienst, geen twee-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd.
- De eisen aan wachtwoorden worden geautomatiseerd afgedwongen. Daar waar dit voor bestaande applicaties nog niet geldt, wordt dit wel zo spoedig mogelijk ingericht.
- Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.
- Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.
- Wachtwoorden worden op een veilige manier uitgegeven (controle identiteit van de gebruiker).
- Er kunnen uitzonderingen bestaan bij de lengte en complexiteit van wachtwoorden. Dit kan alleen na afstemming en goedkeuring van de CISO.
- Gebruikers bevestigen de ontvangst van een wachtwoord.
- Wachtwoorden zijn alleen bij de gebruiker bekend en worden niet opgeschreven.
- Wachtwoorden worden bij voorkeur opgeslagen in een digitale wachtwoordenkluis.
- Gebruikers delen hun wachtwoord nooit met anderen.
- Wachtwoorden mogen niet opeenvolgend zijn.
- Een wachtwoord wordt onmiddellijk gewijzigd indien het vermoeden bestaat dat het bekend is geworden aan een derde.
- Wachtwoorden worden niet gebruikt in automatische inlogprocedures (bijvoorbeeld opgeslagen onder een functietoets of in een macro).

- Misbruik van wachtwoorden dient als beveiligingsincident gemeld te worden aan de IT-servicedesk.
- Nadat voor een gebruikersnaam 7 keer een foutief wachtwoord gegeven is, wordt het account minimaal 15 minuten geblokkeerd.
- Minimaal eens per 6 jaar wordt gecontroleerd of de toegangsrechten van medewerkers nog juist zijn. Dit wordt uitgevoerd door de systeemeigenaar van het informatiesysteem. De controle en afwijkingen dienen te worden gerapporteerd aan de verantwoordelijke proceseigenaar en eindverantwoordelijke, zodat maatregelen kunnen worden genomen om fouten te herstellen. Voor beheerdersaccounts gelden aanvullende beleidsregels en uitgangspunten:
- Toegang tot een beheerdersaccount wordt alleen verleend op basis van twee-factor authenticatie.
- Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven. Er wordt geen informatie getoond die herleidbaar is tot de authenticatiegegevens.
- Voorafgaand aan het aanmelden van een kritische applicatie wordt aan de gebruiker een melding getoond dat alleen geautoriseerd gebruik is toegestaan voor expliciet door de organisatie vastgestelde doeleinden.
- Bij een succesvol loginproces van een kritische applicatie wordt de datum en tijd van de voorgaande login of loginpoging getoond. Deze informatie kan de gebruiker enige informatie verschaffen over de authenticiteit en/of misbruik van het systeem.
- Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.
  - Er wordt automatisch gecontroleerd op goed gebruik van wachtwoorden (onder andere voldoende sterke wachtwoorden, regelmatige wijziging, directe wijziging van initieel wachtwoord).
  - Wachtwoorden hebben een geldigheidsduur zoals beschreven in maatregel 9.4.3.5 van de BIO. Binnen deze tijd dient het wachtwoord te worden gewijzigd. Wanneer het wachtwoord verlopen is, wordt het account geblokkeerd en een wijziging afgedwongen.

## 19. Update en patch beleid

Veel computerbesturingssystemen, zoals Microsoft Windows, Linux en andere, bevatten softwaretoepassingsprogramma's die beveiligingsfouten kunnen bevatten. Af en toe maakt een van die fouten het mogelijk dat een hacker een computer kan compromitteren. Een gecompromitteerde computer vormt een bedreiging voor de integriteit van Senzer en alle computers die ermee zijn verbonden. Bijna alle besturingssystemen en veel softwaretoepassingen hebben periodieke beveiligingspatches die door de leverancier worden uitgebracht en moeten worden toegepast.

### Beleidsregels en uitgangspunten

- Patches, die betrekking hebben op beveiliging of van kritiek belang zijn, moeten zo snel mogelijk worden geïnstalleerd. In het geval dat een kritieke of beveiligingsgerelateerde patch niet centraal kan worden ingezet door IT, moet deze tijdig worden geïnstalleerd met behulp van de beste beschikbare middelen. Kritieke patches dienen binnen 48 uur geïnstalleerd te zijn.
- Het niet correct configureren van nieuwe werkstations is in strijd met dit beleid. Het uitschakelen, omzeilen of knoeien met patchbeheerbeveiligingen en/of software vormt een schending van het beleid en is daarom niet toegestaan.
- Alle systemen en applicaties die in bedrijf zijn binnen Senzer zijn bijgewerkt naar de meest recente versie. Omwille van de veiligheid en om te voorkomen dat er ongemerkt fouten in de patches zitten wordt het principe N-1 ook toegestaan. De afdeling IT maakt hierin zelf de afweging. Waar nodig kan de CISO geconsulteerd worden.
- Er wordt minimaal elk half jaar een scan gedaan door IT om te kijken of alle applicaties en besturingssystemen nog voldoen aan minimaal N-1. De uitslag van de scan wordt gedeeld met de CISO.
- IT is verantwoordelijk voor het zorgen dat alle bekende en redelijke verdedigingen aanwezig zijn om netwerk kwetsbaarheden te verminderen, terwijl het netwerk blijft functioneren.
- IT-management en beheerders zijn verantwoordelijk voor het monitoren van beveiligingsmailinglijsten, het bekijken van meldingen van leveranciers en websites, en het onderzoeken van specifieke openbare websites voor de release van nieuwe patches. Het monitoren omvat onder andere:
  - Geplande scans van derden van het netwerk van Senzer om bekende kwetsbaarheden te identificeren.
  - Identificeren van geïdentificeerde kwetsbaarheden en/of beveiligingsinbreuken.
  - Monitoren van Computer Emergency Readiness Team (CERT)-meldingen en websites van alle leveranciers die hardware of software op het netwerk van Senzer hebben.Bovenstaande wordt vastgelegd in TOPdesk.
- Er zijn patchprocedures opgesteld waarin wordt beschreven wat, waar, wanneer en hoe moet worden gedaan om verwarring te voorkomen, routine vast te stellen, begeleiding te bieden en praktijken controleerbaar te maken. Deze procedures worden minimaal jaarlijks nagekeken op werking en waar nodig aangepast.
- Zodra een nieuwe patch wordt gemeld, zal de afdeling IT de patch downloaden en beoordelen. De patch wordt gecategoriseerd op basis van kritikaliteit om de impact te beoordelen en het installatieschema te bepalen.

## 20. Gebruikersaccount beleid

### Beleidsregels en uitgangspunten

- Alle aangemaakte accounts moeten vergezeld gaan van een schriftelijk verzoek vanuit de leidinggevende van de medewerker
- Alle accounts moeten uniek identificeerbaar zijn aan de hand van de toegewezen gebruikersnaam.
- Gedeelde accounts of groepsaccounts zijn niet toegestaan.
- Alle accounts moeten voldoen aan het wachtwoordbeleid.
- Alle accounts moeten onmiddellijk worden uitgeschakeld de dag na de laatste werkdag van de werknemer.
- Iedereen die in het bezit is van een Senzer account mag hun inloggegevens nooit aan iemand doorgeven, inclusief familieleden.
- Gebruik geen e-mailaccounts van derden (zoals Hotmail, Gmail, enz) of andere externe bronnen voor Senzer-zaken, om ervoor te zorgen dat officiële bedrijfsactiviteiten nooit worden verward met persoonlijke activiteiten.
- Rechten op accounts worden uitgedeeld volgens het least privilege concept.
- Teamleiders en managers controleren elk half jaar de accounts van de medewerkers. Deze controle wordt ter beschikking gesteld voor de CISO.

De volgende punten zijn van toepassing op systeembeheerders of aangewezen personeel:

- Gebruikersaccounts van informatiesystemen moeten zodanig worden opgebouwd dat ze de meest beperkende reeks rechten/privileges of toegangen afdwingen die nodig zijn voor de uitvoering van taken die verband houden met het account van een individu. Bovendien moeten accounts zo worden aangemaakt dat geen enkele gebruiker toestemming kan geven, uitvoeren, beoordelen en controleren voor een enkele transactie om belangenconflicten te voorkomen.
- Alle gebruikersaccounts van informatiesystemen worden actief beheerd. Actief beheer omvat het instellen, activeren, wijzigen, uitschakelen en verwijderen van accounts uit informatiesystemen.
- Toegangscontroles worden bepaald door de vastgestelde procedures te volgen voor nieuwe medewerkers, wijzigingen in medewerkers, beëindiging van medewerkers en verlof. Deze controles worden overlegd met de CISO.
- Alle accountwijzigingen moeten een gedocumenteerd proces hebben om een gebruikersaccount aan te passen aan situaties zoals naamswijzigingen en toestemmingswijzigingen.
- Gebruikersaccounts van informatiesystemen worden maandelijks beoordeeld om inactieve accounts te identificeren. Als een gebruikersaccount gedurende 120 dagen inactief blijft, worden de eigenaren (van het account) en hun leidinggevende op de hoogte gesteld van de aanstaande uitschakeling. Als het account daarna nog steeds 60 dagen inactief blijft, wordt het account handmatig uitgeschakeld of verwijderd.
- Minimaal elke half jaar wordt een lijst van accounts met de systemen die zij beheren verstrekt aan de CISO.
- Er kan een onafhankelijke auditcontrole worden uitgevoerd om ervoor te zorgen dat de accounts correct worden beheerd.

## 21. Externe communicatiebeleid

Binnen Senzer streven we ernaar om een veilige, betrouwbare en gebruiksvriendelijke online omgeving te bieden. Ons externe communicatiebeleid is ontworpen om zowel de integriteit van onze digitale aanwezigheid te waarborgen als om onze klanten duidelijkheid en vertrouwen te bieden. Door strikte naleving van dit beleid, dekken we essentiële risico's af zoals datalekken, ongeautoriseerde toegang en de verspreiding van malware. Bovendien, eenduidigheid wat betreft huisstijl, schrijfstijl en extensiegebruik, die zorgen dat de klant ziet dat het echt van Senzer is. Dit beleid is een belofte aan onze klanten dat de veiligheid van persoonsgegevens een van onze hoogste prioriteit heeft en dat misbruik van onze systemen actief wordt tegengegaan.

### Beleidsregels en uitgangspunten.

- Wanneer het voornemen er is om een nieuwe website te plaatsen, dient dit met het webexpertteam besproken te worden.
- Wanneer de website gehost wordt, zijn er duidelijk afspraken gemaakt met de hostingpartij omtrent de CVD procedure. Bijvoorbeeld: Na het melden van een melding, dient er binnen 3 werkdagen op een melding met een (eerste) beoordeling van de melding gereageerd met een eventuele verwachte datum voor een oplossing.
- Het gebruik van HTTPS is verplicht. Indien hiervan afgeweken wordt dient overleg met de CISO plaats te vinden.
- Er wordt binnen de externe communicatie voldaan aan het informatiebeveiligingsbeleid. Met name het cryptografiebeleid, leveranciersbeleid en het privacybeleid zijn hierin belangrijk.
- Nieuwe websites worden zo ingericht dat ze de disclaimers gepubliceerd op [www.senzer.nl](http://www.senzer.nl), niet schenden. (te weten [het privacybeleid](#), [de proclaimer](#), [de toegankelijkheid](#) en [de algemene voorwaarden](#))
- Het webexpertteam is verantwoordelijk voor de veiligheid van de website. Zij zetten, indien nodig, acties uit bij de leverancier om de veiligheid te verbeteren. Er kan bij de beoordeling gebruik worden gemaakt van de volgende scores:
  - Minimaal 85% op [internet.nl](http://internet.nl)
  - Minimaal een B op [SSL Labs](#)
  - Minimaal een B op [Mozilla Observatory](#)
- Aanbevolen wordt om minimaals jaarlijks de websites op bovenstaande scores te scannen, aangezien de scores in de toekomst kunnen veranderen door toekomstige ontwikkelingen.

## Bijlage 1: BIO verantwoording

Hoofdstuk	Norm	Beschrijving
5. Antivirus beleid	12.2.1	Beheersmaatregelen tegen malware Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.
6. Backup- en restore beleid	12.3.1	Back-up van informatie Regelmatig behoren back-upkopieën van informatie, software en systeemaafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
6. Backup- en restore beleid	12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.
6. Backup- en restore beleid	12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.
6. Backup- en restore beleid	12.3.1.3	In het back-up beleid staan minimaal de volgende eisen: 1. dataverlies bedraagt maximaal 28 uur; 2. hersteltijd in geval van incidenten is maximaal 16 werkuren (2 dagen van 8 uur) in 85% van de gevallen.
6. Backup- en restore beleid	12.3.1.4	Het back-up proces voorziet in opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.
6. Backup- en restore beleid	12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.
7. Classificatiebeleid	9.1.1	Beleid voor toegangsbeveiliging: Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
7. Classificatiebeleid	9.1.2	Toegang tot netwerken en netwerkdiensten: Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
7. Classificatiebeleid	9.1.2.1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.
7. Classificatiebeleid	9.1.2.2	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.
7. Classificatiebeleid	9.2.1	Registratie en afmelden van gebruikers: Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
7. Classificatiebeleid	9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.
7. Classificatiebeleid	9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.

7. Classificatiebeleid	9.2.2	Gebruikers toegang verlenen: Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.
7. Classificatiebeleid	9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.
7. Classificatiebeleid	9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.
7. Classificatiebeleid	9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.
7. Classificatiebeleid	9.2.3	Beheren van speciale toegangsrechten: Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
7. Classificatiebeleid	9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.
7. Classificatiebeleid	9.2.4	Beheer van geheime authenticatie-informatie van gebruikers: Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.
7. Classificatiebeleid	9.2.5	Beoordeling van toegangsrechten van gebruikers: Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
7. Classificatiebeleid	9.2.5.1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.
7. Classificatiebeleid	9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.
7. Classificatiebeleid	9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.
7. Classificatiebeleid	9.2.6	Toegangsrechten intrekken of aanpassen: De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
8. Clear desk en clear screen beleid	11.2.9	'Clear desk'- en 'clear screen'-beleid: Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatieverwerkende faciliteiten te worden ingesteld.
8. Clear desk en clear screen beleid	11.2.9.1	Een onbemende werkplek is altijd vergrendeld.
8. Clear desk en clear screen beleid	11.2.9.2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.
8. Clear desk en clear screen beleid	11.2.9.3	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.
8. Clear desk en clear screen beleid	11.2.9.4	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.

8. Clear desk en clear screen beleid	11.2.9.5	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.
9. Cryptografiebeleid	10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen: Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
9. Cryptografiebeleid	10.1.1.1	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.
9. Cryptografiebeleid	10.1.1.2	Cryptografische toepassingen voldoen aan passende standaarden.
9. Cryptografiebeleid	13.2.3	Elektronische berichten: Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.
9. Cryptografiebeleid	13.2.3.1	Voor de beveiliging van elektronische (e-mail)berichten gelden de vastgestelde open standaarden tegen phishing en afluisteren op de 'pas toe of leg uit'-lijst van het Forum. Voor beveiliging van websiteverkeer gelden de open standaarden tegen afluisteren op de 'pas toe of leg uit'-lijst van het Forum.
9. Cryptografiebeleid	13.2.3.2	Voor veilige berichtenuitwisseling met basisregistraties wordt, conform de 'pas toe of leg uit'-lijst van het Forum, gebruik gemaakt van de actuele versie van Digikoppeling.
9. Cryptografiebeleid	13.2.3.3	Maak gebruik van PKI-overheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenuen.
9. Cryptografiebeleid	13.2.3.4	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.
9. Cryptografiebeleid	14.1.3	Transacties van toepassingen beschermen: Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routing, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.
9. Cryptografiebeleid	18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen: Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.
9. Cryptografiebeleid	18.1.5.1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum.
9. Cryptografiebeleid	13.2.1	Beleid en procedures voor informatietransport: Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.

10. Fysieke toegangsbeleid	11.1.1	Fysieke beveiligingszone: Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatieverwerkende faciliteiten bevatten.
10. Fysieke toegangsbeleid	11.1.1.1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.
10. Fysieke toegangsbeleid	11.1.2	Fysieke toegangsbeveiliging: Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
10. Fysieke toegangsbeleid	11.1.3	Kantoren, ruimten en faciliteiten beveiligen: Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.
10. Fysieke toegangsbeleid	11.1.3.1	Sleutelbeheer is ingericht op basis van een sleutelplan.
10. Fysieke toegangsbeleid	11.1.4	Beschermen tegen bedreigingen van buitenaf: Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
10. Fysieke toegangsbeleid	11.1.4.1	De organisatie heeft geïnteriseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.
10. Fysieke toegangsbeleid	11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.
10. Fysieke toegangsbeleid	11.1.5	Werken in beveiligde gebieden: Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
10. Fysieke toegangsbeleid	11.1.6	Laad- en loslocatie: Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerd, en zo mogelijk te worden afgeschermd van informatieverwerkende faciliteiten om onbevoegde toegang te vermijden.
10. Fysieke toegangsbeleid	6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.
10. Fysieke toegangsbeleid	9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.
10. Fysieke toegangsbeleid	9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.
10. Fysieke toegangsbeleid	9.2.2.3	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.
10. Fysieke toegangsbeleid	9.2.3.1	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.
10. Fysieke toegangsbeleid	9.2.5.2	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.
10. Fysieke toegangsbeleid	9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.
11. Loggingbeleid	12.4.1	Gebeurtenissen registreren: Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.

11. Loggingbeleid	12.4.1.1	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.
11. Loggingbeleid	12.4.1.2	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
11. Loggingbeleid	12.4.1.3	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.
11. Loggingbeleid	12.4.1.5	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.
11. Loggingbeleid	12.4.2	Beschermen van informatie in logbestanden: Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
11. Loggingbeleid	12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.
11. Loggingbeleid	12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
11. Loggingbeleid	12.4.2.3	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.
11. Loggingbeleid	12.4.2.4	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.
11. Loggingbeleid	12.4.3	Logbestanden van beheerders en operators: Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
11. Loggingbeleid	12.4.4	Kloksynchronisatie: De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.
11. Loggingbeleid	16.1.7.1	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.
11. Loggingbeleid	9.4.4.2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.

12. Veilig personeelsbeleid	7.1.1	Screening: Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.
12. Veilig personeelsbeleid	7.2.1	Directieverantwoordelijkheden: De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.
12. Veilig personeelsbeleid	7.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging: Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.
12. Veilig personeelsbeleid	7.2.3	Disciplinaire procedure: Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.
12. Veilig personeelsbeleid	7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband: Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.
12. Veilig personeelsbeleid	8.1.4	Teruggeven van bedrijfsmiddelen: Alle medewerkers en externe gebruikers moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.
12. Veilig personeelsbeleid	9.2.6	Toegangsrechten intrekken of aanpassen: De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.
13. Privacybeleid	18.1.4	Privacy en bescherming van persoonsgegevens: Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.
13. Privacybeleid	18.1.4.1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.
13. Privacybeleid	18.1.4.2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.
14. Telewerken beleid	6.2.2	Telewerken: Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.
16. Leveranciersbeleid	15.1.1	Informatiebeveiligingsbeleid voor leveranciersrelaties: Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.

16. Leveranciersbeleid	15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.
16. Leveranciersbeleid	15.1.1.2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.
16. Leveranciersbeleid	15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
16. Leveranciersbeleid	15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten: Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.
16. Leveranciersbeleid	15.1.2.1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.
16. Leveranciersbeleid	15.1.2.2	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.
16. Leveranciersbeleid	15.1.2.3	In situaties waarin contractvoorwaarden worden opgelegd door leveranciers, is voorafgaand aan het tekenen van het contract met een risicoafweging helder gemaakt wat de consequenties hiervan zijn voor de organisatie. Expliciet is gemaakt welke consequenties geaccepteerd worden en welke gemitigeerd moeten zijn bij het aangaan van de overeenkomst.
16. Leveranciersbeleid	15.1.2.4	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.
16. Leveranciersbeleid	15.1.2.5	Voordat een contract wordt afgesloten, wordt in een risicoafweging bepaald of de afhankelijkheid van een leverancier beheersbaar is. Een vast onderdeel van het contract is een expliciete uitwerking van de exit-strategie.
16. Leveranciersbeleid	15.1.2.6	In inkoopcontracten wordt expliciet de mogelijkheid van een externe audit opgenomen waarmee de betrouwbaarheid van de geleverde dienst kan worden getoetst. Een audit is niet nodig als de contractant door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.
16. Leveranciersbeleid	15.1.3	Toeleveringsketen van informatie- en communicatietechnologie: Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleveringsketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.
16. Leveranciersbeleid	15.1.3.1	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.
16. Leveranciersbeleid	15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers: Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.
16. Leveranciersbeleid	15.2.1.1	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.

16. Leveranciersbeleid	15.2.2	Beheer van veranderingen in dienstverlening van leveranciers: Veranderingen in de dienstverlening van leveranciers, met inbegrip van handhaving en verbetering van bestaande beleidslijnen, procedures en beheersmaatregelen voor informatiebeveiliging, behoren te worden, beheerd, rekening houdend met de kritikaliteit van bedrijfsinformatie, betrokken systemen en processen en herbeoordeling van risico's.
16. Leveranciersbeleid	18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen: Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.
18. Wachtwoordbeleid	9.3.1	Geheime authenticatie-informatie gebruiken: Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.
18. Wachtwoordbeleid	9.3.1.1	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.
18. Wachtwoordbeleid	9.4.3	Systeem voor wachtwoordbeheer: Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
18. Wachtwoordbeleid	9.4.3.1	Als er geen gebruik wordt gemaakt van two-factor authenticatie, is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.
18. Wachtwoordbeleid	9.4.3.2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).
18. Wachtwoordbeleid	9.4.3.3	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.
18. Wachtwoordbeleid	9.4.3.4	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.
18. Wachtwoordbeleid	9.4.3.5	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.
19. Update en patch beleid	12.2.1.3	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.
20. Gebruikersaccount beleid	9.2.1.2	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.

# Bijlage 2: Inkoop-eisen ten aanzien van informatiebeveiliging

## Inleiding

In het huidige digitale tijdperk is de veiligheid van persoonsgegevens van cruciaal belang voor Senzer. Het stellen van duidelijke eisen aan onze leveranciers is een essentieel onderdeel van onze strategie om deze gegevens te beschermen. Door het hanteren van strikte inkoopcriteria, waarborgen we dat alleen leveranciers die voldoen aan onze hoge standaarden voor gegevensbeveiliging en privacy, deel uitmaken van onze toeleveringsketen. Dit is niet alleen een kwestie van naleving van regelgeving, maar ook een fundamentele bedrijfsverantwoordelijkheid die we serieus nemen. Onder anderen is het verzekeren van de integriteit en vertrouwelijkheid van persoonsgegevens een prioriteit die we delen met onze partners. Ook vanuit de toekomstige invoering van de BIO2.0 en de NIS2, waarin een groot onderdeel weggelegd wordt voor het leveranciers- / contractmanagement, is het belangrijk dat we hier oog voor hebben.

Onderstaande punten gelden voor alle leveranciers, ongeacht de grootte van leverancier.

## Inkoop-eisen

- Alle voorwaarden en eisen die gelden voor personeel van de leverancier zijn ook van toepassing op derden, die in opdracht van de leverancier diensten verrichten voor Senzer.
- Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.
- Leverancier zal het bestaan, de aard en de inhoud van de contract, evenals overige bedrijfsinformatie van Senzer geheimhouden en niets daaromtrent openbaar maken zonder schriftelijke toestemming van Senzer vooraf.
- De leverancier staat er voor in dat personeel van de leverancier, overige personeelsleden en derden de bepalingen betreffende gedrag, vertrouwelijkheid en bescherming van gegevens naleven.
- Medewerkers van de leverancier overleggen voor aanvang van de werkzaamheden bij Senzer een recente Verklaring Omtrent het Gedrag (VOG) indien zij inzage hebben tot gevoelige gegevens. De leverancier stemt voorafgaand aan de aanvraag de noodzaak, inhoud en aard hiervan af met Senzer.
- De leverancier accepteert de maatregelen uit de BIO, voor zover van toepassing verklaard door Senzer, en past deze toe op de geleverde producten en/of diensten.
- Incidenten omtrent de dienstverlening of de informatiebeveiliging van gegevens worden altijd doorgegeven aan Senzer en als dat wettelijk noodzakelijk is ook aan de Autoriteit Persoonsgegevens. Bij niet gemelde incidenten waar persoonsgegevens bij betrokken zijn, zal Senzer een ontvangen boete en ontstane schade verhalen op de leverancier. Wanneer een kwetsbaarheid is geconstateerd bij de leverancier, dan zorgt de leverancier er ook voor dat deze wordt opgelost.
- De leverancier houdt de dienst gescheiden van andere klanten.

- Indien de leverancier gegevens van Senzer opslaat voor verwerking, dient dit te gebeuren binnen de EU.
- Leveranciers kunnen aantonen dat er robuuste identificatie- en authenticatiemechanismen geïmplementeerd zijn om ongeautoriseerde toegang tot systemen en gegevens te voorkomen.
- Leveranciers moeten kunnen aantonen dat er strikte toegangscontroles zijn om alleen geautoriseerde gebruikers toegang te verlenen tot specifieke bronnen.
- Gevoelige gegevens worden versleuteld tijdens opslag en verzending. Deze eisen dienen minimaal hetzelfde te zijn als de eisen die Senzer stelt aan zijn gegevens. Hiervoor wordt gebruik gemaakt van het [forum standaardisatie](#) op basis van 'pas toe of leg uit'.
- Leveranciers kunnen aantonen dat er regelmatig beveiligingspatches uitgevoerd worden om bekende kwetsbaarheden te verhelpen.
- Leveranciers houden logs bij en kunnen verdachte activiteiten monitoren om snel te reageren op beveiligingsincidenten.
- Leveranciers moeten een incidentresponsplan hebben om adequaat te reageren op beveiligingsincidenten.
- Leveranciers implementeren fysieke toegangscontroles om apparatuur en faciliteiten te beschermen.
- Leveranciers gebruiken netwerksegmentatie en firewalls om het risico van ongeautoriseerde toegang te minimaliseren.
- Leveranciers kunnen aantonen dat ze voldoen aan de privacywetgeving en persoonsgegevens adequaat beschermen.
- Leveranciers hebben plannen om bedrijfscontinuïteit te waarborgen en snel te herstellen na een incident of ramp.
- Leveranciers moeten cloudservices, die betrekking hebben op de dienstverlening aan Senzer, beveiligen volgens de BIO-normen.
- Leveranciers kunnen aantonen dat ze strenge beveiligingsmaatregelen treffen voor externe toegang tot hun systemen.
- Leveranciers kunnen aantonen dat endpoints (zoals laptops en desktops) beveiligd zijn tegen malware en aanvallen.
- Leveranciers kunnen aantonen dat ze hun medewerkers regelmatig trainen in informatiebeveiliging en daarmee het bewustzijn vergroten.
- De leverancier levert verantwoordingsrapportages aan Senzer op over bovenstaande punten, wanneer Senzer hierom vraagt.
- De leverancier accepteert dat wanneer er persoonsgegevens worden verwerkt in systemen van de leverancier buiten Senzer, er een verwerkersovereenkomst wordt afgesloten als onderdeel van het contract. Tevens worden in het contract afspraken vastgelegd betreffende aansprakelijkheid en schade in geval van incidenten. De standaard verwerkersovereenkomst gemeenten van de IBD wordt gehanteerd (versie 2.5), mits persoonsgegevens worden opgeslagen bij een Europees datacenter. Dit laatste is een eis als het gaat om gegevens met een hoge vertrouwelijkheid (bv. BSN, bijzondere persoonsgegevens).

## Bijlage 3: Functieprofielen

### (Taak)profiel Chief Information Security Officer (CISO)

De CISO behoeft geen zelfstandige functie zijn, maar kan een rol zijn binnen een staande functie.

Positie binnen de huidige organisatie:

- Hiërarchische aansturing door CIO
- Vakinhoudelijk overleg vindt periodiek plaats met de CIO (tevens Concerncontroller en lid van het DT Senzer)

Samenvatting:

De CISO definieert het informatiebeveiligingsbeleid en organiseert en stuurt de informatiebeveiliging van de organisatie overeenkomstig de behoeften en de risicobereidheid van de organisatie. De CISO voert zijn werkzaamheden uit vanuit een onafhankelijke positie en kan daarbij, indien noodzakelijk, rechtstreeks schakelen met de directie en/of bestuur.

Taakinhoud:

- Opstellen van het informatiebeveiligingsbeleid en aanverwant beleid voor de organisatie.
- Opstellen van het jaarlijkse informatiebeveiligingsplan voor de organisatie.
- (ongevraagd en gevraagd) Adviseren en actief uitdragen van beleid op het gebied van informatiebeveiliging.
- Opstellen, in samenwerking met de FG en SO Suwinet, van het kwartaalverslag informatiebeveiliging ten behoeve van het DT Senzer.
- Organiseren van informatiebeveiliging en de daarvoor benodigde expertise met betrekking tot de gehele scope van informatiebeveiliging.
- Adviseren van de systeemeigenaren bij het opstellen van dataclassificaties, autorisatieprocedures en -matrixen.
- Zorgen voor afstemming tussen informatiebeveiliging met andere beveiligingsdomeinen, waaronder privacybescherming, fysieke beveiliging en continuïteitsmanagement.
- Opzetten van een informatiebeveiligingscalamiteitenorganisatie.
- Coördineren van de reactie op ernstige informatiebeveiligings- of IT-incidenten.
- Zorgen voor een projectportfolio voor informatiebeveiliging.
- Initiëren en coördineren van organisatiebrede informatiebeveiligingsactiviteiten en projecten.
- Zorgen voor organisatiebrede richtlijnen, standaarden, methoden en technieken voor informatiebeveiliging.
- Monitoren en borgen de kwaliteit van informatierisicoanalyses, beveiligingsontwerpen en oplossingen.
- Monitoren en borgen het naleven van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design.
- Monitoren en borgen informatiebeveiligingsbewustzijn binnen de organisatie.
- Monitoren van relevante risico's voor de organisatie.
- Borgen dat de organisatie voldoende voorbereid is op toekomstig informatiebeveiligingsrisico's en IT-beveiligingsrisico's.

- Geeft zwaarwegend advies, waar alleen met gegronde motivatie van kan worden afgeweken, waarbij de consequenties van afwijking op het juiste niveau worden aanvaard.
- Monitoren en borgen van de kwaliteit van informatiebeveiligingsassessments.
- Monitoren op basis van assessments, test, reviews en audits in hoeverre de organisatie compliant is met het informatiebeveiligingsbeleid en wet- en regelgeving.
- Informeren bestuur en management over de status van informatiebeveiliging en incidenten en presenteert verbetervoorstellen.

### **(Taak)profiel Functionaris Gegevensbescherming (FG)**

De FG heeft geen zelfstandige functie, maar kan een rol spelen binnen een staande functie.

Positie binnen de huidige organisatie:

- Hiërarchische aansturing door de algemeen directeur.
- Vakinhoudelijk overleg vindt periodiek plaats met de CISO en CIO (tevens Concerncontroller en lid van het DT Senzer).

Samenvatting:

De FG definieert het privacybeleid en organiseert en stuurt de beveiliging van persoonsgegevens van de organisatie overeenkomstig de Algemene Verordening Gegevensbescherming (AVG). De FG voert zijn werkzaamheden zelfstandig uit vanuit een onafhankelijke positie en kan daarbij, indien noodzakelijk, rechtstreeks schakelen met de directie en/of bestuur.

Taakinhoud:

- Opstellen van het privacybeleid, op basis van de AVG, en aanverwant beleid en reglementen voor de organisatie.
- Adviseren en actief uitdragen van beleid op het gebied van de beveiliging van persoonsgegevens.
- Opstellen, in samenwerking met de CISO en SO Suwinet, van het kwartaalverslag informatiebeveiliging ten behoeve van het DT Senzer.
- Adviseren van de systeemeigenaren bij het opstellen van privacy impact analyse.
- Organiseren van informatiebeveiliging en de daarvoor benodigde expertise met betrekking tot de beveiliging van persoonsgegevens.
- Bijhouden van een verwerkingsregister.
- Bijhouden van een register van datalekken bij en beslissen of een datalek wordt gemeld aan de Autoriteit Persoonsgegevens. Coördineren en adviseren bij de afwerking van een datalek.
- Adviseren bij het opstellen van een Verwerkersovereenkomst en het registreren daarvan.
- Initiëren en coördineren van organisatiebrede informatiebeveiligingsactiviteiten en - projecten met betrekking tot de beveiliging van persoonsgegevens.
- Monitoren en borgen informatiebeveiligingsbewustzijn m.b.t. persoonsgegevens binnen de organisatie.
- Onderhouden van interne en externe contacten op het terrein van informatiebeveiliging m.b.t. persoonsgegevens.

## (Taak)profiel Security Officer Suwinet (SO Suwinet)

De SO Suwinet hoeft geen zelfstandige functie zijn, maar kan een rol zijn binnen een staande functie.

Positie binnen de huidige organisatie:

- Hiërarchische aansturing door CISO.
- Vakinhoudelijk overleg vindt periodiek plaats met de CISO en CIO (tevens Concerncontroller en lid van het DT Senzer).

Samenvatting:

Vanuit Senzer is de SO Suwinet verantwoordelijk voor het opzetten en onderhouden van beleid en processen gericht op het veilige gebruik en de continuïteit van Suwinet-Inkijk en het voldoen aan interne en externe eisen op het gebied van Informatiebeveiliging Suwinet-Inkijk. De SO Suwinet voert zijn werkzaamheden zelfstandig uit vanuit een onafhankelijke positie en kan daarbij, indien noodzakelijk, rechtstreeks schakelen met de directie en/of bestuur.

Taakinhoud:

- Opstellen en beheren van beleid, standaarden en procedures op het gebied van informatiebeveiliging Suwinet, inclusief het volgen en signaleren van externe ontwikkelingen en interne ontwikkelingen gericht op Suwinet;
- Zorgdragen voor het opstellen en naleven van informatiebeveiliging ten behoeve van Suwinet.
- Adviseren en actief uitdragen van beleid op het gebied van informatiebeveiliging van Suwinet in de organisatie.
- Uitvoeren van risicoanalyses met betrekking tot informatiebeveiliging Suwinet binnen de organisatie.
- Opstellen van een jaarplanning met betrekking tot informatiebeveiliging Suwinet.
- Coördineren van activiteiten met betrekking tot informatiebeveiliging Suwinet.
- Adviseren van het hoogste management met betrekking tot informatiebeveiliging Suwinet.
- Uitvoeren van interne controles en coördineren van audits van ten behoeve van Suwinet.
- Rapporteren aan het hoogste management, onder andere over naleving van het informatiebeveiligingsbeleid, de voortgang van de implementatie van informatiebeveiligingsmaatregelen en over de uitkomsten van zelf te initiëren interne onderzoeken van Suwinet.
- Onderhouden van interne en externe contacten op het terrein van informatiebeveiliging Suwinet.
- Signaleren van afwijkingen op het informatiebeveiligingsbeleid aangaande Suwinet.

## Vaststellen beleid in het DT

Dit informatiebeveiligingsbeleid treedt in werking na vaststelling door de algemeen directeur van Senzer en vervangt het voormalig beleid. Het beleid wordt jaarlijks geëvalueerd en indien nodig herzien. De meest actuele versie van dit beleid is te vinden op [www.senzer.nl](http://www.senzer.nl).

Aldus vastgesteld door de algemeen directeur van Senzer te Helmond op

Marion van Limpt  
Algemeen Directeur Senzer

**Bezoekadres**  
Montgomeryplein 6  
5705 AX Helmond

t. 0492 58 24 44  
e. [info@senzer.nl](mailto:info@senzer.nl)  
[www.senzer.nl](http://www.senzer.nl)

