senzer

BLAD GEMEENSCHAPPELIJKE REGELING

Nr. 147
14 februari
2020

Officiële uitgave van de gemeenschappelijke regeling Werkbedrijf Atlant De Peel

Informatiebeveiligingsbeleid Senzer 2020-2022

Inhoud:
Het informatiebeveiligingsbeleid Senzer 2020 - 2022 is opgesteld aan de hand van de operationele Baseline Informatiebeveiliging Overheid (BIO) vervaardigd door de Informatiebeveiligingsdienst voor gemeenten (IBD).
Inhoud

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligingsbeleid voor de jaren 2020 tot en met 2022 en vervangt het in 2018 vastgestelde 'Informatiebeveiligingsbeleid Senzer 2018 - 2021'.
Deze nota is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau.

Met dit Informatiebeveiligingsbeleid 2020 - 2022 zet Senzer een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen Senzer te continueren en voort te gaan op de stappen die in de voorgaande jaren gezet zijn. De basis voor dit strategisch beleid is de NEN-ISO/IEC 27002:2017 en de daarvan afgeleide Baseline Informatiebeveiliging Overheid (Kader BIO, zie bijlage 1). De principes zijn gebaseerd op de 10 principes voor informatiebeveiliging (zie bijlage 2).

1.1 Leeswijzer

In hoofdstuk 2 wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatiebeveiligingsplan worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Daarin staan dan ook de acties en planning vermeld, om de praktijk in overeenstemming te brengen met datgene wat in het beleid is geëist. Hoofdstuk 3 beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn.

1.2 Wat is informatiebeveiliging?

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

2. Strategisch beleid2.1 Doelf

Het doel van deze beleidsnota is het presenteren van het Informatiebeveiligingsbeleid Senzer 2020 - 2022. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan.

2.2 Ontwikkelingen

De ontwikkelingen die van belang zijn voor de actualisering van het informatiebeveiligingsbeleid zijn de volgende.

2.2.1 De BIO (zie bijlage 1)

De BIO (Baseline Informatiebeveiliging Overheid) is het nieuwe normenkader voor de gehele overheid. De werkwijze van deze BIO is meer gericht op risicomanagement dan de oude BIG. Dat wil zeggen dat het management nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement van belang. Dit houdt voor het management in, dat men op voorhand keuzes maakt en continu afwegingen maakt of informatie in bestaande en nieuwe processen adequaat beveiligd zijn in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

2.2.2 De 10 principes voor informatiebeveiliging (zie bijlage 2)

De 10 principes voor informatiebeveiliging zijn een aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Management bevordert een veilige cultuur.
2. Informatiebeveiliging is van iedereen.
3. Informatiebeveiliging is risicomanagement.
4. Risicomanagement is onderdeel van de besluitvorming.
5. Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking.
6. Informatiebeveiliging is een proces.
7. Informatiebeveiliging kost geld.
8. Onzekerheid dient te worden ingecalculeerd.
9. Verbetering komt voort uit leren en ervaring.
10. De directie controleert en evalueert.

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

2.2.3 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten

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

2.2.4 Informatie uit incidenten en inbreuken op beveiliging

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

2.3 Standaarden informatiebeveiliging

De basis voor de inrichting van het beveiligingsbeleid is NEN-ISO/IEC 27001:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen. De interbestuurlijke werkgroep Normatiek[1] heeft in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Op grond van de met de gemeenten afgesloten Verwerkersovereenkomsten, afgesloten op basis van de Gemeenschappelijke Regeling WADP/Mandaatbesluit Samenwerking WADP (punt II sub C), geldt het BIO ook voor Senzer. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. De inhoud en structuur van deze nota zijn afgestemd op die van de ISO en de BIO. Ook het Informatiebeveiligingsplan zal deze structuur volgen.

2.4 Plaats van het strategisch beleid

Dit Informatiebeveiligingsbeleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en daarmee richting te geven voor de verdere invulling van informatiebeveiliging op tactisch en operationeel niveau. Deze nota beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. De daaruit voortkomende werkzaamheden worden uitgewerkt in het jaarlijks te schrijven "Informatiebeveiligingsplan Senzer".

2.5 Scope informatiebeveiliging

De scope van dit beleid omvat alle processen, onderliggende informatiesystemen, informatie en gegevens van Senzer, de deelnemende gemeenten en externe partijen, het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

Dit Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de SUWI. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI). Deze worden in aanvullende documenten geformuleerd.
Bewust wordt in dit beleid geen limitatief overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.6 Uitgangspunten

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

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

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

Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van Senzer en de relevante landelijke en Europese wet- en regelgeving, waarbij met name ook de Algemene Verordening Gegevensbescherming (AVG). De AVG regelt in artikel 32 welke maatregelen organisaties moeten treffen in het kader van informatiebeveiliging om op een adequate manier persoonsgegevens te beschermen. Voor wat betreft Senzer is daarnaast uitgegaan van de verwerking van persoonsgegevens, zoals bedoeld in artikel 9 en 10 van de AVG. Deze maatregelen dienen deel uit te maken van het informatiebeveiligingsbeleid van Senzer.

2.6.1 Doelen

De doelen van het informatiebeveiligingsbeleid zijn:

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

2.6.2 Belangrijkste uitgangspunten

De belangrijkste uitgangspunten van het beleid zijn:

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

7. Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.6.3 Invulling van de uitgangspunten

Praktisch wordt als volgt invulling gegeven aan de uitgangspunten:

1. De Algemeen directeur stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
2. De Algemeen directeur stelt jaarlijks het informatiebeveiligingsplan vast.
3. De directie is verantwoordelijk voor het vragen om informatie bij de managers en ziet erop toe dat de managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
4. De Chief Information Officer (CIO) is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
5. De Chief Information Security Officer (CISO) ondersteunt vanuit een onafhankelijke positie de organisatie bij het bewaken en verhogen van de betrouwbaarheid van de informatievoorziening en rapporteert, periodiek in elk geval per kwartaal en tussentijds indien noodzakelijk, hierover rechtstreeks aan de directie.
6. Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
7. De managers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
8. Alle medewerkers van Senzer worden getraind in het gebruik van beveiligingsprocedures.
9. Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.
10. Managers dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende medewerkers de juiste persoonsgegevens ingezien en verwerkt hebben.
11 De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Managers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.
    1.

2.6.4 Randvoorwaarden

Belangrijke randvoorwaarden zijn:

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

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het management verantwoordelijk voor de eigen processen. De tweede lijn (CISO voor wat betreft de algehele informatiebeveiliging en daarnaast de Security-Officer Suwinet en Functionaris Gegevensbescherming met betrekking tot hun specifieke onderdelen respectievelijk Suwinet en AVG) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. 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.

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. De directie zorgt dat de managers 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 overig management. Het onderwerp informatiebeveiliging wordt binnen Senzer gezien als een integraal onderdeel van risicomanagement.

De CIO maakt deel uit van het MT Senzer en geeft namens de directie van Senzer op dagelijkse basis invulling aan de sturende rol door besluitvorming in de directie voor te bereiden en toe te zien op de uitvoering ervan.

3.2 Uitvoering: Managers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle managers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Managers rapporteren aan de directie (via de CIO/CISO) over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten (denk aan bijvoorbeeld: verslag van halfjaarlijkse controle autorisaties informatiesystemen). Afstemming met de afdelingen over de inhoudelijke aanpak vindt plaats door minimaal 2 keer per jaar het onderwerp Informatiebeveiliging te bespreken in het afdelings-/teamoverleggen.

Taken van de managers in het kader van informatiebeveiliging zijn:

1. Het leveren van input voor wijzigingen op maatregelen en procedures.
2. Het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures.
3. Het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld.
4. Bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

3.3 Coördinatie/ondersteuning: CISO

De CISO ondersteunt, adviseert (gevraagd en ongevraagd), coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. De CISO heeft periodiek overleg met de CIO.

Taken van de CISO in het kader van informatiebeveiliging zijn:

1. Het voorbereiden van beleid met betrekking tot informatiebeveiliging.
2. Het ondersteunen/adviseren van de managers bij het uitvoeren van verplichting met betrekking tot informatiebeveiliging (denk aan: uitvoeren dataclassificatie, opstellen en bewaken van autorisatieprocedures- en matrixen).
3. Het archiveren en/of van publiceren van beleidstukken met betrekking informatiebeveiliging en verantwoordingsrapportages van managers.
4. Het opstellen van kwartaalverslagen en jaarverslag met betrekking tot informatiebeveiliging.
5. Het laten uitvoeren van interne en externe audits.

3.4 Controle: Interne Controle

Interne Controle voert jaarlijks een interne audit uit op de juiste uitvoering 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 worden voorbereid door de CISO.

Vastgesteld te Helmond op 09 december 2019.

De Algemeen directeur Senzer,

A.E.W. van Limpt

Bijlage 1: Kader BIO

Inleiding

Het Kader BIO bestaat uit een BBN-toets om het juiste Basis Beveiligingsniveau (BBN) te bepalen en de tabellen met de controls en maatregelen. De BBN toets wordt voor ieder informatiesysteem uitgevoerd. Het BBN bepaalt welke controls vervolgens moeten worden doorlopen. Per control moet worden bepaald welke maatregelen in aanvulling op de verplichte overheidsmaatregelen nodig zijn.

Basisbeveiligingsniveaus
De BIO onderscheidt drie basisbeveiligingsniveaus (BBN). Ieder BBN bestaat uit een aantal controls, een aantal verplichte overheidsmaatregelen en een verantwoordings- en toezichtregime. Elk niveau bouwt voort op het vorige niveau. Daarbij vult BBN2 de controls van BBN1 aan. BBN2 vult ook de overheidsmaatregelen van BBN1 aan of vervangt deze door maatregelen met meer gewicht. Hetzelfde geldt voor BBN3 in relatie tot BBN1 en BBN2.

BBN1
Informatiesystemen op BBN1 niveau zijn systemen waarvoor BBN2 als te zwaar wordt gezien. Het kan voorkomen dat er nog wel hogere beschikbaarheids- en integriteitseisen nodig zijn. BBN1 is waar alle overheidssystemen als minimum aan moeten voldoen.

Controls en overheidsmaatregelen komen voort uit:
- wet- en regelgeving;
- algemeen geldende beveiligingsprincipes (fundamentele controls en maatregelen).

BBN2
Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. BBN2 is van toepassing indien :
1. er vertrouwelijke informatie wordt verwerkt;
2. mogelijke incidenten leiden tot bestuurlijke commotie;
3. er onzekerheid bestaat of ook alle informatie van derden open is;
4. de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

De controls van het BBN2 omvatten de controls van BBN1. Dit geldt ook voor de maatregelen waarbij enkele maatregelen van BBN1 in de BBN2 variant verzwaard zijn. De keuze hiervoor komt voort uit:
1. wet- en regelgeving, in het bijzonder beveiligingseisen a.g.v. WBP/AVG;
2. aansluitvoorwaarden van generieke/gemeenschappelijke diensten;
3. afhankelijkheden in ketens en netwerken;
4. minimale eisen ten behoeve van een efficiënte beveiliging van BBN3.

BBN3
BBN3 richt zich op de bescherming van Departementaal Vertrouwelijk en vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie waarbij weerstand geboden moet worden tegen de dreiging, die uitgaat van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien:
1. verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3;
2. informatie met een rubricering (niet zijnde BBN2) wordt geleverd door derden;
3. aansluiting op een infrastructuur BBN3 is vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen).

BBN-toets
Bij het doorlopen van deze toets is BBN2 het uitgangspunt voor alle informatiesystemen.

<u>Stap 1: Is BBN2 voldoende?</u>
Meestal is BBN2 van toepassing op een specifiek informatiesysteem. Het kan echter zijn dat BBN2 niet voldoende is. BBN2 is onvoldoende indien:
1. de informatie beschermd dient te worden tegen statelijke actoren of vergelijkbare dreigers; of
2. informatie wordt geleverd door derden en deze voor de beveiliging van betreffende informatie BBN3 eisen; of
3. aansluiting op een infrastructuur het BBN3 vereist om informatie te kunnen verwerken op deze infrastructuur (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen)

In elk van deze gevallen is BBN3 of hoger van toepassing. (*Opmerking: BBN3 is niet van toepassing op Senzer*).

<u>Stap 2: Is BBN2 te zwaar?</u>
Bij BBN2 informatiesystemen kan het ongewenst of onbedoeld openbaren van informatie leiden tot BBN2-schade:

1. politieke schade aan een bestuurder: bestuurder moet verantwoording afleggen aan de (gekozen) controlerende organen, bijvoorbeeld n.a.v. verantwoordingsvragen; of
2. diplomatieke schade te herstellen door ambtelijke opschaling; of
3. financiële gevolgen: niet meer op te vangen binnen de begroting van de (uitvoerings)organisatie of uitvoeringsorganisatie; geen accountantsverklaring afgegeven; of
4. verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; of
5. bindende aanwijzing van de AP in verband met schending van de privacy; of
6. directe imagoschade, bijvoorbeeld door negatieve publiciteit.

Zijn dergelijke schades niet aan de orde, dan is BBN1 van toepassing.

Stap 3: Bepaal extra vereisten voor beschikbaarheid en/of integriteit
In het geval van BBN1: leidt uitval van systemen en/of het verminkt raken van informatie tot schade vergelijkbaar met BBN2-schade? In dat geval kan worden overwogen (een deel) van de BIO controls en maatregelen, die toezien op beschikbaarheid dan wel integriteit op het niveau van BBN2 te nemen. De verantwoording en toezicht vindt plaats volgens BBN2.

In het geval van BBN2 of BBN3: leidt uitval van systemen en/of het verminkt raken van informatie tot grotere schade dan de BBN2-schade? In dat geval wordt op basis van expliciete risicoafweging bepaald voor welke controls welke aanvullende en/of zwaardere maatregelen nodig zijn. De verantwoording en toezicht vindt plaats volgens BBN3.

Controls en overheidsmaatregelen
Voor de herkenbaarheid is gekozen om de nummering van de hoofdstukken en de controls in lijn te houden met de nummering uit de ISO27002.
Om het verschil tussen de ISO 27002 controls en de overheidsmaatregelen te duiden, zijn ook verschillende kleurmarkeringen gebruikt:
1. Blauw zijn de ISO controls
2. Groen zijn overheidsmaatregelen

5. Informatiebeveiligingsbeleid
5.1 Aansturing door de directie van de informatiebeveiliging
Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

ISO-nummer	BBN-nummer	Omschrijving
5.1.1	**BBN 1**	**Beleidsregels voor informatiebeveiliging** Ten behoeve van informatiebeveiliging behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.
5.1.1.1	BBN 1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat tenminste de volgende punten: 1. de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; 2. de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; 3. de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; 4. de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; 5. de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; 6. de bevordering van het beveiligingsbewustzijn.
5.1.2	**BBN 1**	**Beoordeling van het informatiebeveiligingsbeleid** Het beleid voor informatiebeveiliging behoort met geplande tussenpozen of als zich significante veranderingen voordoen, te worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
5.1.2.1	BBN 1	Het informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar, of bij belangrijke wijzigingen als gevolg van reorganisatie of verandering in de verantwoordelijkheidsverdeling, beoordeeld en zo nodig bijgesteld.

6. Organiseren van informatiebeveiliging
6.1 Interne organisatie
Doelstelling: Een beheerkader vaststellen om de implementatie en uitvoering van de informatiebeveiliging binnen de organisatie te initiëren en te beheersen.

6.1.1	**BBN 1**	**Rollen en verantwoordelijkheden bij informatiebeveiliging** Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
6.1.1.1	BBN 1	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
6.1.1.2	BBN 1	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
6.1.1.3	BBN 1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.
6.1.1.4	BBN 1	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
6.1.2	**BBN 1**	**Scheiding van taken** Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.
6.1.2.1	BBN 1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.
6.1.3	**BBN 2**	**Contact met overheidsinstanties** Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.
6.1.3.1	BBN 2	Er is door de organisatie uitgewerkt wie met welke (overheids)instanties en toezichthouders contact heeft ten aanzien van informatiebeveiligingsaangelegenheden (vergunningen/incidenten/calamiteiten) en welke eisen voor deze aangelegenheden relevant zijn.
6.1.3.2	BBN 2	Het contactoverzicht wordt jaarlijks geactualiseerd.
6.1.5	**BBN 2**	**Informatiebeveiliging in projectbeheer** Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.

6.2 Mobiele apparatuur en telewerken

Doelstelling: Het waarborgen van de veiligheid van telewerken en het gebruik van mobiele apparatuur.

6.2.1	**BBN 1**	**Beleid voor mobiele apparatuur** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.
6.2.1.1	BBN 2	Mobiele apparatuur is zo ingericht dat geen bedrijfsinformatie onbewust wordt opgeslagen ('zero footprint'). Als zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat (zoals een laptop, tablet en smartphone) de mogelijkheid om de toegang te beschermen door middel van een toegangsbeveiligingsmechanisme en, indien vertrouwelijke gegevens worden opgeslagen, versleuteling van die gegevens. In het geval van opslag van vertrouwelijke informatie moet op deze mobiele apparatuur 'wissen op afstand' mogelijk zijn.
6.2.1.2	BBN 2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: 1. in bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde; 2. het device maakt onderdeel uit van patchmanagement en hardening; 3. het device wordt waar mogelijk beheerd en beveiligd via een MDM Mobile Device Management (MDM)-oplossing; 4. gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt; Periodiek wordt getoetst of de punten 2, 3 en 4 worden nageleefd.
6.2.2	**BBN 2**	**Telewerken** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.

7. Veilig personeel

7.1 Voorafgaand aan het dienstverband

Doelstelling: Waarborgen dat medewerkers en contractanten hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij in aanmerking komen.

7.1.1	**BBN 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.
7.1.1.1	BBN 1	Bij indiensttreding overleggen alle medewerkers (intern en extern) een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG).
7.1.2	**BBN 1**	**Arbeidsvoorwaarden** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.
7.1.2.1	BBN 1	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.

7.2 Tijdens het dienstverband

Doelstelling: Ervoor zorgen dat medewerkers en contractanten zich bewust zijn van hun verantwoordelijkheden op het gebied van informatiebeveiliging en deze nakomen.

7.2.1	**BBN 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.
7.2.1.1	BBN 1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen in staat is om anoniem en veilig beveiligingsissues te kunnen melden.
7.2.2	**BBN 1**	**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.
7.2.2.1	BBN 1	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen
7.2.2.2	BBN 1	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.
7.2.2.3	BBN 1	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen
7.2.3	**BBN 1**	**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.

7.3 Beëindiging en wijziging van dienstverband

Doelstelling: Het beschermen van de belangen van de organisatie als onderdeel van de wijzigings- of beëindigingsprocedure van het dienstverband.

7.3.1	**BBN 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.

8. Beheer van bedrijfsmiddelen

8.1 Verantwoordelijkheid voor bedrijfsmiddelen

Doelstelling: Bedrijfsmiddelen van de organisatie identificeren en passende verantwoordelijkheden ter bescherming definiëren.

8.1.1	**BBN 1**	**Inventariseren van bedrijfsmiddelen** Informatie, andere bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden.
8.1.2	**BBN 1**	**Eigendom van bedrijfsmiddelen** Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.
8.1.3	**BBN 1**	**Aanvaardbaar gebruik van bedrijfsmiddelen** Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.
8.1.3.1	BBN 1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.
8.1.3.2	BBN 1	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.
8.1.4	**BBN 1**	**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.

8.2 Informatieclassificatie

Doelstelling: Bewerkstelligen dat informatie een passend beschermingsniveau krijgt dat in overeenstemming is met het belang ervan voor de organisatie.

8.2.1	**BBN 1**	**Classificatie van informatie** Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.
8.2.1.1	BBN 1	De informatie in alle informatiesystemen is door middel van een expliciete risicoafweging geclassificeerd, zodat duidelijk is welke bescherming nodig is.
8.2.2	**BBN 1**	**Informatie labelen**

		Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.
8.2.3	**BBN 1**	**Behandelen van bedrijfsmiddelen** Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.

8.3 Behandelen van media

Doelstelling: Onbevoegde openbaarmaking, wijziging, verwijdering of vernietiging van informatie die op media is opgeslagen voorkomen.

8.3.1	**BBN 1**	**Beheer van verwijderbare media** Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.
8.3.1.1	BBN 1	Er is een verwijderinstructie waarin is opgenomen dat van herbruikbare media die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd (ISO27002 – implementatierichtlijn 8.3.1.a).
8.3.1.2	BBN 2	De wijze waarop vertrouwelijk of hoger geclassificeerde informatie is opgeslagen, voldoet aan de eisen van het NBV.
8.3.2	**BBN 2**	**Verwijderen van media** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.
8.3.2.1	BBN 2	Media die vertrouwelijke informatie bevatten zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden. Verwijdering vindt plaats op een veilige manier, bijv. door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO27002 – implementatierichtlijn 8.3.2.a)
8.3.2.2	BBN 2	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.
8.3.3	**BBN 2**	**Media fysiek overdragen** Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.
8.3.3.1	BBN 2	Er is voor de gehele organisatie beleid voor het fysiek transport van media vastgesteld.
8.3.3.2	BBN 2	Het gebruik van koeriers of transporteurs voor vertrouwelijk of hoger geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.

9. Toegangsbeveiliging

9.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling: Toegang tot informatie en informatie verwerkende faciliteiten beperken.

9.1.1	**BBN 1**	**Beleid voor toegangsbeveiliging** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.
9.1.2	**BBN 1**	**Toegang tot netwerken en netwerkdiensten** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.
9.1.2.1	BBN 1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.
9.1.2.2	BBN 1	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.

9.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.

9.2.1	**BBN 1**	**Registratie en afmelden van gebruikers** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.
9.2.1.1	BBN 1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.
9.2.1.2	BBN 1	Het gebruiken van groepsaccounts is niet toegestaan tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.
9.2.2	**BBN 1**	**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.
9.2.2.1	BBN 1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.
9.2.2.2	BBN 1	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.

9.2.2.3	BBN 2	Er is een actueel mandaatregister waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten dan wel functieprofielen.
9.2.3	**BBN 1**	**Beheren van speciale toegangsrechten** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.
9.2.3.1	BBN 2	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.
9.2.4	**BBN 1**	**Beheer van geheime authenticatie-informatie van gebruikers** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.
9.2.5	**BBN 1**	**Beoordeling van toegangsrechten van gebruikers** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.
9.2.5.1	BBN 1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.
9.2.5.2	BBN 1	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.
9.2.5.3	BBN 2	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.
9.2.6	**BBN 1**	**Toegangsrechten intrekken of aanpassen** De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatie verwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.

9.3 Verantwoordelijkheden van gebruikers

Doelstelling: Gebruikers verantwoordelijk maken voor het beschermen van hun authenticatie-informatie.

9.3.1	**BBN 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.
9.3.1.1	BBN 2	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.

9.4 Toegangsbeveiliging van systeem en toepassing

Doelstelling: Onbevoegde toegang tot systemen en toepassingen voorkomen.

9.4.1	**BBN 1**	**Beperking toegang tot informatie** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.
9.4.1.1	BBN 2	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.
9.4.1.2	BBN 2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.
9.4.2	**BBN 1**	**Beveiligde inlogprocedures** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.
9.4.2.1	BBN 1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.
9.4.2.2	BBN 2	Voor het verlenen van toegang tot het netwerk door externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.
9.4.3	**BBN 1**	**Systeem voor wachtwoordbeheer** Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.
9.4.3.1	BBN 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 inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.
9.4.3.2	BBN 2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).
9.4.3.3	BBN 2	Het wachtwoordbeleid wordt geautomatiseerd afgedwongen.
9.4.3.4	BBN 2	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.
9.4.3.5	BBN 2	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.
9.4.4	**BBN 1**	**Speciale systeemhulpmiddelen gebruiken** Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.

9.4.4.1	BBN 1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.
9.4.4.2	BBN 2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek
9.4.5	**BBN 1**	**Toegangsbeveiliging op programmabroncode** Toegang tot de programmabroncode behoort te worden beperkt.

10. Cryptografie

10.1 Cryptografische beheersmaatregelen

Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.

10.1.1	**BBN 2**	**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.
10.1.1.1	BBN 2	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: 1. wanneer cryptografie ingezet wordt; 2. wie verantwoordelijk is voor de implementatie; 3. wie verantwoordelijk is voor het sleutelbeheer; 4. welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast; 5. de wijze waarop het beschermingsniveau vastgesteld wordt; 6. bij inter-organisatie communicatie wordt het beleid onderling vastgesteld.
10.1.1.2	BBN 2	Cryptografische toepassingen voldoen aan passende standaarden.
10.1.2	**BBN 1**	**Sleutelbeheer** Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.
10.1.2.1	BBN 2	Ingeval van PKI-overheid certificaten: hanteer de PKI-Overheid-eisen t.a.v. het sleutelbeheer. In overige situaties: hanteer de standaard ISO-11770 voor het beheer van cryptografische sleutels.
10.1.2.2	BBN 2	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.

11. Fysieke beveiliging en beveiliging van de omgeving

11.1 Beveiligde gebieden

Doelstelling: Onbevoegde fysieke toegang tot, schade aan en interferentie met informatie en informatie verwerkende faciliteiten van de organisatie voorkomen.

11.1.1	**BBN 1**	**Fysieke beveiligingszone** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.
11.1.1.1	BBN 1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.
11.1.2	**BBN 1**	**Fysieke toegangsbeveiliging** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
11.1.2.1	BBN 2	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.
11.1.3	**BBN 1**	**Kantoren, ruimten en faciliteiten beveiligen** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.
11.1.3.1	BBN 1	Sleutelbeheer is ingericht op basis van een sleutelplan.
11.1.4	**BBN 1**	**Beschermen tegen bedreigingen van buitenaf** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.
11.1.4.1	BBN 1	De organisatie heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.
11.1.4.2	BBN 1	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.
11.1.5	**BBN 2**	**Werken in beveiligde gebieden** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.
11.1.6	**BBN 1**	**Laad- en loslocatie** Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.

11.2 Apparatuur

Doelstelling: Verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsvoering van de organisatie voorkomen.

11.2.1	**BBN 1**	**Plaatsing en bescherming van apparatuur** Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.
11.2.2	**BBN 1**	**Nutsvoorzieningen** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.
11.2.3	**BBN 1**	**Beveiliging van bekabeling** Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.
11.2.4	**BBN 1**	**Onderhoud van apparatuur** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.
11.2.5	**BBN 1**	**Verwijdering van bedrijfsmiddelen** Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.
11.2.6	**BBN 1**	**Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein** Bedrijfsmiddelen die zich buiten het terrein bevinden, behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.
11.2.7	**BBN 1**	**Veilig verwijderen of hergebruiken van apparatuur** Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
11.2.8	**BBN 1**	**Onbeheerde gebruikersapparatuur** Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.
11.2.9	**BBN 1**	**'Clear desk'- en 'clear screen'-beleid** Er behoort een 'clear desk'-beleid voor papieren documenten en verwijderbare opslagmedia en een 'clear screen'-beleid voor informatie verwerkende faciliteiten te worden ingesteld.
11.2.9.1	BBN 2	Een onbeheerde werkplek in een ongecontroleerde omgeving is altijd vergrendeld.
11.2.9.2	BBN 2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.
11.2.9.3	BBN 2	Sessies op remote desktops worden op het remote platform vergrendeld na 15 minuten. Het overnemen van sessies op remote desktops op een ander client apparaat is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd.
11.2.9.4	BBN 2	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van de token de toegangsbeveiligingslock automatisch geactiveerd.

12. Beveiliging bedrijfsvoering

12.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling: Correcte en veilige bediening van informatie verwerkende faciliteiten waarborgen.

12.1.1	**BBN 1**	**Gedocumenteerde bedieningsprocedures** Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
12.1.2	**BBN 1**	**Wijzigingsbeheer** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.
12.1.2.1	BBN 1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: 1. het administreren van wijzigingen; 2. risicoafweging van mogelijke gevolgen van de wijzigingen; 3. goedkeuringsprocedure voor wijzigingen.
12.1.3	**BBN 1**	**Capaciteitsbeheer** Het gebruik van middelen behoort te worden gemonitord en afgestemd, en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te waarborgen.
12.1.3.1	BBN 1	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijv. DDoS attacks, Distributed Denial of Service attacks) te signaleren en hierop te reageren.
12.1.4	**BBN 1**	**Scheiding van ontwikkel-, test- en productieomgevingen** Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.
12.1.4.1	BBN 2	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.
12.1.4.2	BBN 2	Wijzigingen op de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hierop worden afgeweken.

12.2 Bescherming tegen malware

Doelstelling: Waarborgen dat informatie en informatie verwerkende faciliteiten beschermd zijn tegen malware.

12.2.1	**BBN 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.
12.2.1.1	BBN 1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.
12.2.1.2	BBN 1	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende linken.
12.2.1.3	BBN 1	Software en bijbehorende herstelsoftware die malware opspoort zijn geïnstalleerd en worden regelmatig geüpdatet.
12.2.1.4	BBN 1	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: 1. alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen; 2. bijlagen en downloads vóór gebruik.
12.2.1.5	BBN 1	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.

12.3 Back-up

Doelstelling: Beschermen tegen het verlies van gegevens.

12.3.1	**BBN 1**	**Back-up van informatie** Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid.
12.3.1.1	BBN 1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld
12.3.1.2	BBN 1	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.
12.3.1.3	BBN 2	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.
12.3.1.4	BBN 2	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.
12.3.1.5	BBN 2	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de betrouwbaarheid te waarborgen als ze in noodgevallen uitgevoerd moet worden.

12.4 Verslaglegging en monitoren

Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

12.4.1	**BBN 1**	**Gebeurtenissen registreren** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
12.4.1.1	BBN 1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.
12.4.1.2	BBN 1	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
12.4.1.3	BBN 2	De informatie verwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties), die worden ingezet op basis van een risico-inschatting, mede aan de hand van en de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.
12.4.1.4	BBN 2	Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.
12.4.1.5	BBN 2	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.
12.4.2	**BBN 1**	**Beschermen van informatie in logbestanden** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.
12.4.2.1	BBN 1	Er is een overzicht van logbestanden die worden gegenereerd.
12.4.2.2	BBN 1	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.
12.4.2.3	BBN 2	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.

12.4.2.4	BBN 2	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.
12.4.3	**BBN 1**	**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.
12.4.4	**BBN 1**	**Kloksynchronisatie** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.

12.5 Beheersing van operationele software

Doelstelling: De integriteit van operationele systemen waarborgen.

12.5.1	**BBN 1**	**Software installeren op operationele systemen** Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.

12.6 Beheer van technische kwetsbaarheden

Doelstelling: Benutting van technische kwetsbaarheden voorkomen.

12.6.1	**BBN 1**	**Beheer van technische kwetsbaarheden** Informatie over technische kwetsbaarheden van informatiesystemen die worden gebruikt behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden te worden geëvalueerd en passende maatregelen te worden genomen om het risico dat ermee samenhangt aan te pakken.
12.6.1.1	BBN 1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.
12.6.2	**BBN 1**	**Beperkingen voor het installeren van software** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.
12.6.2.1	BBN 2	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).

12.7 Overwegingen betreffende audits van informatiesystemen

Doelstelling: De impact van auditactiviteiten op uitvoeringssystemen zo gering mogelijk maken.

12.7.1	**BBN 1**	**Beheersmaatregelen betreffende audits van informatiesystemen** Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.

13. Communicatiebeveiliging

13.1 Beheer van netwerkbeveiliging

Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten waarborgen.

13.1.1	**BBN 1**	**Beheersmaatregelen voor netwerken** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
13.1.2	**BBN 1**	**Beveiliging van netwerkdiensten** Beveiligingsmechanismen, dienstverleningsniveaus en beheer eisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
13.1.2.1	BBN 2	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectie-voorzieningen (zoals beschreven in de richtlijn voor implementatie van detectie-oplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.
13.1.2.2	BBN 2	Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).
13.1.2.3	BBN 2	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied, wordt gebruik gemaakt van encryptie middelen waarvoor het NBV een positief inzetadvies heeft afgegeven.
13.1.3	**BBN 1**	**Scheiding in netwerken**

		Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.
13.1.3.1	BBN 2	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.

13.2 Informatietransport

Doelstelling: Handhaven van de beveiliging van informatie die wordt uitgewisseld binnen een organisatie en met een externe entiteit.

13.2.1	**BBN 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.
13.2.2	**BBN 1**	**Overeenkomsten over informatietransport** Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.
13.2.3	**BBN 1**	**Elektronische berichten** Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.
13.2.3.1	BBN 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.
13.2.3.2	BBN 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
13.2.3.3	BBN 2	Maak gebruik van PKI-Overheid certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn o.a. digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.
13.2.3.4	BBN 2	Om zekerheid te bieden over de integriteit van het elektronische bericht wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.
13.2.4	**BBN 1**	**Vertrouwelijkheids- of geheimhoudingsovereenkomst** Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.

14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen

14.1 Beveiligingseisen voor informatiesystemen

Doelstelling: Waarborgen dat informatiebeveiliging integraal deel uitmaakt van informatiesystemen in de gehele levenscyclus. Hiertoe behoren ook de eisen voor informatiesystemen die diensten verlenen via openbare netwerken.

14.1.1	**BBN 1**	**Analyse en specificatie van informatiebeveiligingseisen** De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.
14.1.1.1	BBN 1	Bij nieuwe informatiesystemen en bij wijzigingen op bestaande informatiesystemen moet een expliciete risicoafweging worden uitgevoerd ten behoeve van het vaststellen van de beveiligingseisen, uitgaande van de BIO.
14.1.2	**BBN 1**	**Toepassingen op openbare netwerken beveiligen** Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.
14.1.3	**BBN 1**	**Transacties van toepassingen beschermen** Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen van berichten, onbevoegd openbaar maken, onbevoegd vermenigvuldigen of afspelen.

14.2 Beveiliging in ontwikkelings- en ondersteunende processen

Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.

14.2.1	**BBN 1**	**Beleid voor beveiligd ontwikkelen** Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.
14.2.1.1	BBN 1	De gangbare principes rondom Security by design zijn uitgangspunt voor de ontwikkeling van software en systemen
14.2.2	**BBN 1**	**Procedures voor wijzigingsbeheer met betrekking tot systemen** Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.
14.2.2.1	BBN 1	Voor het wijzigingsbeheer gelden de algemeen geaccepteerde beheerframeworks, zoals ITIL, ASL of BiSL.

14.2.3	**BBN 2**	**Technische beoordeling van toepassingen na wijzigingen besturingsplatform** Als besturingsplatforms zijn veranderd, behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of de beveiliging van de organisatie.
14.2.5	**BBN 1**	**Principes voor engineering van beveiligde systemen** Principes voor de engineering van beveiligde systemen behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.
14.2.5.1	BBN 1	Zie overheidsmaatregel 14.2.1.1
14.2.6	**BBN 1**	**Beveiligde ontwikkelomgeving** Organisaties behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie, die betrekking hebben op de gehele levenscyclus van de systeemontwikkeling.
14.2.6.1	BBN 1	Uitgangspunt voor systeemontwikkeling trajecten is een expliciete risicoafweging. Deze heeft zowel de ontwikkelomgeving als ook het te ontwikkelen systeem in scope.
14.2.7	**BBN 1**	**Uitbestede softwareontwikkeling** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.
14.2.7.1	BBN 1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.
14.2.8	**BBN 1**	**Testen van systeembeveiliging** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.
14.2.9	**BBN 1**	**Systeemacceptatietests** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.
14.2.9.1	BBN 1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.
14.2.9.2	BBN 1	Van de resultaten van de testen wordt verslag gemaakt.

14.3 Testgegevens

Doelstelling: Bescherming waarborgen van gegevens die voor het testen zijn gebruikt.

14.3.1	**BBN 2**	**Bescherming van testgegevens** Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.

15. Leveranciersrelaties

15.1 Informatiebeveiliging in leveranciersrelaties

Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

15.1.1	**BBN 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.
15.1.1.1	BBN 1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen t.a.v. informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.
15.1.1.2	BBN 2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekken tot leverancierstoegang tot bedrijfsinformatie vastgesteld.
15.1.1.3	BBN 2	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
15.1.2	**BBN 1**	**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.
15.1.2.1	BBN 1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.
15.1.2.2	BBN 1	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.
15.1.2.3	BBN 1	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.
15.1.2.4	BBN 1	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaard voorwaarden voor inkoop gehanteerd.
15.1.2.5	BBN 2	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.

15.1.2.6	BBN 2	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 d.m.v. certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.
15.1.3	**BBN 1**	**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.
15.1.3.1	BBN 2	Leveranciers moeten hun keten van toeleveranciers bekend maken en transparant zijn over de maatregelen die zij genomen hebben om de aan hun opgelegde eisen ook door te vertalen naar hun toeleveranciers.

15.2 Beheer van dienstverlening van leveranciers

Doelstelling: Een overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming met de leveranciersovereenkomsten handhaven.

15.2.1	**BBN 1**	**Monitoring en beoordeling van dienstverlening van leveranciers** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.
15.2.1.1	BBN 2	Jaarlijks wordt de prestatie van leveranciers op het gebied van informatiebeveiliging beoordeeld op vooraf vastgestelde prestatie-indicatoren, zoals in het contract opgenomen is.
15.2.2	**BBN 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. Beheer van informatiebeveiligingsincidenten

16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Doelstelling: Een consistente en doeltreffende aanpak bewerkstelligen van het beheer van informatiebeveiligingsincidenten, met inbegrip van communicatie over beveiligingsgebeurtenissen en zwakke plekken in de beveiliging.

16.1.1	**BBN 1**	**Verantwoordelijkheden en procedures** Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.
16.1.2	**BBN 1**	**Rapportage van informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.
16.1.2.1	BBN 1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.
16.1.2.2	BBN 1	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
16.1.2.3	BBN 1	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.
16.1.2.4	BBN 1	Incidenten worden zo snel als mogelijk, maar in ieder geval binnen 24 uur na bekendwording, gemeld bij het meldloket.
16.1.2.5	BBN 1	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.
16.1.2.6	BBN 1	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.
16.1.2.7	BBN 1	Informatie afkomstig uit de responsible disclosure procedure zijn onderdeel van de incidentrapportage.
16.1.3	**BBN 1**	**Rapportage van zwakke plekken in de informatiebeveiliging** Van medewerkers en contractanten die gebruikmaken van de informatiesystemen en -diensten van de organisatie behoort te worden geëist dat zij de in systemen of diensten waargenomen of vermeende zwakke plekken in de informatiebeveiliging registreren en rapporteren. Zie overheidsmaatregel 16.1.2.4
16.1.3.1	BBN 1	Een responsible disclosure procedure is gepubliceerd en ingericht.
16.1.4	**BBN 1**	**Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincidenten.
16.1.4.1	BBN 2	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT.
16.1.5	**BBN 1**	**Respons op informatiebeveiligingsincidenten** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.
16.1.6	**BBN 2**	**Lering uit informatiebeveiligingsincidenten**

		Kennis die is verkregen door informatiebeveiligingsincidenten te analyseren en op te lossen behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.
16.1.6.1	BBN 2	Beveiligingsincidenten worden geanalyseerd met als doel te leren en het voorkomen van toekomstige beveiligingsincidenten.
16.1.6.2	BBN 2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.
16.1.7	**BBN 2**	**Verzamelen van bewijsmateriaal** De organisatie behoort procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.
16.1.7.1	BBN 2	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.

17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer

17.1 Informatiebeveiligingscontinuïteit

Doelstelling: Informatiebeveiligingscontinuïteit behoort te worden ingebed in de systemen van het bedrijfscontinuïteitsbeheer van de organisatie.

17.1.1	**BBN 1**	**Informatiebeveiligingscontinuïteit plannen** De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.
17.1.2	**BBN 1**	**Informatiebeveiligingscontinuïteit implementeren** De organisatie behoort processen, procedures en beheersmaatregelen vast te stellen, te documenteren, te implementeren en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.
17.1.3	**BBN 1**	**Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren** De organisatie behoort de ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.
17.1.3.1	BBN 2	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.
17.1.3.2	BBN 2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.
17.1.3.3	BBN 2	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten minimaal binnen een week hersteld.

17.2 Redundante componenten

Doelstelling: Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

17.2.1	**BBN 1**	**Beschikbaarheid van informatie verwerkende faciliteiten** Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.

18. Naleving

18.1 Naleving van wettelijke en contractuele eisen

Doelstelling: Voorkomen van schendingen van wettelijke, statutaire, regelgevende of contractuele verplichtingen betreffende informatiebeveiliging en beveiligingseisen.

18.1.1	**BBN 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.
18.1.2	**BBN 1**	**Intellectuele-eigendomsrechten** Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.
18.1.3	**BBN 2**	**Beschermen van registraties** Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.
18.1.3.1	BBN 2	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.
18.1.4	**BBN 1**	**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.
18.1.4.1	BBN 1	In overeenstemming met de AVG heeft iedere organisatie een Functionaris Gegevensbescherming (FG) met voldoende mandaat om zijn/haar functie uit te voeren.
18.1.4.2	BBN 2	Organisaties controleren regelmatig de naleving van de privacy regels en informatieverwerking en –procedures binnen haar verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging. Zie overheidsmaatregel 14.2.6.1
18.1.5	**BBN 1**	**Voorschriften voor het gebruik van cryptografische beheersmaatregelen**

		Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.
18.1.5.1	BBN 1	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de 'pas toe of leg uit'-lijst van het Forum. Zie overheidsmaatregel 10.1.1.1

18.2 Informatiebeveiligingsbeoordelingen
Doelstelling: Verzekeren dat informatiebeveiliging wordt geïmplementeerd en uitgevoerd in overeenstemming met de beleidsregels en procedures van de organisatie.

18.2.1	**BBN 1**	**Onafhankelijke beoordeling van informatiebeveiliging** De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan (bijv. beheerdoelstellingen, beheersmaatregelen, beleidsregels, processen en procedures voor informatiebeveiliging), behoren onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen te worden beoordeeld.
18.2.1.1	BBN 2	Er is een information security information system (ISMS) waarmee aantoonbaar de gehele plan-do-check-act cyclus op gestructureerde wijze wordt afgedekt.
18.2.1.2	BBN 2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.
18.2.2	**BBN 1**	**Naleving van beveiligingsbeleid en -normen** De directie behoort regelmatig de naleving van de informatieverwerking en - procedures binnen haar verantwoordelijkheidsgebied te beoordelen aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.
18.2.2.1	BBN 1	In de P&C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.
18.2.3	**BBN 1**	**Beoordeling van technische naleving** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.
18.2.3.1	BBN 2	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of pentesten.

Bijlage 2:
10 PRINCIPES VOOR FORMATIEBEVEILIGING

Colofon

Met dank aan
De expertgroep, de reviewgemeenten en de Informatiebeveiligingsdienst voor Gemeenten die hebben bijgedragen aan het vervaardigen van dit product.
Versiebeheer
Het beheer van dit document berust bij de Vereniging van Nederlandse Gemeenten (VNG).
Opmaak
Chris Koning (VNG)

De 10 principes voor informatiebeveiliging
Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:
1 De directie bevordert een veilige cultuur
Menselijk gedrag en cultuur beïnvloeden op significante wijze alle aspecten van risicomanagement op elk niveau en in elk stadium.
Ik ben mij bewust van de voorbeeldfunctie van een directeur en ik draag uit dat risicomanagement van iedereen is. Ik zorg daarom voor een cultuur waarin iedereen vrij is om dreigingen waar te nemen en te melden. In eerste instantie bij de verantwoordelijke, maar indien nodig ook bij mij als directeur. Ik

spoor managers aan om voorwaarden te scheppen zodat iedereen binnen de organisatie deelgenoot wordt van het proces van risicomanagement. Ik zorg ervoor dat fouten besproken kunnen worden en dat daarmee een lerende organisatie ontstaat. Ten slotte geef ik in mijn eigen doen en laten het goede voorbeeld van hoe je verantwoordelijk omgaat met informatie.

Toelichting

Zonder open cultuur waar iedereen vrij is om te spreken is het niet goed mogelijk om risico's te identificeren en als de risico's niet bekend zijn, kunt u ze ook niet adresseren. Als u in uw organisatie een cultuur bevordert waarin mensen zich vrij voelen om risico's te melden en maatregelen voor te stellen, dan kunt u adequaat reageren op dreigingen en samenhangende risico's.

2 Informatiebeveiliging is van iedereen

Passende en tijdige betrokkenheid van belanghebbenden maakt het mogelijk dat hun kennis, opvattingen en percepties in aanmerking worden genomen. Dit resulteert in een verbeterd bewustzijn en goed geïnformeerd risicomanagement.

Ik maak medewerkers bewust van de risico's van het werken met informatie en ik maak risicomanagement onderdeel van het MT-overleg en laat het anderen in vergaderingen agenderen. Ik zorg ervoor dat iedereen risicomanagement toepast en dat het gezien wordt als vanzelfsprekend en nuttig.

Toelichting

Iedereen moet betrokken worden bij risicomanagement, in alle lagen van de organisatie. Maak gebruik van de kennis en verantwoordelijkheid van proces- en systeem eigenaren. Gebruik uw Chief Information Officer (CIO), Chief Information Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Concerncontroller als onafhankelijke adviseur en laat ze samenwerken in een risicoteam, waar u vanzelfsprekend ook zitting in heeft. Laat uw interne communicatie aandacht besteden aan het verspreiden van de boodschap, het belang en het voordeel van risicomanagement binnen uw organisatie. Goed uitgevoerd risicomanagement creëert waarde voor de organisatie omdat de kwaliteit van besluiten toeneemt en de kans op falen afneemt,

3 Informatiebeveiliging is risicomanagement

Risicomanagement wordt bewust toegepast bij alle organisatie activiteiten.

Ik zorg dat risicomanagement een onderdeel is van het managementoverleg en dialoog. Daarnaast zal ik het integreren in het risicobewustzijn van alle medewerkers en het onderdeel laten zijn van de samenwerking met partners en ik zorg ervoor dat risicomanagement integraal onderdeel uitmaakt van uitbestedingen en samenwerkingen. Ik zorg ervoor dat risicomanagement geformaliseerd wordt binnen de hele organisatie met een duidelijke verdeling van verantwoordelijkheden en heldere besluitvorming.

Toelichting

Risicomanagement werkt alleen als het geïntegreerd is in alle werkprocessen van de organisatie. Dat kan alleen bereikt worden als risico's regelmatig op de agenda staan. Maak lijnmanagers verantwoordelijk voor risicomanagement door afspraken met ze te maken over uw risicobereidheid. Lijnmanagers zijn verantwoordelijk voor de maatregelen en rapportage daarover.

4 Risicomanagement is onderdeel van de besluitvorming

Risicomanagement is onderdeel van alle besluiten en risicomanagement is erg belangrijk.

Ik maak medewerkers mede-eigenaar van het risicoproces op het vlak van informatieveiligheid en ik maak informatiebeveiliging onderwerp van alle overlegstructuren. Ik draag er zorg voor dat besluiten ten aanzien van de omgang met risico's expliciet genomen en vastgelegd worden. Ik laat risicomanagement naadloos aansluiten op de strategische en beleidsmatige doelstellingen van de organisatie. Op deze wijze bied ik een duidelijk kader waarbinnen de medewerkers kunnen opereren.

Toelichting

U kunt als directeur alleen de juiste richting aangeven als informatie u bereikt. Door dreigingen en risico's mee te nemen in de vragen die u stelt aan uw managers kunt u er in uw beslissingen ook rekening mee houden. Zo kunt u bijsturen voordat risico's manifest worden en escalatie voorkomen.

5 Informatiebeveiliging behoeft ook aandacht in (keten)samenwerking

Het risicomanagementproces is aangepast en staat in verhouding tot de externe en interne context van de organisatie die verband houdt met haar doelstellingen.

Ik zorg dat ik de risico's ken die een gevaar vormen voor de informatievoorziening van de bedrijfsvoering van Senzer en ik anticipeer op risico's die voortkomen uit het werken in ketens en ik houd rekening met de complexiteit, de onzekerheid en ambiguïteit in de samenwerking met anderen. Bij samenwerken of uitbesteden van (delen) van de organisatie of processen zorg ik ervoor dat de risico's in kaart gebracht zijn, verantwoordelijkheden verdeeld en dat de juiste maatregelen getroffen worden.

Toelichting

Het risicomanagementproces moet passen bij de organisatie en ondersteunen aan de organisatiedoelstellingen. De keten is zo sterk als de zwakste schakel. Senzer dient met ketenpartners en leveranciers regelmatig het gesprek te voeren over risico's en de maatregelen die ervoor zorgen dat de risico's tot een acceptabel niveau worden teruggebracht.

6 Informatiebeveiliging is een proces

Risico's kunnen ontstaan, veranderen of verdwijnen als de externe en interne context van een organisatie verandert. Risicomanagement detecteert en anticipeert op die veranderingen en gebeurtenissen op een gepaste en tijdige manier.
Ik zorg ervoor dat risicomanagement cyclisch is en daarmee kan ik reageren op veranderingen en toekomstgericht sturen. Het staat daarom regelmatig op de agenda.
Toelichting
Risicomanagement moet een cyclisch, iteratief en terugkerend proces zijn, want dreigingen veranderen, doelstellingen veranderen, de omgeving verandert en wetgeving verandert. Indien u in uw risicomanagement geen rekening houdt met een veranderende omgeving, dan zijn uw maatregelen op termijn wellicht niet doeltreffend of doelmatig.
7 Informatiebeveiliging kost geld
Risico's moeten behandeld worden en er zijn vele manieren om veiligheid te realiseren, maar aan alle zijn kosten verbonden.
Ik zorg ervoor dat er voldoende middelen beschikbaar zijn om de onderkende risico's op een adequate manier te behandelen. Als gebleken is dat een risico een bedreiging is voor de organisatiedoelstellingen en er maatregelen genomen moeten worden, dan zorg ik er ook voor dat de middelen beschikbaar zijn om deze maatregelen uit te voeren.
Toelichting
Risico's kunt u ontwijken, mitigeren, overdragen of wegnemen door het nemen van preventieve-, repressieve- en/of correctieve maatregelen. Welke strategie u ook kiest, ze kosten allemaal middelen in termen van tijd en geld. Voor maatregelen kan derhalve een kosten-batenanalyse worden gemaakt.
8 Onzekerheid dient te worden ingecalculeerd
De input voor risicomanagement is gebaseerd op historische en actuele informatie, evenals op toekomstige verwachtingen. Risicomanagement houdt expliciet rekening met eventuele beperkingen en onzekerheden die aan dergelijke informatie en verwachtingen zijn verbonden. Informatie moet tijdig, duidelijk en beschikbaar zijn voor relevante belanghebbenden.
Risicomanagement is gebaseerd op de best beschikbare informatie vanuit mijn organisatie en vanuit mijn samenwerkingen. Ik zorg ervoor dat alle belanghebbenden op een gestructureerde en voorspelbare wijze informatie delen die bijdraagt aan risicomanagement.
Toelichting
Zonder goede informatie kunt u geen goede risico-inschattingen en besluiten nemen. Zonder goede en tijdige informatie bent u niet bekend met de risico's die uw organisatie loopt.
9 Verbetering komt voort uit leren en ervaring
Risicobeheer wordt voortdurend verbeterd door leren en ervaring.
Door mijn inzet zorg ik ervoor dat risicogestuurd werken doorontwikkeld wordt. Ik reflecteer op ervaringen en ik nodig medewerkers uit tot het delen van ervaringen met betrekking tot de risico's die de informatievoorziening bedreigen. Ik zorg ervoor dat de organisatie kan leren van incidenten en dat de organisatie leert te ontdekken wat wel en wat niet werkt.
Toelichting
Risicomanagement gedijt het beste in een organisatie die leert van ervaringen en op basis hiervan verbeteringen doorvoert. Hoe goed u uw informatiehuishouding ook beveiligt, incidenten zullen altijd voorkomen. Door te zoeken naar verbeterpunten en de wil om te leren bouwt u doorlopend aan het verhogen van uw digitale weerbaarheid.
10 Het bestuur/management controleert en evalueert
Risicomanagement is het controleren en evalueren van resultaten, evenals het nemen van eindverantwoordelijkheid en het doorhakken van lastige knopen.
Ik geef opdracht om de werking van risicomanagement binnen mijn organisatie op effectiviteit en efficiency te (laten) controleren. Naast managementrapportages zijn (externe) controles de manier om te weten te komen of en hoe het beleid in de praktijk uitwerkt. Als bestuurder weeg ik goed geïnformeerd risico's en belangen af en neem ik mijn verantwoordelijkheid om knopen door te hakken.
Toelichting
Controle is belangrijk om goed inzicht te krijgen in de mate waarin het informatiebeveiligingsbeleid en risicomanagement ingebed zijn in de organisatie. Naast verslagen en managementrapportages zijn incidenten, en dan vooral de manier waarop ze afgewikkeld worden, een goede graadmeter om te zien hoe de organisatie omgaat met het onderwerp. Medewerkers kunnen erop vertrouwen dat besluiten op directieniveau genomen worden, wanneer de situatie daar om vraagt.

[1] De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.