gemeente Tholen

GEMEENTEBLAD

Officiële uitgave van de gemeente Tholen

Nr. 53280

2 februari

2024

Strategisch Gemeentelijk Informatiebeveiligings- en privacy beleid gemeente Tholen 2024 tot 2027

1. Inleiding

Deze beleidsnota beschrijft het strategisch informatiebeveiligings- en privacy beleid (IB&P beleid) voor de jaren 2024 tot 2027 en vervangt het in 2019 vastgestelde 'Gemeentelijk Informatiebeveiligingsbeleid 2020-2023'.
Dit beleid is richtinggevend en kaderstellend voor onderwerp-specifieke beleidsdocumenten voor informatiebeveiliging en privacy op tactisch niveau en werkinstructies op operationeel niveau.

Met dit 'Strategisch Gemeentelijk Informatiebeveiliging- en Privacybeleid 2024-2027 zet de gemeente een volgende stap om de beveiliging van persoonsgegevens en andere informatie binnen de gemeente 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 (BIO) (zie bijlage A) en het VNG Borgingsproduct AVG versie 3.0. De principes die zijn gehanteerd bij het opstellen van dit strategisch beleid, zijn gebaseerd op de 10 principes voor informatiebeveiliging zoals uitgewerkt door de VNG en de beginselen uit de AVG voor het verwerken van persoonsgegevens, zie hoofdstuk 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. Tactische en operationele aspecten van informatiebeveiliging en privacy worden verder uitgewerkt en geconcretiseerd in afzonderlijke informatiebeveiligings- en privacy plannen. Dit wordt gedaan op basis van input van de teamleiders, de Chief Information Security Officers (CISO), de privacy functionarissen (Privacy Officer (PO) en Functionaris Gegevensbescherming (FG)), het dreigingsbeeld Nederlandse gemeenten van de IBD en de uitkomsten van risicoanalyses en DPIA's. Hoofdstuk 3 beschrijft 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 (persoons)gegevens en andere informatie.
Het informatiebeveiligingsbeleid geldt voor alle processen van de gemeente 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 en heeft betrekking op het politieke bestuur, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

1.3 Privacy & Gegevensbescherming (AVG)

De gemeente werkt met (persoons)gegevens van inwoners, ondernemers, medewerkers en (keten)partners. Deze gegevens verzamelt de gemeente voor het goed kunnen uitvoeren van de gemeentelijke wettelijke taken. Denk hierbij onder andere aan taken in het sociaal domein, openbare orde en veiligheidsdomein of voor burgerzaken. Om als gemeente deze taken goed uit te voeren zijn persoonsgegevens noodzakelijk.

Bij de omgang met persoonsgegevens van inwoners en personeel hebben gemeenten een grote verantwoordelijkheid. Privacy is een essentieel en complex vraagstuk. Dit komt onder andere door de toenemende digitalisering van de samenleving en dienstverlening van gemeenten, de decentralisatie van overheidstaken naar gemeenten, de gegevensuitwisseling met (keten)partners, de technische mogelijkheden en veranderende wetgeving. Privacy raakt de hele gemeentelijke organisatie en verdient, samen met informatiebeveiliging, continu aandacht. De inwoner moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met deze persoonsgegevens omgaat.

1.4 Ambitie en visie

1.4.1 Visie

De gemeente Tholen streeft naar een veilige en vertrouwelijke informatievoorziening waarin de bescherming van informatie en privacy centraal staat. De visie van de gemeente Tholen is gebaseerd op het

idee dat elke gebruiker van de informatievoorzieningen (intern en extern) moet kunnen rekenen op een robuuste, proactieve en betrouwbare bescherming. In het licht van toenemende cyberdreigingen en technologische ontwikkelingen erkent de gemeente Tholen de noodzaak te streven naar continue verbetering van de informatiebeveiliging om te kunnen blijven anticiperen op nieuwe risico's en adequaat te kunnen reageren op incidenten. De betekenis van informatiebeveiliging gaat voor de gemeente Tholen dan ook verder dan het naleven van regelgeving alleen; het behoort een fundament te zijn en daarmee een onlosmakelijk onderdeel van de organisatie.

1.4.2 Ambitie

De ambitie van de gemeente Tholen is om te streven naar voortdurende verbetering van de informatiebeveiliging en bescherming van privacy, om te kunnen blijven anticiperen op bestaande en nieuwe dreigingen. Daarbij zet de gemeente Tholen in op continue educatie en bewustwording om een cultuur van veiligheid te bevorderen binnen de gemeentelijke organisatie en belanghebbenden. De gemeente maakt hierbij keuzes over de prioritering en fasering van de implementatie van maatregelen, op basis van een steeds terugkerende risicoafwegingen. De insteek van dit risicomanagement is enerzijds dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging en privacy, en anderzijds dat er een vorm van implementatie plaatsvindt die rekening houdt met het veranderen implementatievermogen van de gemeentelijke organisatie. Over de resultaten legt de gemeente ieder jaar via ENSIA (zie www.ensia.nl) verantwoording af aan de gemeenteraad en het Rijk.

2. Strategisch beleid

2.1 Strategische doelen

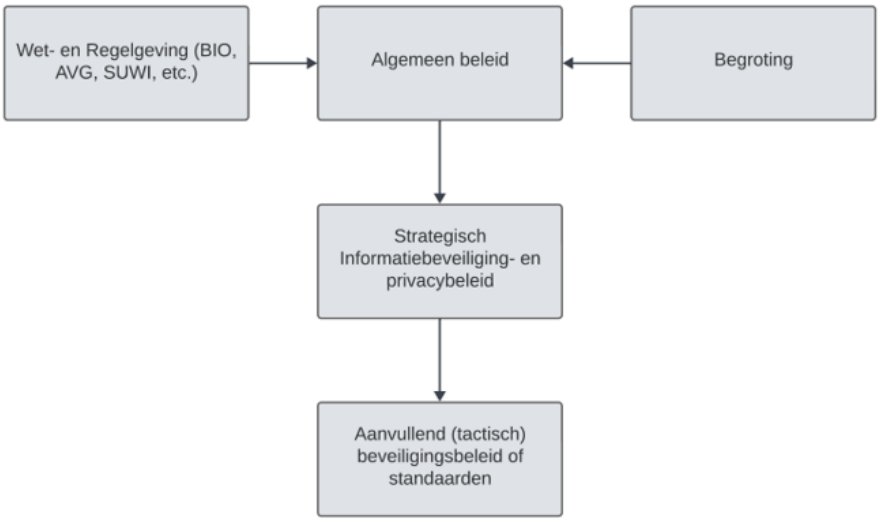
Het doel van deze beleidsnota is om op strategisch niveau richting te geven aan de ambtelijke organisatie en de onderliggende tactische plannen op het gebied van informatiebeveiliging- en privacy voor de jaren 2024 tot 2027.
De uitwerking van dit beleid in concrete maatregelen en activiteiten vindt plaats in een jaarlijks bij te stellen informatiebeveiligings- en privacy plan. Het strategisch beleid op informatiebeveiliging en privacy biedt ondersteuning aan het bestuur, het management en de organisatie bij de sturing op en het beheer van informatieveiligheid en privacy.

De strategische doelen van het IB&P beleid zijn:

- Het managen van de informatiebeveiliging.
- Adequate bescherming van bedrijfsmiddelen en persoonsgegevens.
- Het sturen op en toepassen van dataminimalisatie.
- Het minimaliseren van risico’s van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen van (kritieke) bedrijfsprocessen.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.
- Voldoen aan de wettelijke verplichtingen voortvloeiend uit de AVG en dit op ieder moment met bewijs kunnen aantonen.
- Het waarborgen van de naleving van dit beleid.

2.2 Plaats van het strategisch beleid

Deze beleidsnota beschrijft op strategisch niveau het informatiebeveiligings- en privacy beleid. Het strategisch beleid wordt gebruikt om de basis te leggen voor de tactische beleidsplannen en geeft daarmee richting voor de verdere invulling van informatiebeveiliging en privacy op tactisch en operationeel niveau.



Figuur 1 Visualisering en indruk van de positie van het strategisch beleid.

2.3 10 principes
De 10 principes voor informatiebeveiliging zijn een bestuurlijke aanvulling op het normenkader BIO en gaan over de waarden die de bestuurder zichzelf oplegt. De principes zijn als volgt:

1. Bestuurders bevorderen 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. Het bestuur controleert en evalueert.

De principes gaan vooral over de rol van het bestuur bij het borgen van informatiebeveiliging in de gemeentelijke organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de gemeentelijke processen, dan kan dit directe gevolgen hebben voor inwoners, ondernemers en partners van de gemeente. Daarmee is het onderwerp informatiebeveiliging nadrukkelijk gewenst op de bestuurstafel.

2.4 Ontwikkelingen
De ontwikkelingen die van belang zijn voor de actualisering van het IB&P beleid zijn de volgende:

2.4.1 Regionale samenwerking

- ***Werken onder architectuur***
  Het werken onder architectuur is van belang om (ICT) oplossingen op het gebied van informatiebeveiliging en privacy optimaal beter op elkaar af te stemmen en te laten aansluiten bij de behoeften van de deelnemers in het samenwerkingsverband ICT-WBW.
- ***Zeeuwse norm***
  De Zeeuwse overheid kan door samenwerking haar weerbaarheid versterken met als doel te voorkomen dat er misbruik of oneigenlijk gebruik wordt gemaakt van de Zeeuwse overheid. De thema's en ambities die de Zeeuwse overheden hiervoor nastreven zijn vastgelegd in de Zeeuwse norm weerbare overheid.

2.4.2 De BIO

De BIO (Baseline Informatiebeveiliging Overheid) is het normenkader voor de gehele overheid. De werkwijze van deze BIO is gericht op risicomanagement. Dat wil zeggen dat de teamleiders nu meer dan vroeger moeten werken volgens de aanpak van de ISO 27001 en daarbij is risicomanagement leidend. 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.

2.4.3 Network and Information Security Directive (NIS2)
De Network and Information Security Directive (NIS2-richtlijn) is gericht op versterking van de digitale en economische weerbaarheid van Europese lidstaten. Gemeenten gelden hierbij als 'essentiële entiteit'. De NIS2-richtlijn richt zich op digitale (cyber) risico's voor netwerk- en informatiesystemen. NIS2 kent een aantal verplichtingen: zorgplicht, meldplicht, registratieplicht en toezicht.

2.4.4 De AVG
Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds digitaler wordende overheid maakt het zorgvuldig omgaan met persoonsgegevens steeds complexer en noodzakelijker. De gemeente Tholen is zich hiervan bewust en wil daarom met dit beleid aangeven hoe in algemene zin invulling wordt gegeven aan nationale en Europese wet- en regelgeving op het gebied van privacy, waaronder de Algemene Verordening Gegevensbescherming (AVG).

2.4.5 De WPG
De gemeente heeft buitengewoon opsporingsambtenaren (BOA) in dienst. Zij verwerken naast gegevens die onder de AVG vallen ook gegevens die vallen onder de wet Politiegegevens (WPG). Hiervoor moet de gemeente beleid en samenhangende procedures hebben ingeregeld die betrekking hebben op toegangsrechten, autorisaties, data classificatie, risico-inschatting, registratie en logging, meldplicht en documentatieplicht.

2.4.6 Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten
Het Dreigingsbeeld Informatiebeveiliging Nederlandse Gemeenten van de Informatiebeveiligingsdienst (IBD) geeft zicht op incidenten en factoren uit het verleden, aangevuld met een verwachting voor het heden en de nabije toekomst. Dit dreigingsbeeld wordt gebruikt om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.4.7 Beveiligingsadviezen Nationaal Cyber Security Centrum (NCSC)
Beveiligingsadviezen die door het NCSC worden gepubliceerd naar aanleiding van een recent gevonden kwetsbaarheid of geconstateerde dreiging. Beveiligingsadviezen beschrijven de mogelijke gevolgen en mogelijke oplossingen van een kwetsbaarheid of dreiging.

2.4.8 Informatie uit incidenten, inbreuken op de beveiliging en datalekken
De gemeente gebruikt naast het hierboven genoemde dreigingsbeeld ook systemen waarin incidenten worden vastgelegd. Deze systemen geven ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.5 Standaarden informatiebeveiliging
De BIO is gebaseerd op de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017. De maatregelen worden op basis van best practices bij (lokale) overheden en NEN-ISO/IEC 27002:2017 genomen. Voor de ondersteuning van gemeenten bij het formuleren en realiseren van hun informatiebeveiligingsbeleid heeft de interbestuurlijke werkgroep Normatiek[1] in 2018 de Baseline Informatiebeveiliging Overheid (BIO) uitgebracht, afgeleid van beide NEN-normen. Deze BIO bestaat uit een baseline met verschillende niveaus van beveiligen. De inhoud en structuur van deze beleidsnota is afgestemd op die van de BIO. Ook het Informatiebeveiligings- en privacyplan zal deze structuur volgen.
Binnen de gemeente wordt naast ICT ook Operationele Technologie (OT) ingezet. Met OT worden systemen bedoeld voor de besturing van apparaten voor middel van Proces Automatisering (PA). Het beveiligingsbeleid van de gemeente is ook voor de bescherming van PA en dit beleid betreft dan ook beleidsteams die zich met PA bezig houden.[2] Voor de bescherming van PA gebruikt de gemeente de Cybersecurity Implementatie Richtlijn (CSIR).[3]

2.6 Scope informatiebeveiliging en privacy
De scope van deze beleidsnota omvat alle gemeentelijke processen, onderliggende informatiesystemen, procesautomatisering, informatie en gegevens van de gemeente en externe partijen (bijvoorbeeld politie), het gebruik daarvan door medewerkers en (keten)partners in de meest brede zin van het woord, ongeacht locatie, tijdstip en gebruikte apparatuur.

1) *De Interbestuurlijke werkgroep Normatiek bestaat uit vertegenwoordigers van bijvoorbeeld VNG en de IBD, maar ook waterschappen, provincies en het rijk.*
2) https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs/BIACS+2022.pdf
3) https://www.cert-wm.nl/csir

Dit strategisch gemeentelijke Informatiebeveiligingsbeleid is een algemene basis en dekt tevens aanvullende beveiligingseisen uit wetgeving af zoals voor de AVG, UAVG, Wpg, BRP, PNIK/PUN, DigiD en SUWI. Voor bepaalde kerntaken gelden op grond van deze en wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen (bijvoorbeeld SUWI, gemeentelijke basisregistraties en DigiD met norm B.01 eisen). Deze worden in aanvullende beleidsdocumenten geformuleerd.

Bewust wordt in het strategisch beleid geen uitputtend overzicht van onderliggende documenten opgenomen. In de onderliggende documenten wordt de link naar het strategisch beleid gelegd.

2.7 Uitgangspunten
Het bestuur, Het DT en het teammanagement spelen een cruciale rol bij het uitvoeren van dit strategische IB&P beleid. Het teammanagement maakt een inschatting van het belang dat de verschillende delen van de informatievoorziening voor de gemeente heeft, de (privacy) risico's die de gemeente hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

Het gehele gemeentelijke management geeft richting aan informatiebeveiliging en privacy en laat zien dat zij informatiebeveiliging en privacybescherming ondersteunt en zich hierbij betrokken voelt. Dit gebeurt door het actief uitdragen en handhaven van het IB&P beleid van en voor de hele gemeente. Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen, procesautomatisering en (persoons)gegevens(verzamelingen). Dit beleid is in lijn met het algemene beleid van de gemeente en de relevante landelijke en Europese wet- en regelgeving.

2.7.1 Belangrijkste uitgangspunten
De belangrijkste uitgangspunten van het beleid zijn:
- De uitvoering van de informatiebeveiliging en privacybescherming is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de gemeente Tholen hebben een interne (proces)eigenaar die de vertrouwelijkheid, privacyeisen en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie en ketens van informatiesystemen ligt dan ook bij de eigenaar van de informatie;
- Door periodieke controle, planning én coördinatie wordt de kwaliteit van de informatievoorziening en privacy verankerd binnen de organisatie. Het IB&P beleid vormt samen met de tactische informatiebeveiliging- en privacyplannen het fundament onder een betrouwbare informatievoorziening en privacy bescherming. In deze plannen wordt de betrouwbaarheid van de informatievoorziening en privacy organisatiebreed benaderd. De plannen worden periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en risicoanalyses voor informatiebeveiliging en privacy;
- Informatiebeveiliging en privacybescherming is een continu verbeterproces. 'Plan, do, check en act' vormen samen het managementsysteem van informatiebeveiliging en privacybescherming.
- De gemeente stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen en te voldoen aan de privacy eisen volgens de wijze zoals gesteld in dit beleid;
- Regels en verantwoordelijkheden voor het IB&P beleid dienen te worden vastgelegd en vastgesteld;
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig (persoons)gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken;
- Vastgestelde beleidsstukken en uitwerkingen daarvan (bijv. procedures, standaarden en werkinstructies) worden centraal beheerd in het managementsysteem voor informatiebeveiliging en privacybescherming.
- Tijdens Planning & Control-gesprekken dient er aandacht te zijn voor de informatiebeveiliging en privacy n.a.v. de rapportage van de CISO en of de FG. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- Hoewel de basiskernregistraties (zoals BRP, PUN/PNIK, SUWI, BAG, BGT) en toekomstige basisregistraties belangrijk zijn in het kader van informatiebeveiliging, krijgen zij niet meer of minder voorrang dan andere (primaire) processen binnen de gemeente. Het samenspel van alle processen binnen de bedrijfsvoering is belangrijk voor de missie en de visie van de gemeente en het behalen van de doelen die zijn gesteld.
- Alle medewerkers van de gemeente worden getraind in het gebruik van beveiligingsprocedures.
- Alle medewerkers hebben een minimale basiskennis van de privacywetgeving en weten deze bewust toe te passen in hun dagelijks werk. Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie. Een bewustwordingsprogramma draagt eraan bij dat medewerkers hiertoe in staat zijn.

- Informatiebeveiliging en privacybescherming maakt deel uit van de ontwikkelingsbeoordelingssystematiek en wordt besproken tussen de manager en de medewerker.

2.7.2 Randvoorwaarden

Randvoorwaarden zijn de eisen waaraan moet worden voldaan om het strategisch IB&P beleid uit te kunnen voeren. Belangrijke randvoorwaarden zijn:

- De informatiebeveiliging en privacy eisen maken deel uit van afspraken met ketenpartners, leveranciers en gemeenschappelijke regelingen en worden periodiek geëvalueerd/gecontroleerd.
- Kennis en bewustzijn van informatiebeveiliging en privacybescherming en omgaan met persoonsgegevens binnen de organisatie dienen actief bevorderd en geborgd te worden.
- Jaarlijks wordt het informatiebeveiligings- en privacyplan opgesteld onder leiding van het hoofd informatiebeveiliging, gebaseerd op:
  - Dit IB&P beleid;
  - De uitkomsten van de jaarlijkse Eenduidige Normatiek Single Information Audit (ENSIA);
  - Andere audit resultaten;
  - Het dreigingsbeeld gemeenten van de IBD;
  - Uitkomsten risico-analyses en DPIA's;
  - De door de teamleiders ingebrachte onderwerpen voor de informatievoorziening waarvoor zij verantwoordelijk zijn, bijvoorbeeld als uitkomst van een risicoanalyse of een privacy analyse (DPIA).

- Om uitvoering te kunnen geven aan dit strategisch beleid en het IB&P plan worden voldoende financiële middelen en uitvoeringscapaciteit ter beschikking gesteld.

3. Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging en privacy op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij het in de bedrijfsvoering bekende 'Three Lines Model' (eerder bekend als 'Three Lines of Defense').

1. In dit model is het lijnmanagement in de eerste lijn verantwoordelijk voor het realiseren van informatiebeveiliging en privacy binnen de eigen processen;
2. In de tweede lijn bewaken de CISO, security officers en Privacy Officers, of het lijnmanagement zijn verantwoordelijkheden ook daadwerkelijk neemt. Zij adviseren en ondersteunen het lijnmanagement met het coördineren van maatregelen;
3. In de derde lijn wordt het geheel door een (interne) auditor en/of FG van een objectief oordeel voorzien met mogelijkheden tot verbetering, hier is ook de ENSIA coördinator gepositioneerd.

3.1 college van B&W

De eindverantwoordelijkheid ten aanzien van alle informatie en informatiesystemen ligt bij het college van B&W, de Burgemeester (bij taken in het kader van handhaven Openbare Orde en Veiligheid) of de gemeenteraad. De eindverantwoordelijkheden zijn benoemd in het register van verwerkingen. Dit geldt voor alle gemeentelijke informatiesystemen ongeacht waar deze worden gehost.

3.2 Directieteam (DT)

Het DT zorgt dat alle (persoons)gegevens, processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een teamleider. Het DT zorgt dat de teamleiders zich verantwoorden over de beveiliging en bescherming van de privacy van de (persoons)gegevens of andere informatie die onder hen berust. Het DT zorgt dat de eindverantwoordelijke portefeuillehouders binnen het college gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging en privacybescherming een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan het college zich ook verantwoorden naar de raad.

Het DT stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. Het DT draagt zorg voor het uitwerken van tactische informatiebeveiligings- en privacybeleidsonderwerpen en laat zich hierin bijstaan door de CISO en PO van de gemeente. Het DT autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging en privacybescherming wordt in de gemeente Tholen gezien als een integraal onderdeel van risicomanagement.

3.2.1 Taken en Verantwoordelijkheden van het DT

- Het DT stelt jaarlijks de tactische informatiebeveiligings- en privacyplannen vast.
- Het DT is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.

- Het DT is verantwoordelijk voor het vragen om informatie bij de teamleiders en ziet erop toe dat de teamleiders adequate maatregelen genomen hebben voor de bescherming van de (persoons)gegevens, informatiesystemen en procesautomatiseringsystemen die onder hun verantwoordelijkheid valt.

3.3 Teamleiders
Informatiebeveiliging en privacy valt onder de verantwoordelijkheden van alle teammanagers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. De verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, (persoons)gegevens, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Teamleiders rapporteren aan de het DT over de door hen tactisch en operationeel uitgevoerde informatiebeveiligings- en privacybeschermende activiteiten. Afstemming met de teams over de inhoudelijke aanpak vindt plaats door minimaal jaarlijks het onderwerp informatiebeveiliging en privacy te bespreken in het bedrijfsvoeringsoverleg.

3.3.1 Taken en Verantwoordelijkheden van de teamleiders
- De teamleiders zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- De teamleiders zijn verantwoordelijk voor de borging van de AVG binnen de processen waarvoor zij verantwoordelijk zijn en het bijbehorende verwerkingsregister.
- De teamleiders zijn verantwoordelijk voor het oefenen met informatiebeveiligings- en privacy incidenten en bedrijfscontinuïteit.
- Teamleiders dienen erop toe te zien dat de controle op het verwerken van persoonsgegevens regelmatig wordt uitgevoerd, zodat zij kunnen vaststellen dat alleen rechthebbende ambtenaren de juiste persoonsgegevens ingezien en verwerkt hebben.
- De beveiligingsmaatregelen worden bepaald op basis van risicomanagement. Teamleiders voeren quickscans informatiebeveiliging uit op basis van de BIO en bij verwerken van persoonsgegevens tevens (Pre-)DPIA's op basis van de AVG, om deze risico-afwegingen te kunnen maken.
- Teamleiders zijn verantwoordelijk voor het voldoen aan wet- en regelgeving die op hun processen van toepassing zijn en geven invulling aan de rollen die binnen die wet- en regelgeving bedacht is;
- Teamleiders dragen binnen de eigen teams het IB&P beleid uit en de daaraan gerelateerde procedures;
- Teamleiders zijn verantwoordelijk voor het vroegtijdig signaleren van de voornaamste (privacy)bedreigingen waaraan bedrijfsinformatie is blootgesteld;
- Teamleiders betrekken vroegtijdig de CISO en de PO bij nieuwe of gewijzigde processen, functionaliteiten en applicaties en leveren input voor wijzigingen op maatregelen en procedures;
- Teamleiders voeren risicoanalyses en (pre-)DPIA's uit voor de processen waar zij verantwoordelijk voor zijn;
- Teamleiders bespreken beveiligingsincidenten en privacy inbreuken en de consequenties die dit moet hebben voor beleid en maatregelen.

3.4 Chief Information Security Officer (CISO)
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 hierover rechtstreeks aan het DT, voorafgaand aan de P&C-gesprekken.

3.5 Functionaris gegevensbescherming (FG)
De Functionaris voor Gegevensbescherming (FG) is verantwoordelijk voor het intern onafhankelijk toezien op en adviseren van het college van B&W over de juiste en zorgvuldige omgang met persoonsgegevens zoals de AVG voorschrijft. De FG brengt een jaarverslag uit waarin hij zijn bevindingen en aanbevelingen vastlegt.
Het DT en de teamleiders stellen proactief informatie over de bescherming van persoonsgegevens ter beschikking aan de functionaris gegevensbescherming. Desgevraagd verstrekken zij aanvullende informatie aan de functionaris gegevensbescherming.

3.6 Controle en verantwoording
Dit Strategisch IB&P Beleid is een verantwoordelijkheid van het bestuur van de gemeente Tholen. De bestuurders en directeur(en) van de gemeente Tholen werken volgens de 10 principes voor informatiebeveiliging en de beginselen voor het verwerken van persoonsgegevens. Zij geven sturing aan het onderwerp informatiebeveiliging en privacy door het geven van voorbeeldgedrag en het vragen om informatie. Het DT is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging en privacy aan respectievelijke portefeuillehouders. Het DT rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

3.6.1 ENSIA
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dit betekent dat er een ENSIA-coördinator is aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teamleiders. De teamleiders leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten. Via ENSIA verantwoordt de gemeente zich ook aan de toezichthouders van de stelsels waaronder DIGID/BAG/SUWI.

3.6.2 AVG
Burgemeesters en wethouders leggen verantwoording af aan de gemeenteraad over het naleven van de privacywet (AVG).

Middels deze verantwoording worden het bestuur van de gemeente Tholen en de raad geïnformeerd. De betrokkenheid van het bestuur is essentieel, en laat zien dat de gemeente Tholen informatiebeveiliging en privacybescherming serieus neemt en het een onderdeel laat zijn van de ambities om informatie van haar inwoners adequaat te beschermen.

Vastgesteld op d.d. 12 december 2023

Burgemeester en wethouders van de gemeente Tholen,

de secretaris,
w.g. J.K. Fraanje

de burgemeester,
w.g. M.L.P. Sijbers

Bijlage A Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) is geheel gestructureerd volgens NEN-ISO/IEC 27001:2017, bijlage A en NEN-ISO/IEC 27002:2017. Het Forum Standaardisatie heeft deze normen opgenomen in de 'pas toe-of-leg uit'- lijst met verplichte standaarden voor de publieke sector, volgens het comply or explain principe. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.

De BIO beschrijft de invulling van de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 voor de overheid. Met klem vermeldt zij dat de BIO deze normen niet vervangt.
In de BIO hebben specifieke overheidsmaatregelen de tekstkleur groen. NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017 beschrijven details voor implementatie (implementatierichtlijnen) en eisen voor de procesinrichting (o.a. het ISMS uit NEN-ISO/IEC 27001:2017). Die documenten geven dus de details voor de toepassing, die niet in de BIO zijn beschreven en die nodig blijven voor een goede implementatie van de BIO.

Wijzigingshistorie:

Versie	Datum	Opmerkingen
0.1	11-6-2017	Aanpassingen van BIR 2017 versie 0.6
0.2	11-7-2017	Omschrijven naar ISO 27001 aanpak (hoofdstuk 4), samenvoegen hoofdstuk 3 en 4, ISO 27001 aanpak in hoofdstuk 4, tekstuele aanpassing controls (must/should)
0.3		Verschillende opmerkingen verwerkt
0.4	10-10-2017	Diverse opmerkingen verwerkt van leden, splitsen baseline in 2 delen, analoog aan de BIR2017
0.5	20-10-2017	Hoofdstuk 4 toegevoegd in deel 2 om ISMS te borgen als control / maatregel
0.6	20-02-2018	Verder aanscherping als gevolg van review commentaar, maken apart addendum voor specifieke Rijks zaken
0.7	02-05-2018	Aanpassing als gevolg van commentaar BZK, 3 delen samengevoegd, alignment met de BIR2017 bewerkstelligd, totale herziening BIO, ISMS-deel als gevolg van commentaar laten vervallen
0.8	21-05-2018	Verdere aanpassingen als gevolg van commentaar en opmerkingen door gemeenten, waterschappen en provincies
0.9	25-05-2018	Verdere aanpassingen als gevolg van commentaar en verspreiding concept onder leden werkgroep Normatiek
1.0	01-06-2018	Laatste wijzigingen en commentaar NCSC en BZK verwerkt
1.01	11-10-2018	Wijzigingen uit de community, opmerkingen Forum Standaardisatie en kleine typo's aangepast, copyright NEN toegevoegd
1.02	01-11-2018	Aanwijzing NEN, jaartal ISO veranderd van 2013 naar 2017, inhoudelijk geen wijzigingen, de 2017 versie is ontstaan als gevolg van een Europees besluit.
1.03	13-03-2019	Aangepaste passage over gebruik van de NEN-ISO/IEC 27001:2017 en NEN-ISO/IEC 27002:2017. Deze passage en de wijzigingshistorie verplaatst van pagina 4 naar pagina 2.
1.04	04-11-2019	Aanpassingen van BIO 1.03 naar 1.04 als gevolg van onderhoudsronde BIO 2019. Betreft correctie van feitelijke onjuistheden en splitsing / aanpassing / verplaatsing van bepaalde maatregelen.
1.04zv	17-06-2020	Verwijzingen naar handreikingen eruit verwijderd. Deze worden opgenomen in een apart document dat op de BIO-overheid-portaal wordt gepubliceerd en onderhouden

Voorwoord

Informatiebeveiliging vormt een belangrijk kwaliteitsaspect van de informatievoorziening van de overheid. Het beveiligen van informatie is echter geen eenmalige zaak, maar een proces waarbij steeds de Plan-Do-Check-Act cyclus wordt doorlopen. Het doorlopen van dit proces is een verantwoordelijkheid van het lijnmanagement. Om te voorkomen dat informatie en informatiesystemen te licht of te zwaar worden beveiligd, vormt risicomanagement een belangrijk onderdeel in dit proces.

De eerste stap in het beveiligingsproces is het maken van een risicoafweging. Daarbij wordt een inschatting gemaakt van mogelijke schade als informatiesystemen (tijdelijk) niet beschikbaar zijn, de informatie niet integer is en/of deze informatie in verkeerde handen valt. Ook wordt een inschatting gemaakt van de dreigingen waartegen de overheid beschermd moet worden. De inschatting van mogelijke schade en dreigingen leidt tot beveiligingseisen om het risico te beperken. Om deze eisen af te dekken worden passende maatregelen getroffen of wordt het (rest)risico geaccepteerd.

De Baseline Informatiebeveiliging Overheid (BIO) helpt het lijnmanagement bij het nemen van zijn verantwoordelijkheid ten aanzien van informatiebeveiliging. Het ingewikkelde proces van risicomanagement wordt met de BIO vereenvoudigd. In de BIO zijn namelijk op basis van de generieke schades en dreigingen voor de overheid standaard basisbeveiligingsniveaus (BBN's) gedefinieerd met bijbehorende beveiligingseisen die moeten worden ingevuld. Per bedrijfsproces bepaalt het lijnmanagement het BBN; de BIO biedt daarvoor een zogenaamde BBN-toets.

In de BIO staat per BBN beschreven aan welke controls uit de ISO 27002 (Code voor Informatiebeveiliging) moet worden voldaan. Bij alle controls dient, op basis van een individuele risicoafweging, bepaald te worden hoe aan de beveiligingsdoelstelling van de control voldaan kan worden. Daarbij zijn de controls, waar van toepassing, gedeeltelijk uitgewerkt in verplichte, concrete overheidsmaatregelen. De controls zijn toebedeeld aan rollen, waarmee de verdeling over verantwoordelijken makkelijker is. Zo kan ook de dienstenleverancier die de expertise heeft, bepalen met welke concrete maatregelen hij de control invult.

Ten slotte moet verantwoording worden afgelegd over de risicoafweging en over de effectieve invulling van de controls. Deze verantwoording is onderdeel van de bestuurlijke verantwoording over de beveiliging van informatiesystemen. De wijze en mate van detail van de verantwoording hangt af van het BBN. Des te hoger het BBN, des te meer detail nodig is in verband met de hogere potentiële impact. Dienstenleveranciers leggen verantwoording af aan hun (gedeelde) opdrachtgever en er wordt verantwoording afgelegd aan de ketenpartners met wie afspraken over de beveiliging van informatie zijn gemaakt. De opdrachtgever ziet erop toe dat de afgenomen diensten in overeenstemming met de gestelde eisen beveiligd zijn; de afnemers van de diensten mogen hierop vertrouwen en worden door de opdrachtgever geïnformeerd over uitzonderingssituaties.

De BIO biedt hiermee de basis om te zorgen dat de beveiliging van informatie(systemen) bij alle bedrijfsonderdelen van de overheid bevorderd wordt. Deze bedrijfsonderdelen kunnen erop vertrouwen dat gegevens die worden verstuurd naar of worden ontvangen van andere onderdelen van de overheid, in lijn met wet- en regelgeving, passend beveiligd zijn. Waar naleving (nog) niet volledig mogelijk is, dienen de bedrijfsonderdelen via een 'explain' de eventuele risico's inzichtelijk te maken aan hun ketenpartners.

De BIO is opgedeeld in twee delen waarbij het eerste deel de achtergrond weergeeft en het tweede deel het daadwerkelijk uit te voeren kader omvat.

Deel 1 Achtergrond BIO

1. Informatiebeveiliging bij de overheid
1.1 Inleiding
Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen[4].

De BIO beoogt zo de beveiliging van informatie(systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie. Daarmee is de BIO ook van toepassing op besturings- en meetprocessen voor zover deze binnen een bestuursorgaan gebruikt worden.

4) Artikel 1 sub a Voorschrift Informatiebeveiliging Rijksdienst 2007, *Stcrt.* 2007, 122/11.

De BIO is van toepassing op de overheid. In verband hiermee is de BIO van toepassing op de volgende bestuursorganen:
- Rijksdienst
- Provincies
- Waterschappen
- Gemeentes

Daarnaast wordt aanbevolen de BIO te verankeren in de taakomschrijving van de overige overheidsorganisaties en organisaties waarmee de overheid publiek-privaat samenwerkt en private samenwerkingen waarbij de overheid de enige aandeelhouder is.

1.2 Informatiebeveiligingskaders en uitgangspunten overheid
De overheid past risicomanagement toe om tot de juiste beveiliging van informatie en informatiesystemen te komen binnen de context van de bedrijfsdoelstellingen. Risicomanagement is het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes[5].

De insteek van risicomanagement in het kader van de BIO is dat er cyclisch en methodisch vanuit een PDCA-cyclus wordt omgegaan met informatiebeveiliging. De overheidslagen kiezen als basis voor deze procesmatige inrichting van risicomanagement en het inrichten van de PDCA-cyclus voor de NEN/ISO 27001:2017[6]. Voor de rijksoverheid vindt nadere specificatie plaats in de algemene voorschriften voor de beveiliging van informatiesystemen: het Beveiligingsvoorschrift Rijksdienst[7] (BVR), het Voorschrift Informatiebeveiliging Rijksdienst[8] (VIR) en het Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie[9] (VIR-BI)

Voor de BIO geldt (op basis van deze documenten van NEN/ISO 27001 en BVR, VIR en VIR-BI) kort samengevat het volgende:
- Een ruime definitie voor een informatiesysteem, namelijk "een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie"[10].
- Het lijnmanagement is verantwoordelijk voor de beveiliging van informatie(systemen).
- Informatiebeveiliging is een cyclisch proces, volgens de Plan-Do-Check-Act cyclus[11].
- Deze Plan-Do-Check-Act cyclus maakt het lijnmanagement verantwoordelijk voor het treffen van maatregelen op basis van risicomanagement.
- De secretaris/algemeen directeur van een organisatie is eindverantwoordelijk[12] voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie[13].
- Het lijnmanagement stelt op basis van een expliciete risicoafweging de betrouwbaarheidseisen voor zijn informatiesystemen vast[14].
- Op basis van de betrouwbaarheidseisen kiest, implementeert en draagt het lijnmanagement de maatregelen uit[15].

De BIO is allereerst een gemeenschappelijk normenkader voor de beveiliging van de informatie(systemen) van de overheid. Daarnaast concretiseert de BIO een aantal normen tot verplichte overheidsmaatregelen:
- op grond van wet- en regelgeving[16];
- vanwege de gemeenschappelijke veiligheid van informatieketens;

5) Artikel 5 lid 2 BVR en Artikel 1 sub d BVR.
6) De NEN/ISO 31000-aanpak wordt gezien als een goed alternatief voor de 27001.
7) Beveiligingsvoorschrift Rijksdienst 2013, *Stcrt.* 2013, 15496.
8) Voorschrift Informatiebeveiliging Rijksdienst 2007, *Stcrt.* 2007, 122/11.
9) Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie 2013, *Stcrt.* 2013, 15497.
10) Artikel 1 sub b VIR.
11) Artikel 4 VIR, ISO 6.1 en 9.1.
12) In sommige organisaties heet de eindverantwoordelijke "bestuursvoorzitter" of "directeur" en moet de term "secretaris/algemeen directeur" als "bestuursvoorzitter" of "directeur" worden gelezen.
13) Artikel 5 lid 2 BVR en Artikel 4 lid 1 BVR.
14) Artikel 4 sub a en sub b VIR, ISO 27001 6.1 en 6.2.
15) Artikel 4 sub a en sub b VIR, ISO 27001 6.1 en 6.2.
16) Zie voor nadere detaillering: Bijlage 1: Wet- en regelgeving.

- omdat deze fundamenteel zijn voor een betrouwbare c.q. professionele informatievoorziening.

De Baseline Informatiebeveiliging Overheid BIO is gebaseerd op de ISO 27002- standaard[17].

1.3 ISO 27002
De ISO 27002 'Code voor Informatiebeveiliging' geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbeteren van informatiebeveiliging binnen een organisatie. Deze standaard is een best practice om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van de ISO 27001-standaard[18]. De ISO 27002 kan dienen als een praktische richtlijn voor het ontwerpen van veiligheidsstandaarden binnen een organisatie en als effectieve methode voor het bereiken van deze veiligheid.

De ISO bestaat uit 114 controls; de term 'control' wordt in de ISO vertaald als een beheersmaatregel[19]. De BIO volgt de opbouw van de ISO 27002 en zijn controls. De controls zijn in de BIO letterlijk[20] overgenomen. Dit vergemakkelijkt afstemming met externe partners of leveranciers. Daarnaast vult de BIO enkele bepalingen uit het VIR inzake PDCA-cyclus en verantwoordelijkheden op een generieke wijze in[21].

1.4 Evaluatie en bijstelling
Door de snelle ontwikkelingen van de techniek verouderen maatregelensets voor informatiebeveiliging snel. De BIO is daarom zo veel mogelijk op een abstractieniveau geschreven waarbij dergelijke wijzigingen en ontwikkelingen een zo klein mogelijke impact hebben op de maatregelen.[22] De BIO beschrijft het wat en niet het hoe. Desondanks kunnen wijzigingen noodzakelijk zijn bij bijvoorbeeld aanpassingen van onderliggende wet- en regelgeving of nieuwe dreigingen en kwetsbaarheden.

Dit document wordt daarom regelmatig in zijn geheel geëvalueerd en indien nodig bijgesteld. Daarnaast wordt specifiek bezien of er wijzigingen en aanvullingen in de maatregelen en de (operationele) handreikingen nodig of gewenst zijn om hiermee de praktische toepasbaarheid te vergroten. Besluiten hierover worden via de bestaande informatiebeveiligingsgremia genomen en door de beheerder van de BIO verwerkt[23].

1.5 Forum Standaardisatie
De overheid volgt de standaarden die op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie[24] (hierna het Forum) staan. De BIO is gebaseerd op de NEN-ISO/IEC 27002:2017 en vanuit de BIO wordt verwezen naar de NEN-ISO/IEC 27001:2017, beide standaarden staan op de 'pas toe of leg uit'-lijst[25] van het Forum. Ook een aantal technische maatregelen uit de BIO staan op de 'pas toe of leg uit'-lijst of op de 'open standaarden'-lijst[26] van het Forum. Deze technische invullingen zijn niet allemaal uitgewerkt in deze BIO. Er is voor gekozen alleen aan te geven of de maatregel ingevuld wordt door een verplichte of open standaard van het Forum. Hierdoor wordt de BIO minder onderhoudsgevoelig.

2. Opzet van de BIO
2.1. Opzet BBN's
Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen. Daarom onderscheidt de BIO drie basisbeveiligingsniveaus (BBN's). Voor

17) NEN-ISO/IEC 27002:2017, (dit is de 27002:2013 met geconsolideerde correctiebladen C1 en C2).
18) De NEN-ISO/IEC 27001-standaard bevat eisen waar het managementsysteem voor informatiebeveiliging aan dient te voldoen. Het is deze norm waartegen wordt geaudit bij certificering. Deze standaard specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's van een organisatie.
19) De Nederlandse versie van ISO 27002 spreekt van beheersmaatregelen. Er zijn echter ook implementatiemaatregelen. Om het onderscheid daartussen makkelijker te maken, hanteert de BIO de Engelse term, namelijk 'controls'. Het gebruik van deze term sluit aan bij de informatiebeveiligingspraktijk.
20) In tegenstelling tot de verschillende oude baselines, zijn de controls dus niet tekstueel aangepast.
21) Met name artikel 4 sub a en sub b van het VIR.
22) Ook de ISO is vanuit dit principe opgesteld.
23) Daartoe is in het OBDO een procedure overeengekomen.
24) Zie ook de website van het Forum Standaardisatie op https://www.forumstandaardisatie.nl
25) Zie ook: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
26) Zie ook: https://www.forumstandaardisatie.nl/open-standaarden/lijst/aanbevolen

BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'. BBN3[27] is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheidslagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is.

De keuze voor een BBN wordt gemaakt door de proceseigenaar en is gebaseerd op risicomanagement. De BIO gaat vergezeld van een methode van risicoafweging, de BBN-toets[28]. In Deel 2 wordt deze methode verder toegelicht[29].

2.2. Controls

Na de BBN-toets doorloopt het lijnmanagement alle toepasselijke controls[30] uit de BIO[31]. Op basis van een risicoafweging wordt bepaald hoe moet worden voldaan aan de gestelde beveiligingsdoelstellingen van de controls. Voor het voldoen aan deze doelstellingen kunnen implementatierichtlijnen uit de ISO 27002, overheidsmaatregelen en/of operationaliseringen in handreikingen worden gebruikt.

Er geldt een hardheidsbepaling: in het geval een control voor een specifiek geval niet van toepassing *kan* zijn, *is* de control niet van toepassing. Dit geldt bijvoorbeeld voor een control die betrekking heeft op een externe koppeling, terwijl het betreffende informatiesysteem geen externe koppeling heeft. De organisatie hoeft zich daar niet over te verantwoorden.

2.3. Implementatierichtlijnen

Iedere control is in de ISO 27002 uitgewerkt in implementatierichtlijnen. Bij het uitvoeren van risicoafwegingen zijn de implementatierichtlijnen zeer nuttig. Ze helpen bij het kiezen van de benodigde beveiligingsmaatregelen. Deze richtlijnen moeten dus worden gezien als voorbeelden hoe de controls uitgewerkt *kunnen* worden in maatregelen; het volgen van deze richtlijnen is niet verplicht.
Deze implementatierichtlijnen zijn niet in de BIO opgenomen, hiervoor wordt verwezen naar de ISO 27002.

2.4. Overheidsmaatregelen

Een deel van de controls is uitgewerkt in verplichte maatregelen, omdat zij:

- voortvloeien uit *wet- en regelgeving*[32]. Het niet treffen van een dergelijke maatregel is dan in strijd met deze externe wet- en regelgeving;
- zo basaal zijn dat zij het *fundament* vormen van een betrouwbare c.q. professionele informatievoorziening;
- dienstbaar zijn aan de beveiliging in een procesketen of netwerk; niet-naleving door een enkele organisatie is per saldo *ineffectief* voor de gehele keten. Het vormt een risico voor alle andere partijen in de keten en leidt bij hen tot extra maatregelen en kosten. Voor de keten als geheel is dit *inefficiënt*. Voor een *generieke dienst* geldt een afweging die analoog is aan het ketenvraagstuk.

De BIO noemt deze verplichte maatregelen 'overheidsmaatregelen'. De overheidsmaatregelen dekken niet de gehele beveiligingsdoelstellingen van de control af. Net als bij de controls geldt hier een hardheidsbepaling: in het geval een maatregel voor een specifiek geval niet van toepassing *kan* zijn, vervalt de verplichting. Dit geldt bijvoorbeeld voor een overheidsmaatregel die betrekking heeft op een externe koppeling, terwijl het betreffende informatiesysteem geen externe koppeling heeft.

Bij een aantal overheidsmaatregelen zijn verwijzingen toegevoegd naar relevante wet- en regelgeving. Deze verwijzingen zijn of overheidsbreed geldend of specifiek toegesneden op een aandachtsgebied (bijvoorbeeld de 'Gedragsregeling voor de digitale werkomgeving') en hebben een verplichtend karakter.

27) De aanvullende eisen die gelden vanaf BBN3 zijn in deze huidige versie van de BIO nog niet nader uitgewerkt.
28) De BBN-toets is geen volwaardige vervanger van de Quickcan BIO of van een andere uitgebreide risicoanalysemethodiek. De BBN-toets zorgt er alleen voor dat eenvoudig het juiste BBN geselecteerd kan worden en dat bepaald kan worden in hoeverre extra eisen noodzakelijk zijn.
29) Gewerkt gaat worden aan een handreiking waarin ten opzichte van de drie BBN-niveaus wisselingen in niveaus voor de aspecten beschikbaarheid, integriteit en vertrouwelijkheid worden aangegeven. Wellicht gaan de controls en maatregelen nog nader gespecificeerd worden naar de drie verschillende aspecten.
30) De Nederlandse versie van ISO 27002 spreekt van beheersmaatregelen. Er zijn echter ook implementatiemaatregelen. Om het onderscheid daartussen makkelijker te maken, hanteert de BIO de Engelse term, namelijk 'controls'. Het gebruik van deze term sluit aan bij de informatiebeveiligingspraktijk.
31) Met uitzondering van twee controls (6.1.4 en 14.2.4) bevat de BIO alle controls uit de ISO 27002.
32) Het gaat dan enkel om de beveiligingseisen die voortvloeien uit wet- en regelgeving. Andere vereisten vallen buiten de scope van de BIO.

2.5. Addendum
De BIO is generiek geschreven en geldig voor alle doelgroepen. Sommige overheidslagen hebben specifieke wet- en regelgeving die alleen gelden binnen die overheidslaag.
Om tegemoet te komen aan de behoefte van deze overheidslagen en deze specifieke wet- en regelgeving niet verloren te laten gaan, is er aan de BIO een addendum toegevoegd. In dit addendum is deze wet- en regelgeving gekoppeld aan de control of maatregel waartoe zij behoren. Het addendum is toegevoegd aan de BIO in deel 3.

2.6. Operationalisering in handreikingen
Om de praktische toepasbaarheid van de BIO te verhogen, wordt de BIO aangevuld met handreikingen. Dit zijn aanbevelingen in het kader van de bedrijfsvoering die geen verplichtend karakter hebben en niet essentieel zijn voor de werking van een stelsel. Een handreiking geeft dus advies hoe bepaalde normen, standaarden, technieken of maatregelen te implementeren of te hanteren zijn. Een handreiking kan meer specifiek zijn toegesneden op een overheidslaag (interdepartementaal, gemeentebreed, etc.) of op een bepaald aandachtsgebied.

In deze BIO zijn geen verwijzingen opgenomen naar handreikingen. Een actueel overzicht met alle verwijzingen wordt geboden in een apart document dat te vinden is op het BIO-overheid portaal.

2.7. Rollen
In het algemeen geldt dat onderdelen van de BIO op verschillende plaatsen in de organisatie worden toegepast op grond van verschillende verantwoordelijkheden en gezagsverhoudingen. De BIO onderscheidt drie (hoofd)rollen: de secretaris/algemeen directeur, de proceseigenaar en de dienstenleverancier. Deze rollen zijn hieronder beschreven vanuit het perspectief van informatiebeveiliging. Er zijn uiteraard meer rollen betrokken bij informatiebeveiliging, zoals toezichthouder en medewerker, maar het gaat hier om de verantwoordelijke voor de uitvoering van de control.

Secretaris/algemeen directeur	Als eindverantwoordelijke voor het beveiligingsbeleid in de organisatie is de secretaris/algemeen directeur verantwoordelijk voor de uitvoering van organisatiebrede vraagstukken ten aanzien van informatiebeveiliging[33]. In de praktijk kan deze rol worden uitgevoerd door bijvoorbeeld de CIO of een directeur Inkoop[34].
Proceseigenaar	Onder de proceseigenaar wordt de lijnmanager verstaan die verantwoordelijk is voor de beveiliging van het betreffende proces / informatiesysteem.
Dienstenleverancier	Bedoeld wordt de dienstenleverancier (bijvoorbeeld SSO) binnen de overheid of organisaties in de markt waaraan de secretaris/algemeen directeur of proceseigenaar (een deel van) de beveiligingstaak inbesteedt respectievelijk uitbesteedt.

In de BIO staat aangegeven welke controls voor welke rol toepasselijk zijn. Omdat de overheid pluriform is georganiseerd, is deze toedeling indicatief. De BIO verplicht wel om de controls en overheidsmaatregelen die bij de rollen staan intern toe te delen en hierbij rekening te houden met voldoende functiescheiding. In het algemeen is de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden, terug te vinden in het informatiebeveiligingsbeleid van de organisatie. [35]

3. Basisbeveiligingsniveaus
Zoals in paragraaf 2.1 beschreven, onderscheidt de BIO drie basisbeveiligingsniveaus (BBN's). 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.

Als informatie wordt ontvangen van derden wordt deze ontvangen informatie behandeld conform de aanwijzingen van de afzender. Als de afzender geen markering of rubricering meegeeft wordt de ontvangen informatie behandeld conform de classificatie-eisen van het ontvangende proces.

33) In sommige organisaties heet de eindverantwoordelijke "secretaris-generaal", "directeur" of "bestuursvoorzitter" en moet de term "secretaris/algemeen directeur" als "secretaris-generaal", "directeur" of "bestuursvoorzitter" worden gelezen.
34) Bij het Rijk kan dat bijvoorbeeld ook de beveiligingsambtenaar (BVA) zijn.
35) Artikel 3 sub b VIR.

3.1. BBN1
Informatiesystemen op BBN1 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).

3.2. BBN2
Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. BBN2 is van toepassing indien[36]:
- er vertrouwelijke informatie wordt verwerkt;
- mogelijke incidenten leiden tot bestuurlijke commotie;
- de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

Het te beschermen belang van BBN2 is maximaal Departementaal Vertrouwelijk (DepV), (zoals gedefinieerd in het VIR-BI)/vergelijkbaar vertrouwelijk bij andere overheidslagen en privacygevoelige informatie met een verhoogd vertrouwelijkheidsniveau. Dergelijke informatie komt veelvuldig voor bij de overheid. Het gaat verder om commercieel vertrouwelijke informatie of informatie in het kader van beleidsvorming; het is dus niet beperkt tot als DepV/vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie.

BBN2-informatie wordt preventief beschermd tegen alle dreigingen met uitzondering van geavanceerde dreigingen, zoals Advanced Persistent Threats (APT's), afkomstig van statelijke actoren of beroepscriminelen. Daarvoor geldt een bescherming achteraf: zij dienen te kunnen worden gedetecteerd, waarop vervolgens passend gereageerd moet worden. Voor informatiesystemen waar Departementaal Vertrouwelijke informatie en vergelijkbaar vertrouwelijk bij andere overheidslagen wordt verwerkt en waar weerstand tegen de geavanceerde dreiging van statelijke actoren of gelijkwaardige beroepscriminelen is vereist, is het BBN2 dus niet voldoende.

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:
- wet- en regelgeving, in het bijzonder beveiligingseisen als gevolg van WBP/AVG;
- aansluitvoorwaarden van generieke/gemeenschappelijke diensten;
- afhankelijkheden in ketens en netwerken;
- minimale eisen ten behoeve van een efficiënte beveiliging van BBN3.

3.3. BBN3
BBN3 richt zich op de bescherming van als Departementaal Vertrouwelijk en vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie, waarbij weerstand geboden moet worden tegen de dreiging, zoals Advanced Persistant Threats (APT's), die uitgaat van statelijke actoren en beroepscriminelen. BBN3 is van toepassing indien:
- verlies van informatie een grote impact heeft, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op BBN3;
- informatie met een rubricering (niet zijnde BBN2) wordt geleverd door derden;
- 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).

Om redenen van efficiency sluit BBN3 aan op relevante NAVO-regelgeving waarin ook al rekening wordt gehouden met het bieden van weerstand tegen statelijke actoren[37]. Dit betekent dat BBN3 bestaat uit de controls en overheidsmaatregelen uit BBN2, aangevuld met relevante eisen uit het VIR-BI, relevante bepalingen uit regelingen andere overheidslagen en uit het NAVO-verdrag voor de beveiliging van informatie[38]. Niet alle delen/maatregelen zijn van toepassing voor de nationale context en voor

36) Zie de BBN-toets in Deel 2 voor meer details.

37) Zowel voor EU als voor NAVO gerubriceerde informatie geldt dat de beveiligingsvoorschriften standaard rekening houden met het bieden van weerstand tegen statelijke actoren. Voor de BIO is uiteindelijk gekozen om aan te sluiten bij de NAVO-regelgeving omdat de NAVO-eisen gedetailleerder zijn dan die van de EU en daarmee meer zekerheid bieden dat ook daadwerkelijk weerstand tegen statelijke actoren kan worden geboden. Voor de goede orde: alleen op NATO gerubriceerde informatie heeft het NAVO-verdrag rechtstreekse werking, BBN3 is Nederlandse informatie waarop het NAVO-verdrag niet rechtstreeks werkt; de toepasselijkheid van het NAVO-verdrag voor BBN3 is een keuze die de overheid zelf via deze BIO maakt.

38) CM(2002)49 met bijbehorende enclosures en directives.

NATO Restricted[39]. In de uitwerking van BBN3 zal daarom specifiek aangegeven worden welke delen/maatregelen van het NAVO-verdrag specifiek van toepassing zijn.

4. Verantwoording over de BIO
De secretaris/algemeen directeur van een organisatie is *eindverantwoordelijk* voor de integrale beveiliging en de inrichting en werking van de beveiligingsorganisatie[40].
In die hoedanigheid is hij eindverantwoordelijk voor de implementatie van alle beveiligingskaders in zijn organisatie, dus ook voor een juiste toepassing van de BIO.

De bestuurlijke verantwoording over de toepassing van de BIO is onderdeel van de verantwoording over de beveiliging van informatie(systemen). Hier wordt ook verantwoording afgelegd aan de ketenpartners met wie afspraken over de beveiliging van informatie zijn gemaakt.

4.1. Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau
De ISO 27001 en het VIR bepalen dat het lijnmanagement vaststelt dat de getroffen maatregelen aantoonbaar overeenstemmen met de betrouwbaarheidseisen en dat deze maatregelen worden nageleefd[41].
De proportionaliteit die eerder beschreven is, is ook van toepassing bij het toekennen van het niveau waar de verantwoordelijkheid voor risicomanagement wordt belegd:
- Voor BBN1 is de proceseigenaar volledig verantwoordelijk voor het nemen van (verstandige) beslissingen. Slechts incidenteel en op verzoek informeert deze de CISO over de stand van zaken met betrekking tot zijn BBN1-informatiesystemen.
- Voor BBN2 geldt dat de proceseigenaar het informatiesysteem voor ingebruikname (bij voorkeur in ontwerp-/ontwikkelfase) ter consultatie voorlegt aan de CISO[42].
- Voor BBN3 geldt dat vooraf toestemming verleend moet worden door de secretaris/algemeen directeur voor het verwerken van bijzondere informatie (conform het VIR-BI)[43]. Voor het verlenen van toestemming is mandatering mogelijk naar bijvoorbeeld de CIO of CISO en bij het Rijk naar de BVA.

Organisaties kunnen voor BBN1 en BBN2 hiervan afwijken in het informatiebeveiligingsbeleid[44].

4.2. Explains op overheidsmaatregelen
Overheidsmaatregelen die niet van toepassing zijn, hoeven niet als 'explain' te worden benoemd.

De organisatie dient te beschikken over een registratie van overheidsmaatregelen waaraan niet of nog niet geheel kan worden voldaan. Dit zijn explains volgens het 'comply or explain' principe. Daarbij worden tevens de daaruit voortvloeiende risico's aangegeven.

Explains ten aanzien van overheidsmaatregelen kunnen bij het samenwerken in ketens zorgen voor een verschil in bescherming tussen partijen waardoor een risico ontstaat voor de verwerkte (en gedeelde) informatie. Partijen met explains moeten dit afstemmen met hun (samenwerk- of keten)partners, zodat ze samen passende maatregelen of tijdelijke maatregelen treffen die het risico mitigeren of verkleinen zolang de explains niet conform de BIO geïmplementeerd zijn.
Voor rijksonderdelen geldt: explains die de veiligheid van andere delen van de rijksdienstonderdelen raken, worden voorzien van een advies van de Security Accreditation Authority (SAA, ingevuld door de Subcommissie Informatiebeveiliging) en door het ministerie voorgelegd aan het CIO-Beraad.

4.3. Ketensamenwerking
Binnen de overheid en met andere externe partijen wordt veel in ketens samengewerkt en daarom vormt, zoals in paragraaf 1.1 aangegeven, de gemeenschappelijke veiligheid van informatieketens ook een basis voor de concretisering van de overheidsmaatregelen.

Een keten is een samenwerkingsverband tussen organisaties die naast hun eigen doelstellingen, één of meer gemeenschappelijk gekozen (of door de politiek opgelegde) doelstellingen nastreven. Deze ketenpartners zijn zelfstandig, maar zijn ook afhankelijk van elkaar waar het gaat om het bereiken van

39) Er zijn passages die enkel op de bescherming van informatie met een rubricering van NATO Confidential en hoger betrekking hebben.
40) Artikel 4 lid 1 BVR.
41) Artikel 4 sub b VIR.
42) Bij DepV informatie geldt, conform het VIR-BI, het BBN3-regime voor verantwoording.
43) Artikel 3 sub b VIR-BI.
44) Artikel 3 sub b VIR.

de gezamenlijke (keten)doelstellingen[45]. Een informatieketen betreft de uitwisseling van informatie binnen zo'n samenwerkingsverband.

Ook in het kader van ketensamenwerking kan de verantwoordelijkheid voor informatiebeveiliging niet worden gedelegeerd.

In het geval dat een organisatie informatie aan ketenpartners toevertrouwt, blijft deze organisatie er verantwoordelijk voor dat ketenpartners de toevertrouwde informatie zorgvuldig beschermen. De organisatie moet daarom aansluitvoorwaarden eisen of stellen aan de leverende of afnemende partij. Tevens moet de organisatie leveringsgaranties bieden aan de afnemende partij. De organisatie moet hiervoor inzichtelijk hebben van welke informatiesystemen en infrastructuren zij afhankelijk is, welke afhankelijk zijn van haar en hoe de governance van beide hierop is ingericht.

4.4. Dienstenleveranciers
In de BIO wordt bij het van toepassing verklaren van controls en overheidsmaatregelen geen onderscheid gemaakt in interne of externe dienstenleveranciers. Ook bij de wijze waarop verantwoording wordt afgelegd over hun diensten worden interne en externe dienstenleveranciers gelijk behandeld. Dit betekent voor alle dienstenleveranciers het volgende.

- Periodiek leggen alle dienstenleveranciers verantwoording af via een Statement of Compliance (of deel-ICV; met toepasselijke reikwijdte) aan de opdrachtgever bij de overheid.
- De dienstenleveranciers volgen de beveiligingseisen die de overheidsorganisaties of ketenpartners stellen aan de diensten van de dienstenleverancier. Uit efficiencyoverwegingen kan een dienstenleverancier een standaard beveiligingsniveau aanbieden, maar dit doet geen afbreuk aan de genoemde verantwoordelijkheid van de overheidsorganisaties.
- Voor diensten die aan één organisatie worden aangeboden, legt de dienstenleverancier verantwoording af aan de opdrachtgevende organisatie. De opdrachtgevende organisatie neemt de verantwoording op in haar ICV. De opdrachtgevende organisatie houdt ook toezicht op specifieke dienstverlening.
- Voor diensten die aan meerdere overheden of overheidsonderdelen worden aangeboden, stelt de dienstenleverancier één verantwoording op ten behoeve van alle afnemers. Voor het Rijk wordt in het CIO-Beraad jaarlijks vastgesteld wie toezicht houdt op de beveiliging van deze diensten.

Naast de verantwoording over hun diensten zijn de dienstenleveranciers ook zelf als organisatie gebonden aan informatiebeveiligingsregels. Hierbij is wel een onderscheid aanwezig tussen interne en externe dienstenleveranciers:

- Interne dienstenleveranciers zijn, als onderdeel van de overheid, zelf ook rechtstreeks gebonden aan de BIO. Ze zijn daarmee gehouden aan de reguliere verantwoordings- en toezichtprocedures van de betreffende overheidslagen. Bij het Rijk geldt onder meer het toezicht vanuit de ADR, ARK en de BVA. De interne dienstenleverancier is ook gebonden aan het jaarlijks opleveren van een In Control Verklaring (ICV). Hierin verklaart de dienstenleverancier dat hij voor zijn eigen bedrijfsvoering aan de BIO voldoet (inclusief de overheidsmaatregelen).
- Externe dienstenleveranciers zijn geen onderdeel van de overheid en zijn daarmee zelf niet rechtstreeks gebonden aan de BIO of het opleveren van een ICV. Ze moeten wel voldoen aan de eisen van de opdrachtgever. Voorwaarden ten behoeve van informatiebeveiliging moeten daarom in het contract zijn vastgelegd. In de BIO zijn in hoofdstuk 15 over leveranciersrelaties controls en overheidsmaatregelen opgenomen die moeten zorgen voor een goede borging van informatiebeveiliging in contracten.

Het is mogelijk dat een (externe) dienstenleverancier beschikt over een kwaliteitskeurmerk zoals een ISO 27001-certificaat of bijvoorbeeld een ISAE 3402-verklaring. De waarde van zo'n keurmerk of verklaring is afhankelijk van de reikwijdte en diepgang. Het zegt meestal iets over het proces dat bij de dienstenleverancier is ingericht. Hoewel dit dus wel meerwaarde heeft, overlap kent met de BIO-controls en gebruikt kan worden als onderdeel van het Statement of Compliance, omvat en vervangt het niet volledig de verantwoording over de overheidsmaatregelen uit de BIO. Er zullen altijd aanvullende afspraken gemaakt moeten worden over de 'gap' tussen keurmerk of verklaring en de BIO-controls. Hierover moet aanvullend worden verantwoord.

Deel 2 Kader BIO

Inleiding
Het Kader BIO bestaat uit een BBN-toets om het juiste basisbeveiligingsniveau (BBN) te bepalen en de tabellen met de controls en maatregelen. De BBN-toets wordt voor ieder bedrijfsproces uitgevoerd. Het BBN bepaalt welke controls vervolgens moeten worden doorlopen. Per control moet worden bepaald

45) https://noraonline.nl/wiki/Ketensturing/De_wereld_van_ketens/Wat_is_een_keten%3F

welke maatregelen in aanvulling op de verplichte overheidsmaatregelen nodig zijn. Voor meer toelichting op de opzet van de BIO en de BBN's wordt verwezen naar Deel 1 van deze BIO.

In het document zijn de controls dan als volgt opgebouwd:

Controlnummer overeenkomstig met ISO 27002	**BBN (1, 2 of 3)**	**Controltekst (ISO 27002)**	**Verantwoordelijke(n)**
O-maatregelnummer	BBN (1, 2 of 3)	O-maatregel	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier

Om het verschil tussen de ISO 27002 controls en de overheidsmaatregelen te duiden, zijn ook verschillende kleurmarkeringen gebruikt:
- **Blauw zijn de ISO-controls.**
- **Groen zijn overheidsmaatregelen (O-maatregel).**

In de kolom 'Verantwoordelijke(n)' staat aangegeven wie voor de uitvoering van de control verantwoordelijk is: secretaris/algemeen directeur (eindverantwoordelijke voor de bedrijfsvoering van een organisatie), proceseigenaar en/of dienstenleverancier.

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

Stap 1: Is BBN2 voldoende?
Meestal is BBN2 van toepassing op een specifiek informatiesysteem. Het kan echter zijn dat BBN2 niet voldoende is. BBN2 is onvoldoende indien:
- de informatie beschermd dient te worden tegen statelijke actoren of vergelijkbare dreigers;
- informatie wordt geleverd door derden en deze voor de beveiliging van betreffende informatie BBN3 eisen;
- 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 (zie VIR-BI in geval van het Rijk) van toepassing.

Stap 2: Is BBN2 te zwaar?
Bij BBN2-informatiesystemen kan het ongewenst of onbedoeld openbaren van informatie leiden tot BBN2-schade:
- Politieke schade aan een bestuurder: bestuurder moet verantwoording afleggen aan de (gekozen) controlerende organen, bijvoorbeeld naar aanleiding van verantwoordingsvragen.
- diplomatieke schade te herstellen door ambtelijke opschaling.
- Financiële gevolgen: niet meer op te vangen binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven.
- Verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers.
- Bindende aanwijzing van de Autoriteit Persoonsgegevens in verband met schending van de privacy
- 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 het toezicht vinden 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 het toezicht vinden 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 ISO 27002.

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.

5.1.1	**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.	Secretaris/algemeen directeur
5.1.1.1	1	Er is een informatiebeveiligingsbeleid opgesteld door de organisatie. Dit beleid is vastgesteld door de leiding van de organisatie en bevat ten minste de volgende punten: a) 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. b) De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. c) De toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers. d) De gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn. e) De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. f) De bevordering van het beveiligingsbewustzijn.	

5.1.2	**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.	Secretaris/algemeen directeur
5.1.2.1	1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen 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	**1**	**Rollen en verantwoordelijkheden bij informatiebeveiliging** Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	Secretaris/algemeen directeur
6.1.1.1	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	1	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	
6.1.1.3	1	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	
6.1.1.4	1	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	

6.1.2	**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.	Proceseigenaar Dienstenleverancier
6.1.2.1	1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.	

6.1.3	**2**	**Contact met overheidsinstanties** Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
6.1.3.1	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	2	Het contactoverzicht wordt jaarlijks geactualiseerd.	

6.1.4	**-**	**Vervallen**	-

6.1.5	**2**	**Informatiebeveiliging in projectbeheer** Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	Proceseigenaar Dienstenleverancier

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

6.2.1	**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.	Proceseigenaar Dienstenleverancier
6.2.1.1	2	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet 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	2	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: a) In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde. b) Het device maakt deel uit van patchmanagement en hardening. c) Er wordt gebruik gemaakt van Mobile Device Management MDM of van Mobile Application Management (MAM)-oplossingen. d) 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. e) Periodiek wordt getoetst of de punten in lid a), b) en c) worden nageleefd.	

6.2.2	**2**	**Telewerken** Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	Secretaris/algemeen directeur Dienstenleverancier

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	**1**	**Screening** Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante	Secretaris/algemeen directeur

		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.	Proceseigenaar
7.1.1.1	1	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.	

7.1.2	**1**	**Arbeidsvoorwaarden** De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	Secretaris/algemeen directeur Proceseigenaar
7.1.2.1	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	**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.	Secretaris/algemeen directeur
7.2.1.1	1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen anoniem en veilig beveiligingsissues kan melden.	

7.2.2	**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.	Secretaris/algemeen directeur Proceseigenaar
7.2.2.1	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	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	1	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn 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	**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.	Secretaris/algemeen directeur

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	**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, gecom-	Secretaris/algemeen directeur Proceseigenaar

		municeerd 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	**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.	Proceseigenaar Dienstenleverancier

8.1.2	**1**	**Eigendom van bedrijfsmiddelen** Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	Proceseigenaar Dienstenleverancier

8.1.3	**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.	Secretaris/algemeen directeur Proceseigenaar
8.1.3.1	1	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.	
8.1.3.2	1	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.	

8.1.4	**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.	Secretaris

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

8.2.2	**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.	Proceseigenaar

8.2.3	**1**	**Behandelen van bedrijfsmiddelen** Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstem-	Proceseigenaar Dienstenleverancier

		ming 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	**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.	Proceseigenaar Dienstenleverancier
8.3.1.1	1	Er is een verwijderinstructie waarin is opgenomen dat van verwijderbare media die herbruikbaar zijn en die de organisatie verlaten de onnodige inhoud onherstelbaar verwijderd is (ISO 27002 – implementatierichtlijn 8.3.1.a).	

8.3.2	**2**	**Verwijderen van media** Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	Dienstenleverancier
8.3.2.1	2	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.	
8.3.2.2	2	Verwijdering vindt plaats op een veilige manier, bijvoorbeeld 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 (ISO 27002 – implementatierichtlijn 8.3.2.a).	
8.3.2.3	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	**2**	**Media fysiek overdragen** Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	Secretaris/algemeen directeur
8.3.3.1	2	Er is een vastgestelde procedure voor het fysiek transport van media.	
8.3.3.2	2	Het gebruik van koeriers of transporteurs voor transport van op BBN2 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	**1**	**Beleid voor toegangsbeveiliging** Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Secretaris

9.1.2	**1**	**Toegang tot netwerken en netwerkdiensten** Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Dienstenleverancier
9.1.2.1	1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	
9.1.2.2	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	**1**	**Registratie en afmelden van gebruikers** Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Proceseigenaar Dienstenleverancier
9.2.1.1	1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	
9.2.1.2	1	Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	

9.2.2	**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.	Proceseigenaar Dienstenleverancier
9.2.2.1	1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.	
9.2.2.2	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	2	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	

9.2.3	**1**	**Beheren van speciale toegangsrechten** Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	Proceseigenaar Dienstenleverancier
9.2.3.1	2	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	

9.2.4	**1**	**Beheer van geheime authenticatie-informatie van gebruikers** Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	Dienstenleverancier

9.2.5	**1**	**Beoordeling van toegangsrechten van gebruikers** Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	Proceseigenaar Dienstenleverancier
9.2.5.1	1	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld.	
9.2.5.2	1	De opvolging van bevindingen is gedocumenteerd en wordt behandeld als beveiligingsincident.	
9.2.5.3	2	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.	

9.2.6	**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.	Proceseigenaar Dienstenleverancier

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

9.3.1	**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.	Secretaris/algemeen directeur Dienstenleverancier
9.3.1.1	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	**1**	**Beperking toegang tot informatie** Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	Proceseigenaar Dienstenleverancier
9.4.1.1	2	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	
9.4.1.2	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	**1**	**Beveiligde inlogprocedures** Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	Proceseigenaar Dienstenleverancier
9.4.2.1	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	2	Voor het verlenen van toegang tot het netwerk aan 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	**1**	**Systeem voor wachtwoordbeheer** Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	Dienstenleverancier
9.4.3.1	1	Als er geen gebruik wordt gemaakt van two-factor authenticatie, is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal foutieve inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen, is vastgelegd.	
9.4.3.2	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	2	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	
9.4.3.4	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	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 zes maanden.	

9.4.4	**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.	Dienstenleverancier
9.4.4.1	1	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.	

9.4.4.2	2	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.	

9.4.5	**1**	**Toegangsbeveiliging op programmabroncode** Toegang tot de programmabroncode behoort te worden beperkt.	Proceseigenaar Dienstenleverancier

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	**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.	Secretaris
10.1.1.1	2	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	
10.1.1.2	2	Cryptografische toepassingen voldoen aan passende standaarden.	

10.1.2	**1**	**Sleutelbeheer** Er dient beleid te worden ontwikkeld en geïmplementeerd met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels welke de gehele levensduur van de cryptografische sleutels omvat.	Dienstenleverancier
10.1.2.1	2	Ingeval van PKIoverheid-certificaten: hanteer de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties: hanteer de standaard ISO 11770 voor het beheer van cryptografische sleutels.	
10.1.2.2	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	**1**	**Fysieke beveiligingszone** Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	Secretaris/algemeen directeur
11.1.1.1	1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van standaarden.	

11.1.2	**1**	**Fysieke toegangsbeveiliging** Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	Secretaris/algemeen directeur
11.1.2.1	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	**1**	**Kantoren, ruimten en faciliteiten beveiligen** Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	Proceseigenaar Dienstenleverancier
11.1.3.1	1	Sleutelbeheer is ingericht op basis van een sleutelplan.	

11.1.4	**1**	**Beschermen tegen bedreigingen van buitenaf** Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	Proceseigenaar Dienstenleverancier
11.1.4.1	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	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	**2**	**Werken in beveiligde gebieden** Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	Proceseigenaar Dienstenleverancier

11.1.6	**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.	Dienstenleverancier

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

11.2.1	**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.	Dienstenleverancier

11.2.2	**1**	**Nutsvoorzieningen** Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	Dienstenleverancier

11.2.3	**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.	Dienstenleverancier

11.2.4	**1**	**Onderhoud van apparatuur** Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	Dienstenleverancier

11.2.5	**1**	**Verwijdering van bedrijfsmiddelen**	Dienstenleverancier

		Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	

11.2.6	**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.	Dienstenleverancier

11.2.7	**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.	Dienstenleverancier
		Zie overheidsmaatregelen van 8.3.2.	

11.2.8	**1**	**Onbeheerde gebruikersapparatuur** Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	Proceseigenaar Dienstenleverancier

11.2.9	**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.	Secretaris/algemeen directeur Dienstenleverancier
11.2.9.1	2	Een onbemensde werkplek is altijd vergrendeld.	
11.2.9.2	2	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	
11.2.9.3	2	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	
11.2.9.4	2	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.	
11.2.9.5	2	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het 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	**1**	**Gedocumenteerde bedieningsprocedures** Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	Proceseigenaar Dienstenleverancier

12.1.2	**1**	**Wijzigingsbeheer** Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	Proceseigenaar Dienstenleverancier
12.1.2.1	1	In de procedure voor wijzigingenbeheer is minimaal aandacht besteed aan: (a) het administreren van wijzigingen; (b) risicoafweging van mogelijke gevolgen van de wijzigingen;	

		(c) goedkeuringsprocedure voor wijzigingen.	

12.1.3	**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.	Dienstenleverancier

12.1.4	**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.	Proceseigenaar Dienstenleverancier
12.1.4.1	2	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	
12.1.4.2	2	Wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.	

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

12.2.1	**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.	Secretaris/algemeen directeur Dienstenleverancier
12.2.1.1	1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.	
12.2.1.2	1	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.	
12.2.1.3	1	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.	
12.2.1.4	1	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. (b) Bijlagen en downloads vóór gebruik.	
12.2.1.5	1	De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld 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	**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.	Proceseigenaar Dienstenleverancier
12.3.1.1	1	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld	
12.3.1.2	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	2	In het back-upbeleid staan minimaal de volgende eisen:	

		(a) Dataverlies bedraagt maximaal 28 uur. (b) Hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.	
12.3.1.4	2	Het back-upproces 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	2	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden.	

12.4 Verslaglegging en monitoren
Doelstelling: Gebeurtenissen vastleggen en bewijs verzamelen.

12.4.1	**1**	**Gebeurtenissen registreren** Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	Proceseigenaar Dienstenleverancier
12.4.1.1	1	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.	
12.4.1.2	1	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	
12.4.1.3	2	De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	
12.4.1.4	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	2	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	

12.4.2	**1**	**Beschermen van informatie in logbestanden** Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing en onbevoegde toegang.	Dienstenleverancier
12.4.2.1	1	Er is een overzicht van logbestanden die worden gegenereerd.	
12.4.2.2	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	2	Er is een (onafhankelijke) interne audit procedure die minimaal half jaarlijks toetst op het ongewijzigd bestaan van logbestanden.	
12.4.2.4	2	Oneigenlijk wijzigen of verwijderen van loggegevens of pogingen daartoe worden zo snel mogelijk gemeld als beveiligingsincident via de procedure voor informatiebeveiligingsincidenten conform hoofdstuk 16.	

12.4.3	**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.	Dienstenleverancier

12.4.4	**1**	**Kloksynchronisatie** De klokken van alle relevante informatie verwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met één referentietijdbron.	Dienstenleverancier

12.5 Beheersing van operationele software
Doelstelling: De integriteit van operationele systemen waarborgen.

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

12.6 Beheer van technische kwetsbaarheden
Doelstelling: Benutting van technische kwetsbaarheden voorkomen.

12.6.1	**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.	Dienstenleverancier
12.6.1.1	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	**1**	**Beperkingen voor het installeren van software** Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	Dienstenleverancier
12.6.2.1	2	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat 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	**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.	Proceseigenaar Dienstenleverancier

13. Communicatiebeveiliging
13.1 Beheer van netwerkbeveiliging
Doelstelling: De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten waarborgen.

13.1.1	**1**	**Beheersmaatregelen voor netwerken** Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Dienstenleverancier

13.1.2	**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.	Dienstenleverancier
13.1.2.1	2	Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), 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	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	2	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	
13.1.2.4	1	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.	

13.1.3	**1**	**Scheiding in netwerken** Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden.	Dienstenleverancier
13.1.3.1	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	**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.	Secretaris/algemeen directeur

13.2.2	**1**	**Overeenkomsten over informatietransport** Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	Proceseigenaar Dienstenleverancier

13.2.3	**1**	**Elektronische berichten** Informatie die is opgenomen in elektronische berichten behoord passend te zijn beschermd.	Dienstenleverancier
13.2.3.1	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	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	2	Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	
13.2.3.4	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	**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.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier

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	**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.	Proceseigenaar
14.1.1.1	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	**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.	Dienstenleverancier
		Zie overheidsmaatregel 13.2.3.3.	

14.1.3	**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.	Dienstenleverancier
		Zie overheidsmaatregel 13.2.3.3.	

14.2 Beveiliging in ontwikkelings- en ondersteunende processen
Doelstelling: Bewerkstelligen dat informatiebeveiliging wordt ontworpen en geïmplementeerd binnen de ontwikkelingslevenscyclus van informatiesystemen.

14.2.1	**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.	Secretaris/algemeen directeur Proceseigenaar
14.2.1.1	1	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.	

14.2.2	**1**	**Procedures voor wijzigingsbeheer met betrekking tot systemen**	Proceseigenaar Dienstenleverancier

		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	1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.	

14.2.3	**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.	Dienstenleverancier

14.2.4	**-**	**Vervallen**	-

14.2.5	**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.	Dienstenleverancier
14.2.5.1	1	Zie overheidsmaatregel 14.2.1.1	

14.2.6	**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.	Dienstenleverancier
14.2.6.1	1	Systeemontwikkelomgevingen worden passend beveiligd op basis van een expliciete risicoafweging	

14.2.7	**1**	**Uitbestede softwareontwikkeling** Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	Proceseigenaar
14.2.7.1	1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.	

14.2.8	**1**	**Testen van systeembeveiliging** Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	Dienstenleverancier

14.2.9	**1**	**Systeemacceptatietests** Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	Proceseigenaar Dienstenleverancier
14.2.9.1	1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.	
14.2.9.2	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	**2**	**Bescherming van testgegevens**	Proceseigenaar

		Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	Dienstenleverancier

15. Leveranciersrelaties
15.1 Informatiebeveiliging in leveranciersrelaties
Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

15.1.1	**1**	**Informatiebeveiligingsbeleid voor leveranciersrelaties** Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, te worden overeengekomen en gedocumenteerd.	Secretaris/algemeen directeur Proceseigenaar
15.1.1.1	1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen ten aanzien van informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd. Deze eisen zijn gebaseerd op een expliciete risicoafweging.	
15.1.1.2	2	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	
15.1.1.3	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	**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.	Proceseigenaar Dienstenleverancier
15.1.2.1	1	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in de (inkoop)contracten waar informatie een rol speelt.	
15.1.2.2	1	In de inkoopcontracten worden expliciet prestatie-indicatoren en de bijbehorende verantwoordingsrapportages opgenomen.	
15.1.2.3	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	1	Ter waarborging van vertrouwelijkheid of geheimhouding worden bij IT-inkopen standaardvoorwaarden voor inkoop gehanteerd.	
15.1.2.5	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	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 door middel van certificering aantoont dat de gewenste betrouwbaarheid van de dienst is geborgd.	

15.1.3	**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.	Proceseigenaar Dienstenleverancier
15.1.3.1	2	Leveranciers moeten hun keten van toeleveranciers bekendmaken en transparant zijn over de maatregelen die zij genomen hebben om de aan hen opgelegde eisen ook door te vertalen naar hun toeleveranciers.	

15.2 Beheer van dienstverlening van leveranciers

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

15.2.1	**1**	**Monitoring en beoordeling van dienstverlening van leveranciers** Organisaties behoren regelmatig de dienstverlening van leveranciers te monitoren, te beoordelen en te auditen.	Proceseigenaar
15.2.1.1	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	**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.	Proceseigenaar

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	**1**	**Verantwoordelijkheden en procedures** Directieverantwoordelijkheden en -procedures behoren te worden vastgesteld om een snelle, doeltreffende en ordelijke respons op informatiebeveiligingsincidenten te bewerkstelligen.	Secretaris/algemeen directeur Proceseigenaar

16.1.2	**1**	**Rapportage van informatiebeveiligingsgebeurtenissen** Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
16.1.2.1	1	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.	
16.1.2.2	1	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.	
16.1.2.3	1	Alle medewerkers en contractanten hebben aantoonbaar kennisgenomen van de meldingsprocedure van incidenten.	
16.1.2.4	1	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.	
16.1.2.5	1	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.	
16.1.2.6	1	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.	
16.1.2.7	1	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage[48].	

16.1.3	**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.	Proceseigenaar Dienstenleverancier
		Zie overheidsmaatregel 16.1.2.4	

48)Voorheen werd Coordinated Vulnerability Disclosure (CVD) responsible disclosure genoemd.

16.1.3.1	1	Een Coordinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht[49].	

16.1.4	**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.	Proceseigenaar Dienstenleverancier
16.1.4.1	2	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende 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	**1**	**Respons op informatiebeveiligingsincidenten** Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Proceseigenaar Dienstenleverancier

16.1.6	**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.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
16.1.6.1	2	Beveiligingsincidenten worden geanalyseerd met als doel te leren en toekomstige beveiligingsincidenten te voorkomen.	
16.1.6.2	2	De analyses van de beveiligingsincidenten worden gedeeld met de relevante partners om herhaling en toekomstige incidenten te voorkomen.	

16.1.7	**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.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
16.1.7.1	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	**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.	Secretaris/algemeen directeur Proceseigenaar

17.1.2	**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.	Proceseigenaar Dienstenleverancier

49) Voorheen werd Coordinated Vulnerability Disclosure (CVD) responsible disclosure genoemd.

17.1.3	**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.	Proceseigenaar Dienstenleverancier
17.1.3.1	2	Continuïteitsplannen worden jaarlijks getest op geldigheid en bruikbaarheid.	
17.1.3.2	2	Door het uitvoeren van een expliciete risicoafweging worden de bedrijfskritische procesonderdelen met hun bijbehorende betrouwbaarheidseisen geïdentificeerd.	
17.1.3.3	2	De dienstverlening van de bedrijfskritische onderdelen wordt bij calamiteiten uiterlijk binnen een week hersteld.	

17.2 Redundante componenten
Doelstelling: Beschikbaarheid van informatie verwerkende faciliteiten bewerkstelligen.

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

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	**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.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier

18.1.2	**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.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier

18.1.3	**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.	Proceseigenaar Dienstenleverancier
18.1.3.1	2	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	

18.1.4	**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.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
18.1.4.1	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	2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	
		Zie overheidsmaatregel 14.2.6.1	

18.1.5	**1**	**Voorschriften voor het gebruik van cryptografische beheersmaatregelen** Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	Secretaris/algemeen directeur
18.1.5.1	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	**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.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
18.2.1.1	2	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	
18.2.1.2	2	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	

18.2.2	**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.	Secretaris/algemeen directeur Proceseigenaar Dienstenleverancier
18.2.2.1	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	**1**	**Beoordeling van technische naleving** Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	Proceseigenaar Dienstenleverancier
18.2.3.1	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 penetratietesten.	

Bijlage 1: Wet- en regelgeving
Om de BIO praktisch uitvoerbaar te maken, zijn in veel overheidsmaatregelen verwijzingen opgenomen naar bestaande wet- en regelgeving. Deze verwijzingen hebben als voordeel dat degene die met de BIO aan de slag gaat er concreet op gewezen wordt dat er reeds bestaande wet- en regelgeving is waarin (beveiligings)eisen zijn vastgelegd. Bovendien zijn deze verwijzingen zo ook in het stramien van de ISO 27002-indeling gepositioneerd. Er is bewust gekozen voor het maken van verwijzingen en niet

voor het herformuleren om misinterpretatie te voorkomen. Voor de genoemde wet- en regelgeving geldt dat de BIO alleen bepaalde beveiligingsaspecten heeft meegenomen. Het is niet de intentie dat de BIO de genoemde wet- en regelgeving volledig afdekt.

In de overheidsmaatregelen zijn verwijzingen opgenomen naar de volgende wet- en regelgeving:
- Ades baseline profile standard
- Algemeen Rijksambtenarenreglement (ARAR)
- Algemene Rijksvoorwaarden bij IT-overeenkomsten (ARBIT 2016)
- AVG (deze vervangt de WBP en is 25 mei 2018 van kracht geworden);
- Beveiligingsvoorschrift 2013 (BVR 2013), *Staatscourant*. 2013, 15496
- CM(2002)49
- Gedragsregeling voor de digitale werkomgeving (1 juli 2016; SGO-besluit)
- Het NkBR (Normenkader Beveiliging Rijkskantoren) 2015
- Interne klokkenluidersregeling
- ITIL, ASL of BiSL framework
- Kader Rijkstoegangsbeleid
- NCSC classificatie kwetsbaarheidswaarschuwingen
- 'Pas toe of leg uit'-lijst van het Forum Standaardisatie.
- Programma van Eisen PKI Overheid
- Responsible disclosure procedure
- Voorschrift Informatiebeveiliging Rijksdienst (VIR2007), *Staatscourant*. 2007, 122/11
- Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie (VIR-BI 2013)
- Wet veiligheidsonderzoeken (WVO)
- Archiefwet
- Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI)
- Wet basisregistratie personen (Wet BRP)
- Telecommunication Infrastructure Standard for Data Centers (TIA-942)

De BIO richt zich alleen op het aspect informatiebeveiliging. Mogelijk hebben de hierboven genoemde wetten en voorschriften een bredere werking dan alleen informatiebeveiliging. Invoering van de BIO dekt niet altijd deze wetten en voorschriften volledig af.

Bijlage 2: Basisbeveiligingsniveaus
De basisbeveiligingsniveaus zijn uitgewerkt langs de lijnen beschikbaarheid, integriteit en vertrouwelijkheid. De BBN-toets helpt bij het kiezen van het best passende niveau. De beschikbaarheidsniveaus zijn gebaseerd op de geldende beschikbaarheidsniveaus die door de grote interne dienstenleveranciers worden gehanteerd. De vertrouwelijkheidsniveaus zijn in lijn gebracht met de schadescenario's die gelden voor de Te Beschermen Belangen. De onderverdeling is als volgt:

BBN1:	beschikbaarheid	=	Laag	integriteit	=	Laag	vertrouwelijkheid	=	Laag
BBN2:	beschikbaarheid	=	Midden	integriteit	=	Midden	vertrouwelijkheid	=	Midden
BBN3:	beschikbaarheid	=	Midden	integriteit	=	Midden	vertrouwelijkheid	=	Hoog

BBN1	
Beschikbaarheid = Laag	Het informatiesysteem mag incidenteel uitvallen voor maximaal twee weken (ook in piekperiodes) en dit heeft nauwelijks of geen gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: - financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet tot het niet krijgen van een accountantsverklaring; - beperkt verlies van management control; - irritatie en ongemak bij burgers geventileerd in de media; - interne negatieve publiciteit (imagoschade). Deze gevolgen worden als volgt gekwantificeerd: - Kantoorautomatisering en organisatiespecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. - Maximaal dataverlies 28 uur. - Maximale hersteltijd in geval van incidenten is binnen 40 werkuren (vijf werkdagen van 8 uur) in 85% van de gevallen.

Integriteit = Laag	Er zijn geen bijzondere maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid van informatie te waarborgen[50]. Het verlies van integriteit kan leiden tot beperkte schade, bijvoorbeeld: - financiële gevolgen; op te vangen binnen de vastgestelde ruimte binnen de begroting van de organisatie of uitvoeringsorganisatie; leidt nog niet tot het niet krijgen van een accountantsverklaring; - beperkt verlies van management control; - irritatie en ongemak bij burgers geventileerd in de media; - interne negatieve publiciteit (imagoschade).
Vertrouwelijkheid = Laag	Kennisname van informatie door ongeautoriseerden (buitenstaanders) is niet gewenst, maar leidt niet tot schade van enige omvang. Het gaat hier om ongerubriceerde informatie. Het openbaar worden van deze informatie kan leiden tot: - financiële gevolgen: op te vangen binnen de begroting van de organisatie of uitvoeringsorganisatie; - irritatie en ongemak bij burgers geventileerd in de media; - interne negatieve publiciteit (imagoschade).

BBN2	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en dit heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: - politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; - diplomatieke schade te herstellen door ambtelijke opschaling; - financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; - belangrijk verlies van management control; - verlies van publiek respect; klachten van burgers; - organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: - Kantoorautomatisering en organisatiespecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. - Maximaal dataverlies 24 uur. - Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (twee dagen van 8 uur).
Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR-definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: - politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; - diplomatieke schade te herstellen door ambtelijke opschaling; - financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; - belangrijk verlies van management control; - verlies van publiek respect; klachten van burgers; - organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Vertrouwelijkheid = Midden	Bescherming van gegevens en andere te beschermen belangen in de processen van de overheid, waar onder andere vertrouwelijkheid aan de orde is, omdat het om gevoelige informatie gaat. Het openbaar worden van de gegevens kan leiden tot:

50) VIR-definitie.

	- politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; - diplomatieke schade te herstellen door ambtelijke opschaling; - financiële gevolgen: niet meer op te vangen binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; - verlies van publiek respect; klachten van burgers of significant verlies van motivatie van medewerkers; - bindende aanwijzing van de AP in verband met schending van de privacy; - directe imagoschade, bijvoorbeeld door negatieve publiciteit.

BBN3	
Beschikbaarheid = Midden	Het informatiesysteem mag beperkt korte tijd uitvallen voor maximaal één week (ook in piekperiodes) en dit heeft voelbare gevolgen voor burgers/gebruikers. Uitval kan leiden tot beperkte schade, bijvoorbeeld: - politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; - diplomatieke schade te herstellen door ambtelijke opschaling; - financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; - belangrijk verlies van management control; - verlies van publiek respect; klachten van burgers; - organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers. De beschikbaarheid wordt als volgt gekwantificeerd: - Kantoorautomatisering en organisatiespecifieke systemen hebben tijdens openingstijden een beschikbaarheid van minimaal 98% op maandbasis ook in piekperiodes. - Maximaal dataverlies 24 uur. - Maximale hersteltijd in geval van incidenten is binnen 16 werkuren (twee dagen van 8 uur).
Integriteit = Midden	Er zijn passende maatregelen noodzakelijk om de juistheid, tijdigheid en volledigheid (VIR-definitie) te waarborgen. Het verlies van integriteit kan leiden tot forse schade, bijvoorbeeld: - politieke schade aan een bestuurder: bestuurder moet zich verantwoorden naar aanleiding van verantwoordingsvragen; - diplomatieke schade te herstellen door ambtelijke opschaling; - financiële gevolgen: niet meer op te vangen binnen de vastgestelde ruimte binnen de begroting van de (uitvoerings)organisatie; geen accountantsverklaring afgegeven; - belangrijk verlies van management control; - verlies van publiek respect; klachten van burgers; - organisatiebrede negatieve publiciteit (imagoschade) of significant verlies van motivatie van medewerkers.
Vertrouwelijkheid = Hoog	Verlies van informatie heeft een grote impact, waarvan niet uit te leggen is als deze niet gerubriceerd is en beschermd wordt op het niveau van BBN3: - informatie wordt door derden geleverd met een rubricering (niet zijnde BBN2); - aansluiting op een infrastructuur vereist BBN3 (bijvoorbeeld om al op de infrastructuur aanwezige gerubriceerde informatie niet in gevaar te brengen) om informatie te kunnen verwerken op deze infrastructuur; - weerstand tegen statelijke actoren is noodzakelijk.

Deel 3 Addendum BIO

1 Inleiding Addendum

In dit addendum worden alle eisen genoemd die specifiek en verplichtend zijn voor een bepaalde overheidslaag. Omdat de rijksoverheid een aantal specifieke documenten heeft zoals het VIR, VIR-BI, die niet gelden voor andere overheidslagen, zijn deze nadrukkelijk opgenomen in dit addendum. Voorts

zijn teksten opgenomen die niet goed te verwerken waren in de eerste twee delen en dit komt dan voornamelijk door de rol van het NCSC voor de rijksoverheid en de aanwezigheid van een aantal sectorale CERT's bij de andere overheidslagen.

Het addendum is aanvullend op de teksten en normen uit deel 1 en 2.

5. Informatiebeveiligingsbeleid
5.1 Aansturing door de directie van de informatiebeveiliging

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
5.1.1.1	Rijk	1	Richtlijn: VIR, artikel 3	Secretaris/algemeen directeur
5.1.2.1	Rijk	1	Richtlijn: VIR, artikel 3, lid e	Secretaris/algemeen directeur
5.1.2.1	Rijk	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.	Secretaris/algemeen directeur

6. Organiseren van informatiebeveiliging
6.1 Interne organisatie

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
6.1.1.2	Rijk	1	Richtlijn: VIR, VIR-BI, BVR	Secretaris/algemeen directeur
6.1.3.3	Rijk	1	De organisatie verstrekt contactgegevens aan het NCSC ten behoeve van de opvolging van incidenten, kwetsbaarheden en dreigingen.	Secretaris/algemeen directeur/ Dienstenleverancier
6.1.3.3	Gemeente Waterschap	1	De organisatie verstrekt contactgegevens aan de sectorale CERT ten behoeve van de opvolging van incidenten, kwetsbaarheden en dreigingen.	Secretaris/algemeen directeur/ Dienstenleverancier

7. Veilig personeel
7.1 Voorafgaand aan het dienstverband

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
7.1.1	Rijk	1	Richtlijn: VIR-BI	Secretaris/algemeen directeur Proceseigenaar
7.1.1.1	Rijk	1	Bij indiensttreding overleggen alle medewerkers (intern en extern) een specifiek voor de functie verstrekte Verklaring Omtrent het Gedrag (VOG).	

7.2 Tijdens het dienstverband

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
7.2.1	Rijk	1	Richtlijn: interne klokkenluidersregeling	Secretaris/algemeen directeur

8. Beheer van bedrijfsmiddelen
8.1 Verantwoordelijkheid voor bedrijfsmiddelen

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
8.1	Rijk	1	Richtlijn: Gedragsregeling voor de digitale werkomgeving	Secretaris/algemeen directeur Proceseigenaar

8.3 Behandelen van media

8.3.1	Rijk	2	VIR-BI: goedgekeurde producten NBV	Proceseigenaar Dienstenleverancier

8.3.1.2	Rijk	2	De wijze waarop vertrouwelijk of hoger gerubriceerde informatie is opgeslagen, voldoet aan de eisen van het NBV.	Proceseigenaar Dienstenleverancier

11. Fysieke beveiliging en beveiliging van de omgeving
11.1 Beveiligde gebieden

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
11.1.1.1	Rijk	1	Er wordt voor het inrichten van beveiligde zones gebruik gemaakt van: a: het Kader Rijkstoegangsbeleid (2010); b: het Normenkader Beveiliging Rijkskantoren (NkBR 2015); c: het Beveiligingsvoorschrift Rijk (BVR 2013).	Secretaris/algemeen directeur

11.1.3.1	Rijk	1	Aanwijzing: NkBR 5.4	Proceseigenaar Dienstenleverancier

15. Leveranciersrelaties
15.1 Informatiebeveiliging in leveranciersrelaties

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
15.1.2	Rijk	1	VIR-BI	Proceseigenaar Dienstenleverancier
15.1.2	Rijk	1	ARBIT	Proceseigenaar Dienstenleverancier
15.1.2	Gemeente	1	GIBIT	Proceseigenaar Dienstenleverancier

16. Beheer van informatiebeveiligingsincidenten
16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen

Maatregel	Organisatie	BBN	Richtlijn	Verantwoordelijke(n)
16.1.4.1	Rijk	2	Informatiebeveiligingsincidenten die hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, behoren zo snel mogelijk (binnen 72 uur) al dan niet geautomatiseerd te worden gemeld aan het NCSC door of namens het department security contact (DSC, operationele contactpersoon voor het NCSC) of de Chief Information Security Officer (CISO).	Secretaris/algemeen directeur

Bijlage B De 10 bestuurlijke principes voor informatiebeveiliging
Behorende bij de Baseline Informatiebeveiliging Overheid (BIO)

Informatiebeveiliging en de gemeentelijke bestuurder
Gemeenten wisselen op alle beleidsterreinen informatie uit en beheren dat op vele manieren. Binnen de eigen organisatie, maar ook daarbuiten: met inwoners, ondernemers, ketenpartners en medeoverheden. Door informatie te delen kunnen gemeenten onder andere hun dienstverlening beter organiseren, de veiligheid van inwoners verbeteren en meer mensen aan het werk krijgen. Als professionele organisatie past hierbij dat gemeenten ook de beveiliging van informatie adequaat organiseren. Informatie moet immers beschikbaar, actueel, volledig en betrouwbaar zijn en mag alleen door bevoegden zijn in te zien. Bij de uitwisseling moeten gemeenten te allen tijde rekening houden met beveiligings- en privacyaspecten omdat ze een maatschappelijke en wettelijke verantwoordelijkheid hebben om de gegevens van hun inwoners onder alle omstandigheden te beschermen. De risico's rondom de vertrouwelijkheid, integriteit en beschikbaarheid van informatie(systemen) maken dat het onderwerp informatiebeveiliging niet mag ontbreken op de bestuurstafel.

Mens, proces en techniek
Informatieveiligheid is veel meer dan ICT, het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met risico's omgaat. Is de medewerker zich bewust van die risico's? Zijn bestuurders zich bewust van de risico's van en voor de organisatie? Gemeentelijke bestuurders zijn verantwoordelijk voor de informatiebeveiliging binnen gemeentelijke organisatie. Beveiliging van gegevens en systemen is een zaak van organisatie, procedures, werkprocessen en in de laatste plaats techniek. Het gaat om de mens, de manier waarop deze werkt en het gereedschap waarmee het werk verricht wordt.

Risicomanagement is de basis
De bestuurder is verantwoordelijk voor een veilige informatievoorziening. Het is daarom aan de bestuurder om de risicobereidheid te bepalen en daarmee ook te controleren of de maatregelen binnen de organisatie de risico's terugbrengen tot een voor de bestuurder acceptabel niveau. Overschrijding van dat niveau vereist expliciete besluitvorming. Risicomanagement staat daarmee aan de basis van informatiebeveiliging. Er dient een continu proces van identificatie en beoordeling van risico's plaats te vinden om te bepalen wat nodig is om informatie adequaat te beschermen. Hierbij moet worden opgemerkt dat het risico nul niet bestaat en dat het aan het bestuur is om te bepalen hoeveel of welk risico acceptabel is. En de risico's zijn talrijk: privacyschendingen door een datalek, economische schade door het uitlekken van vertrouwelijke plannen, fysieke schade door storingen in systemen in de openbare ruimte.

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

Bestuurlijke aanvulling op de normen en regels
In aanvulling op de baseline bevat dit document de bijbehorende principes voor bestuurders. Daarmee gaat dit document over waarden die u zichzelf als bestuurder oplegt. Deze waarden dienen verbonden te zijn aan de waarden van uw organisatie. Dit document is de bestuurlijke aanvulling op de baseline en helpt u om de juiste dingen te doen. De principes gaan daarom vooral over u en uw rol bij het borgen van informatiebeveiliging in uw organisatie. Deze principes ondersteunen de bestuurder bij het uitvoeren van goed risicomanagement. Informatiebeveiliging creëert waarde, voorkomt schade en draagt bij aan de bedrijfsdoelstellingen van de organisatie. Om dat te bewerkstelligen zijn de volgende principes belangrijk:

1. Bestuurders bevorderen 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 bestuurder 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 bestuurder. 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. Ik ben transparant naar de raad en zorg ervoor dat hij ook zijn rol kan pakken op dit onderwerp.

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 Security Officer (CISO), Functionaris Gegevensbescherming (FG) en Controller 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 bestuurlijk overleg 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 en als risico's een plek/paragraaf krijgen in alle bestuurlijke documenten. 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 chefsache.

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 bestuurder 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 de gemeente 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. De gemeente 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-, repressieven/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 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 bestuursniveau genomen worden, wanneer de situatie daar om vraagt.

Bijlage C Lokale governance Informatiebeveiliging gemeente Tholen

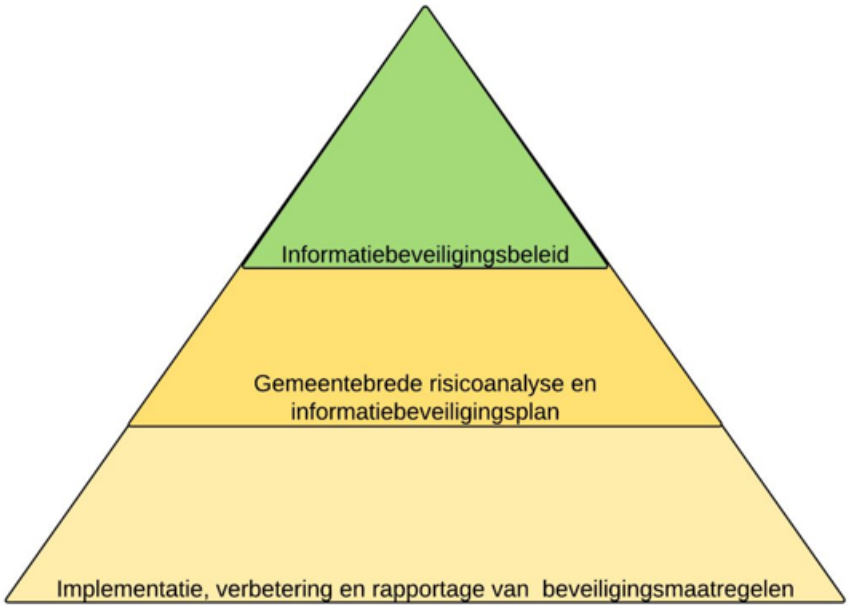
Versie	Datum	Door	Wijzigingen
1.0	01-11-2017	CISO	Eerste versie
1.1	03-10-2019	CISO	Tekstuele aanpassingen, verantwoordelijkheden afdeling overstijgende (informatie)systemen, BRO beheerder toegevoegd, term 'verantwoordelijken' omgezet in 'eigenaar', verantwoordelijkheden en taken op afdelingsniveau en teamniveau omschrijving dubbelrollen toegevoegd, organigram en piramide geactualiseerd, bij de FG meldingen AP toegevoegd, toevoeging Collegeverklaring DigiD en SUWI-officer.
1.2	25-11-2020	CISO	Rol FG aangepast
1.3	12-12-2023	CISO	Document geactualiseerd conform huidige situatie.

1. Verantwoordelijkheid en bevoegdheid informatieveiligheidsbeleid
De gemeenteraad draagt een specifieke bevoegdheid voor de controle en de toetsing op de werking van beleid binnen de gemeente, zo ook voor informatiebeveiliging. De verantwoordelijkheid voor informatiebeveiliging ligt op bestuurlijk niveau bij het college van burgemeester en wethouders en op ambtelijk niveau bij de gemeentesecretaris.

De vaststelling en implementatie van de informatiebeveiligingsstructuur en de gemeentebrede beleidsnormen vormen de verantwoordelijkheid van het college van burgemeester en wethouders van de gemeente Tholen. Voor het nemen van operationele maatregelen is de gemeentesecretaris gemandateerd. Dit geldt ook in geval van ketenafhankelijkheid en bij afdeling-overstijgende (informatie)systemen.

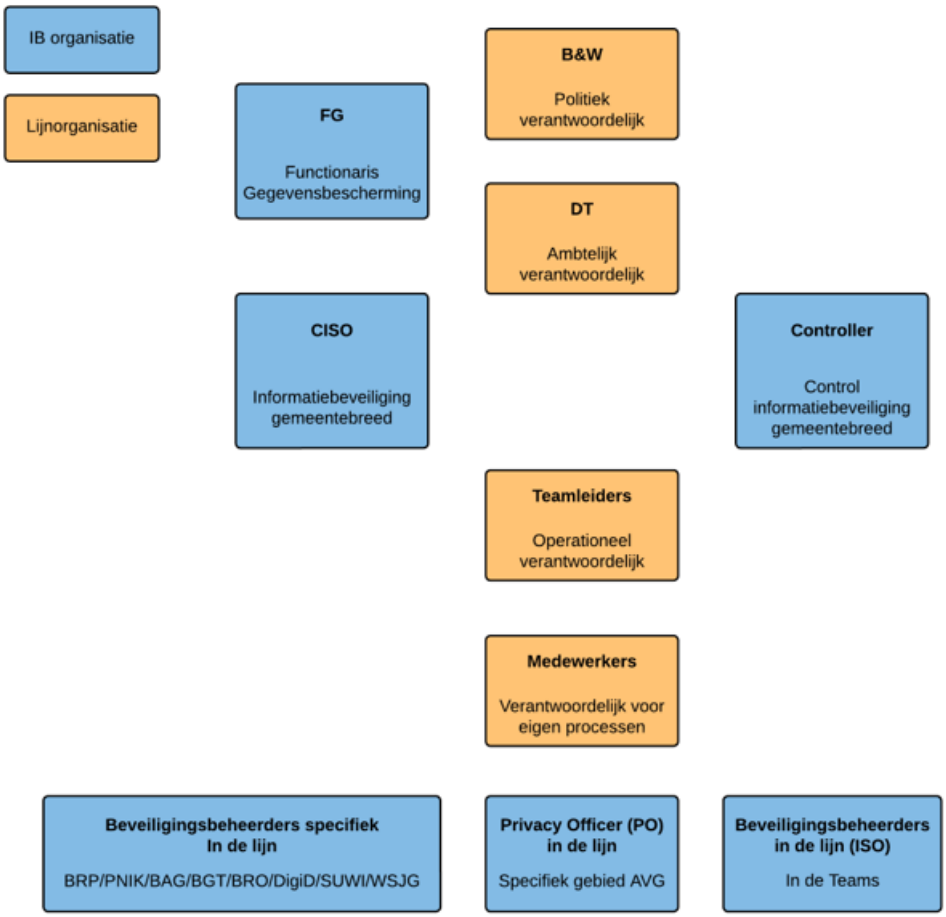
De teamleiders zijn verantwoordelijk voor de informatiesystemen en processen waarvan zij eigenaar zijn. Zij dienen deze systemen en processen te classificeren en in te richten zodat er adequate maatregelen kunnen worden getroffen om de veiligheidsrisico's te beheersen. Een belangrijk aspect van deze verantwoordelijkheid is om de medewerkers mee te nemen in hun verantwoordelijkheid ten aanzien van de veiligheid van informatie in hun dagelijkse werkprocessen.

1.1 Informatiebeveiligingspiramide



Afbeelding 1: Weergave van het strategisch informatiebeveiligingsbeleid, de tactische inrichting en de operationele uitvoering in de vorm van een piramide.

1.2 Organigram Informatieveiligheidsorganisatie



Afbeelding 2: Organigram van de informatiebeveiligingsorganisatie

2. Beschrijving van rollen, taken en verantwoordelijkheden

2.1 College Burgemeester & Wethouders

Het College van B&W van de gemeente Tholen draagt als eigenaar van gemeentelijke informatieprocessen en (informatie)systemen de politieke verantwoordelijkheid voor een passend niveau van informatiebeveiliging. Het college stelt de kaders ten aanzien van informatiebeveiliging op basis van landelijke en Europese wet- en regelgeving en landelijke normenkaders. Het college is verantwoordelijk voor een duidelijk te volgen informatieveiligheidsbeleid en stimuleert het management van de organisatieonderdelen om beveiligingsmaatregelen te nemen. Als eigenaar van informatie en (informatie)systemen heeft het college zijn verantwoordelijkheden (macht tot handelen) op het gebied van beveiliging gemandateerd aan de gemeentesecretaris.

2.2 Gemeentesecretaris

De gemandateerde verantwoordelijkheid voor informatiebeveiliging ligt bij de gemeentesecretaris. Deze stelt met het managementteam het gewenste niveau van informatiebeveiliging vast voor de gemeente. De beveiligingseisen worden per bedrijfsproces vastgesteld. De gemeentesecretaris is verantwoordelijk voor de juiste implementatie van de beveiliging in de bedrijfsprocessen en in de in- en externe (informatie)systemen en wijst voor ieder (informatie)systeem een procesverantwoordelijke of systeemeigenaar aan. De operationele verantwoordelijkheid voor deze systemen en informatieprocessen is belegd bij leidinggevenden op organisatieniveau. Degemeentesecretaris en *het* MT hebben in ieder geval de volgende verantwoordelijkheden:

- Het stellen van kaders en het geven van sturing ten aanzien van de veiligheid van informatie;
- Het sturen op concern risico's;
- Periodiek evalueren van beleidskaders en deze bijstellen waar nodig;
- Het (laten) controleren of de getroffen veiligheidsmaatregelen overeenstemmen met de betrouwbaarheidseisen en of deze veiligheidsmaatregelen voldoende bescherming bieden;
- Het beleggen van de verantwoordelijkheid voor informatiebeveiligingscomponenten en systemen;

- Het inrichten van functiescheiding tussen uitvoerende, controlerende en beleidsbepalende taken met betrekking tot informatiebeveiliging;
- Het aanwijzen van een coördinator informatiebeveiliging en een controller informatiebeveiliging.

2.3 Functionaris Gegevensbescherming

De Functionaris gegevensbescherming (FG) is intern toezichthouder op de verwerking van persoonsgegevens. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de AVG. De FG adviseert bij de implementatie van essentiële elementen van de AVG, zoals de beginselen van gegevensverwerking, de rechten van de betrokkenen, "privacy by design en privacy by default", de administratie van gegevensverwerkingen, beveiliging van het verwerkingsproces, en melding van en communicatie over datalekken. Voor de invulling van taken, verantwoordelijkheden en positionering van de FG worden de "richtlijnen voor functionarissen voor gegevensbescherming (Data Protection Officer, DPO) gevolgd van de Groep Gegevensbescherming Artikel 29, welke door de Autoriteit Persoonsgegevens (AP) is gepubliceerd waaronder:

- Controle op- en advies over naleving van de algemene verordening gegevensbescherming
- Samenwerken met de toezichthoudende autoriteit en handelen als contactpunt

2.4 Coördinator Informatieveiligheid (CISO)

Deze rol is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. De CISO ziet organisatiebreed toe op de naleving van het informatieveiligheidsbeleid en daaruit voortvloeiende maatregelen, zorgt voor onderzoek en adviseert in complexe beveiligingsvraagstukken, initieert organisatiebrede security awareness programma's en opleidingen en vervult een adviserende rol naar managementteam en gemeentebestuur. Tevens zorgt de coördinator informatiebeveiliging voor heldere communicatie bij incidenten op het vlak van informatiebeveiliging. De rol van CISO heeft een strategisch karakter. De CISO:

- Coördineert het formuleren van informatieveiligheidsbeleid en houdt dit actueel;
- Stelt het informatieveiligheidsplan op en zorgt voor de actualisatie van dat plan;
- Coördineert de uitvoering van informatieveiligheidsmaatregelen uit het informatieveiligheidsplan;
- Stelt een afstemmingsmechanisme op voor overleg en rapportage met betrekking tot informatieveiligheid;
- Ondersteunt de directie en de leidinggevenden met kennis over informatieveiligheid, zodat zij hun verantwoordelijkheid voor de betrouwbaarheid van de informatievoorziening juist kunnen invullen en initieert organisatiebrede security awareness programma's;
- Is aanspreekpunt voor medewerkers van de gemeente over het onderwerp informatieveiligheid;
- Volgt de externe invloeden die van invloed zijn op het informatieveiligheidsbeleid en het informatieveiligheidsplan;
- Zorgt voor registratie van informatieveiligheidsincidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Initieert security audits (indien van toepassing ook risico analyses);
- Rapporteert over de informatieveiligheid van de gemeente in de P&C managementrapportages;
- Ziet toe op naleving van het informatieveiligheidsbeleid en daaruit vloeiende maatregelen.

2.5 Verantwoordelijkheden en taken op teamniveau

De leidinggevenden (teamleiders) zijn verantwoordelijk voor de (informatie) veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling c.q. team. De leidinggevenden hebben in ieder geval de volgende verantwoordelijkheden:

- Het uit (laten) voeren van maatregelen uit het informatieveiligheidsplan die op de afdeling van toepassing zijn;
- Op basis van een expliciete risicoafweging opstellen van betrouwbaarheidseisen voor de afdelingsinformatiesystemen;
- De keuze, de implementatie en het uitdragen van de maatregelen die voortvloeien uit de betrouwbaarheidseisen;
- Het sturen op resultaatsafspraken, beveiligingsbewustzijn, op bedrijfscontinuïteit en op naleving van regels en richtlijnen (gedrag en risicobewustzijn);
- Het rapporteren, via de CISO, over compliance aan wet- en regelgeving en algemeen beleid van de gemeente in de P&C managementrapportages;
- Classificeren van informatie (uitgangspunt GEMMA/GIBIT);
- Verstrekken, intrekken van en controleren op autorisaties;
- Incidenteel melden van datalekken aan betrokkenen

Een persoon vervult bij voorkeur slechts één van onderstaande functies. Het is echter mogelijk om door capaciteitsgebrek als afdeling of team te beslissen om een persoon meerdere rollen te geven. Het is

echter niet wenselijk om een toezichthoudende rol te combineren met een verantwoordelijke of uitvoerende rol. Dit omdat de rol van toezichthouder in dat geval moeilijk zuiver uit te voeren valt. De slager keurt dan namelijk zijn eigen vlees.

2.6 Controller Informatieveiligheid
Deze rol is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatieveiligheidsbeleid, de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten. De Controller informatiebeveiliging:

- Toetst periodieke op de juiste naleving, de werking, de effectiviteit en de kwaliteit van de maatregelen ten aanzien van informatieveiligheid;
- Controleert de voortgang van het uitvoeren van de maatregelen uit het informatieveiligheidsplan;
- Houdt toezicht op de periodieke actualisatie van informatieveiligheidsbeleid en het Informatiebeveiligingsplan;
- Toets en bewaakt het niveau van informatieveiligheid;
- Toetst het evaluatieproces van beveiligingsincidenten.

2.7 Regiefunctionaris ICT
De Regiefunctionaris ICT is in de organisatie direct aanspreekpunt voor het ICT samenwerkingsverband ICTWBW. ICTWBW beheert de werkplekken, serverplatformen, lokale netwerken en de toegang tot straalverbindingen, externe netwerkverbindingen (zoals Gemnet en SUWInet) en verzorgt het technische (wijzigings)beheer van databases, bedrijfsapplicaties en kantoorautomatiseringshulpmiddelen. Verder zijn zij verantwoordelijk voor het (laten) realiseren van alle technische aansluitingen op andere ketenpartners en landelijke voorzieningen. Daarnaast zijn zij verantwoordelijk voor de implementatie van ICT-technische beveiligingsmaatregelen. Verantwoording over het gevoerde beheer van de getroffen beveiligingsmaatregelen wordt aan de proceseigenaren voor (informatie)systemen afgelegd.

2.8 Privacy beheerder
Deze rol is gericht op de uitvoering en de naleving van de Algemene Verordening Gegevensbescherming (AVG). De privacy beheerder is aanspreekpunt op het vlak van bescherming van persoonsgegevens en privacy binnen de organisatie en informeert en adviseert het management, bestuur en de collega's van de organisatie over de wijze waarop optimaal gebruik van informatie kan worden gemaakt. De Privacy beheerder draagt tevens bij aan de bewustwording en doorontwikkeling van Informatiebeveiliging en Privacy in de organisatie. De Privacy beheerder:

- Houdt toezicht op de naleving van specifieke regelgeving, waaronder de AVG en de Wet Basisregistratie Personen (BRP);
- Adviseert organisatiebreed over privacybescherming en over activiteiten ter bescherming van persoonsgegevens;
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Geeft aanwijzingen aan gebruikers van systemen met betrekking tot persoonsregistraties;
- Geeft (ongevraagd) advies over alle procedures en producten die betrekking hebben op de registratie van personen;
- Is contactpersoon van de gemeente voor de Autoriteit Persoonsgegevens (AP);
- Beheert het register met daarin alle persoonsregistraties die onder verantwoordelijkheid van de organisatie vallen.
- Levert een bijdrage aan de ontwikkeling van beleid, protocollen, normen, regelingen en gedragscodes.

2.9 ENSIA Coördinator
De gemeente verantwoordt zich over informatiebeveiliging middels de ENSIA-systematiek. Dit betekent dat er een ENSIA-coördinator is aangewezen. Deze zorgt ervoor dat de informatie die nodig is voor het beantwoorden van vragen binnen ENSIA wordt opgehaald bij de verantwoordelijke teamleiders. De teamleiders leveren alle informatie die nodig is voor het invullen van de jaarlijkse ENSIA-vragenlijsten. Via ENSIA verantwoordt de gemeente zich aan de toezichthouders van de stelsels waaronder DIGID/BAG/SUWI. De ENSIA- Coördinator heeft een toezichthoudende en controlerende taak op 'compliance', d.w.z. overeenstemming van de beveiligingsorganisatie met een voorgeschreven norm (ENSIA). De ENSIA Coördinator werkt aan het begeleiden, bewaken en bijsturen van het ENSIA- verantwoordingsproces, het creëren van bewustzijn over informatieveiligheid voor de hele gemeente en het organiseren van samenwerking.

2.9.1 Beveiligingsbeheerder
Deze rol is uitvoerend verantwoordelijk voor het beheer, de coördinatie en advies ten aanzien van de informatieveiligheid van specifieke gegevensverzamelingen. In wetgeving worden verschillende benamingen aan rollen gegeven voor veelal dezelfde taken en verantwoordelijkheden ten aanzien van spe-

cifieke gegevensverzamelingen. Om eenduidigheid in naamgeving te verkrijgen wordt in dit beleidsdocument de veiligheidsverantwoordelijkheid ten aanzien van een specifieke gegevensverzameling toegewezen aan, en gedefinieerd als Beveiligingsbeheerder. Hierna volgen de deelgebieden waarbij een beveiligingsbeheerder is aangewezen met vermelding van eventuele officiële rolbenaming: BRP, Reisdocumenten (officieel autorisatiebevoegde Reisdocumenten/Aanvraagstations), Rijbewijzen (Autorisatiebevoegde Rijbewijzen), BAG, SUWI (officieel Security Officer SUWI volgens het BKWI) en DigiD. Daarnaast worden er beveiligingsbeheerders aangewezen op verschillende aspecten van de gemeentelijke bedrijfsvoering: Facilitaire Zaken (gebouwenbeheer), ICT, DIV, P&O, WSJG, BRO en BGT/GEO.
De beveiligingsbeheerder is -voor het toegewezen deelgebied- verantwoordelijk voor:

- Het geheel van activiteiten gericht op de naleving en verbetering van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid en de onderliggende informatieveiligheidsplannen. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons;
- De medewerker voert interne controles uit en let op de naleving van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.2 Beveiligingsbeheerder BRP

De Beveiligingsbeheerder BRP is verantwoordelijk voor het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen Basisregistratie Personen, het toetsen op de uitvoering van regelgeving en procedures ten aanzien van de Basisregistratie Personen, de evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever Basisregistratie Personen (College B&W).
De Beveiligingsbeheerder BRP:

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.3 Beveiligingsbeheerder waardedocumenten (PNIK)

De Beveiligingsbeheerder waardedocumenten is verantwoordelijk voor het toezicht op het beheer en de ontwikkeling van beveiligingsprocessen Waardedocumenten (PNIK), het toetsen op de uitvoering van regelgeving en procedures ten aanzien van het waardedocumentenproces, de evaluatie van de beveiligingsprocessen en het verzorgen van een managementrapportage aan de opdrachtgever Waardedocumenten (College B&W). De Beveiligingsbeheerder waardedocumenten (PNIK):

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.4 Beveiligingsbeheerder BAG

De Beveiligingsbeheerder BAG is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. Hieronder vallen de preventie van beveiligingsincidenten, de detectie van dergelijke incidenten en het geven van een adequate respons. De medewerker coördineert de toepassing van specifieke wet- en regelgeving. De beveiligingsbeheerder rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

- Draagt zorg voor de BAG-gerelateerde maatregelen uit de BIO in ENSIA;
- Rapporteert de uitkomsten van de zelfevaluatie van de BAG in ENSIA aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.5 Beveiligingsbeheerder SUWI

De beveiligingsbeheerder SUWI beheert beveiligingsprocedures en -maatregelen in het kader van Suwinet, zodanig dat de beveiliging van Suwinet overeenkomstig wettelijke eisen is geïmplementeerd.
De beveiligingsbeheerder SUWI:

- Bevordert en adviseert over de beveiliging van Suwinet,en doet voorstellen tot implementatie c.q. aanpassing van plannen op het gebied van de beveiliging van Suwinet;
- Ziet er op toe dat de maatregelen worden nageleefd;
- Evalueert de uitkomsten van verbetermaatregelen;

- Verzorgt rapportages met betrekking tot de beveiligingsstatus van Suwinet aan het MT en/of college;
- Doet controles op het gebruik van Suwinet door de gemeente en vraagt daarvoor (specifieke) rapportages op bij het BKWI;
- Draagt zorg voor de ICT-gerelateerde maatregelen uit de BIO in ENSIA;
- Doet jaarlijks een zelfevaluatie op het geldende (specifieke) normenkader en stelt de Collegeverklaring op in het kader van ENSIA;
- Is aanspreekpunt tijdens de externe audit op de Collegeverklaring;
- Rapporteert de uitkomsten van de zelfevaluatie en externe audit op Suwinet aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.6 Beveiligingsbeheerder DigiD
De Beveiligingsbeheerder DigiD is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. Hieronder vallen:
- De preventie van beveiligingsincidenten en het geven van een adequate respons;
- Draagt zorg voor de DigiD-gerelateerde maatregelen uit de BIO in ENSIA;
- Doet jaarlijks een zelfevaluatie op het geldende (specifieke) normenkader en stelt de Collegeverklaring op in het kader van ENSIA;
- Rapporteert aan het college van B&W, de CISO en de Controller informatiebeveiliging.

2.9.7 Beveiligingsbeheerder Gebouwenbeheer
De Beveiligingsbeheerder Gebouwenbeheer is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op facilitaire zaken en Huisvesting en Services en is verantwoordelijk voor de fysieke toegangsbeveiliging en kantoorinrichting (archiefkasten, kluizen enzovoort).
De Beveiligingsbeheerder Gebouwenbeheer:
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de CISO en de Controller informatieveiligheid.

2.9.8 Beveiligingsbeheerder ICT
De Beveiligingsbeheerder ICT is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op ICT. De Beveiligingsbeheerder ICT is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het Informatieveiligheidsplan. De Beveiligingsbeheerder ICT:
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Draagt zorg voor de ICT-gerelateerde maatregelen uit de BIO en ENSIA;
- Rapporteert aan de CISO en de Controller informatieveiligheid.

2.9.9 Beveiligingsbeheerder DIV
De Beveiligingsbeheerder DIV is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op DIV en is verantwoordelijk voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie, het informatieveiligheidsplan en wet en regelgeving specifiek ten aanzien van DIV, waaronder de Archiefwet in relatie tot de wet Revitalisering Generiek Toezicht (RGT). De Beveiligingsbeheer DIV:
- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de CISO en de Controller informatieveiligheid.

2.9.9.1 Beveiligingsbeheerder P&O
De Beveiligingsbeheerder P&O is de directe contactpersoon voor de organisatie ten aanzien van alle activiteiten informatieveiligheid die betrekking hebben op P&O en heeft een belangrijke adviesrol op het gebied van organisatie en informatieprocessen. De Beveiligingsbeheerder P&O is verantwoordelijk

voor het geheel van activiteiten gericht op de naleving van de maatregelen en procedures die voortkomen uit het informatieveiligheidsbeleid, inclusief de normenkaders voor audit en (zelf)evaluatie en het informatieveiligheidsplan. De Beveiligingsbeheer P&O:

- Organiseert activiteiten ter voorkoming van beveiligingsincidenten;
- Zorgt voor registratie van incidenten en is verantwoordelijk voor de juiste afhandeling en evaluatie van incidenten;
- Coördineert de toepassing van specifieke wet- en regelgeving;
- Rapporteert aan de CISO en de Controller informatieveiligheid.

2.9.9.2 Functioneel applicatiebeheerder
De Functioneel applicatiebeheer is verantwoordelijk voor het geheel van activiteiten gericht op het ondersteunen van de informatiesystemen en de waarborging van continuïteit aan de gebruikerszijde van de informatievoorziening.

2.9.9.3 Certificaatbeheerder
De certificaatbeheerder beheert de elektronische sleutels van PKI/Overheid conform de voorschriften. Public key infrastructure (PKI) is het systeem waarmee uitgiften en beheer van digitale certificaten wordt gerealiseerd. Aan het gebruik zijn voorschriften verbonden ten aanzien van installatie, beveiliging, update, geldigheid en toepassing. De certificaatbeheerder is hiervoor verantwoordelijk.

2.9.9.4 Gegevensbeheerder
De Gegevensbeheerder is verantwoordelijk voor het geheel van activiteiten gericht op de inhoudelijke kwaliteitszorg betreffende het gegevens verzamelen, de gegevensverwerking en de informatievoorziening.

2.9.9.5 Gegevenseigenaar
De gegevenseigenaar (ook wel Informatie-eigenaar of Data-eigenaar) is verantwoordelijk voor de gegevens binnen een specifiek data domein. Een gegevenseigenaar moet ervoor zorgen dat de gegevens binnen zijn domein correct wordt beheerd over verschillende systemen en bedrijfsactiviteiten. Specifieke verantwoordelijkheden voor de gegevenseigenaar zijn:

- Goedkeuren van data definities;
- Zorgen voor de juistheid van informatie zoals gebruikt binnen en door de gehele organisatie;
- Datakwaliteit;
- Beoordelen en goedkeuren van de Master Data Management (MDM) aanpak, resultaten en activiteiten. MDM heeft als doel het stroomlijnen van data uitwisseling en het bieden van een enkele, consistente weergave van kritische data voor iedereen binnen de organisatie.
- Samenwerken met andere Data-eigenaren om data problemen en onbegrip tussen de verschillende bedrijfseenheden op te lossen;
- Input geven over softwareoplossingen, beleid of wettelijke vereisten die van invloed zijn op het data domein van de Data-eigenaar.

2.9.9.6 Proceseigenaar
De proceseigenaar is verantwoordelijk voor een proces. Deze verantwoordelijkheid kan meerdere aspecten betreffen:

- Het ontwerp en de invoering van het proces zelf. We onderscheiden een procesontwikkelingsverantwoordelijkheid (omvat zowel ontwerp als verbetering van het proces) en een procesimplementatie-verantwoordelijkheid (inclusief de verantwoordelijkheid voor interne audits waarmee aangetoond wordt dat het proces 'werkt');
- De resultaten van het proces. Deze procesbesturingsverantwoordelijkheid betreft de operationele beheersing en logistieke aspecten van resultaat (kwaliteit, tijd) en resourceverbruik (mensen, middelen). Het gaat daarbij om de eind- resultaten van het proces;
- Hiërarchische verantwoordelijkheid voor de medewerkers met de belangrijkste rollen in het proces.

2.9.9.7 Systeemeigenaar
De systeemeigenaar bepaalt wat er nodig is voor een optimale ondersteuning van de informatievoorziening van de bedrijfsprocessen. De systeemeigenaar (die ook proceseigenaar kan zijn) bepaalt de prioriteiten voor zowel de exploitatie als het doorvoeren van wijzigingen. Het budget betreft niet alleen de ICT-kosten, maar ook bijvoorbeeld wat beschikbaar is voor de ondersteuning door functioneel beheer. Systeemeigenaarschap is geen ICT-rol. Een systeemeigenaar mag voor wat betreft de technologie afstand nemen, maar is wel verantwoordelijk voor de informatievoorziening die nodig is voor de ondersteuning van bedrijfsprocessen.

2.9.9.8 Autorisatiebevoegde Reisdocumenten/Aanvraagstations
De Autorisatiebevoegde Reisdocumenten is verantwoordelijk voor het beheer van de autorisaties voor de reisdocumentenmodules (RAAS en aanvraagstations).

2.9.9.9 Autorisatiebevoegde Rijbewijzen De Autorisatiebevoegde Rijbewijzen is verantwoordelijk voor het beheer van de autorisaties voor rijbewijzen, inclusief aanmelding bij de RDW.
2.9.9.10 Vertrouwde Contactpersoon Informatiebeveiliging (VCIB) De VCIB krijgt waarschuwingen en informatie van de IBD met een vertrouwelijk karakter over mogelijke bedreigingen en incidenten waarvan de inhoud een vertrouwelijk karakter heeft en die niet met anderen gedeeld mogen worden.
2.9.9.11 Algemene Contactpersoon Informatiebeveiliging (ACIB) De ACIB krijgt algemene waarschuwingen en informatie van de IBD met een niet vertrouwelijk karakter over algemene bedreigingen en incidenten.

3. Overleg en afstemmingsorganen
De CISO is voorzitter van het overleg informatiebeveiliging dat 2 maal per jaar bij elkaar komt. Bij dit overleg zijn aanwezig:
- De (CISO);
- De Controller informatiebeveiliging;
- Agenda-leden: Beveiligingsbeheerders t.a.v: BRP,PNIK, BRO, BAG, SUWI, DigiD, GEO/BGT;
- Agenda-leden: Beveiligingsbeheerders t.a.v: Gebouwen, ICT, DIV en P&O;
- Agenda-lid: Privacy beheerder;
- Agenda-leden: Directielid of specialist, Regiefunctionaris ICT.

3.1 Onderwerpen
- Voortgang uitvoering maatregelen Beveiligingsplan c.q. Plan van Aanpak;
- Behandeling veiligheidsincidenten;
- Planning en voorbereiding van audits, inspecties en evaluaties;
- Evaluatie en actualisatie informatiebeveiliging en informatieveiligheidsplan;
- Actuele informatiebeveiligingsonderwerpen.

4. ICT crisisbeheersing
Voor interne crisisbeheersing is een kernteam informatiebeveiliging geïnstalleerd. Dit team komt uitsluitend bij elkaar in geval van grote incidenten of calamiteiten. Dit team bestaat o.a. uit:
- De coördinator informatieveiligheid (CISO);
- Functionaris Gegevensbescherming (FG);
- Regiofunctionaris;
- De beveiligingsbeheerder ICT;
- Betrokken MT lid (verantwoordelijk voor ICT/Informatievoorziening);
- Relevante experts;
- Een lid van het team Communicatie.

5. Rapporteren beveiligingsincidenten
De CISO wordt door de proceseigenaren geïnformeerd over beveiligingsincidenten en legt deze vast ten behoeve van rapportages. Hieronder vallen o.a. inbreuken op en (ver)storingen in de informatietechnologie, datacommunicatie of andere infrastructurele voorzieningen die gevolgen kunnen hebben voor de continuïteit en integriteit van de bedrijfsprocessen evenals signaleringen dat het informatieveiligheidsbeleid niet wordt nageleefd.
Er wordt minimaal eenmaal per jaar gerapporteerd aan het DT door de coördinator Informatieveiligheid (CISO).

6. Verantwoordelijkheden afdeling overstijgende (informatie)systemen
Afdeling overstijgende (informatie)systemen binnen de gemeente Tholen worden onder de verantwoordelijkheid van de systeemeigenaar (contracthouder) gefaciliteerd en onderhouden. Deze systemen, die door meer dan één gemeentelijk organisatieonderdeel worden gebruikt, bevatten gegevens die door meerdere organisatieonderdelen worden vastgelegd. Voor ieder afdeling overstijgend (informatie)systeem heeft de directie het primaat dit te mandateren aan een organisatieonderdeel dat daarmee verantwoordelijk wordt voor de gehele gegevensverzameling of het (informatie)systeem.
De gemandateerd eigenaar van een afdeling overstijgend (informatie)systeem draagt er zorg voor dat bij het gebruik ervan de wettelijke eisen en de gemeentelijke voorschriften (het gemeentelijk informatieveiligheidsbeleid) worden nageleefd en dat de verantwoordelijkheden voor (informatie)beveiliging voor alle betrokken partijen duidelijk omschreven zijn. De systeemeigenaar rapporteert over de mate van compliancy van overstijgende systemen en schaft waar nodig nieuwe systemen aan, escaleert meldingen over systemen wanneer niet wordt voldaan aan afspraken (SLA),

De procesverantwoordelijke maakt schriftelijk afspraken met het gemeentelijke organisatieonderdeel of de externe organisatie dat van het afdeling overstijgend (informatie)systeem gebruik maakt (de gebruikende partij).

Minimaal worden in deze afspraken vastgelegd:
- Voorwaarden voor het toegestane gebruik van het afdeling overstijgend (informatie)systeem;
- De verantwoordelijkheden van de gebruikende partij voor de gegevens uit het afdeling overstijgend (informatie)systeem;
- Voorwaarden met betrekking tot de bescherming van het verwerken van persoonsgegevens;
- Voorwaarden die de gebruikende partij verplichten voorzieningen te treffen voor een passend niveau van informatiebeveiliging;
- Procedure(s) betreffende autorisatie van medewerkers;
- Procedure(s) betreffende toezicht op de naleving van de afspraken en oplossing van eventuele geschillen;
- Het recht op inzage in de resultaten van de externe audit bij de gebruikende partij waaruit blijkt in welke mate deze aan het gemeentelijk informatieveiligheidsbeleid voldoet.

7. Contracten met derden
7.1 Service level agreement (niveau van dienstverlening)
Bij structurele / langdurige ondersteuning (externe inhuur) en/of uitbesteding van beheer van (een deel van) de (informatie)systemen, netwerken, en/of werkstations of hosting van websites wordt tussen de gemeente / een afdeling en de externe partij een Service Level Agreement (SLA) afgesloten. Hierin staan afspraken over het niveau van informatiebeveiliging en een duidelijke definitie van de verantwoordelijkheden op het gebied van informatiebeveiliging. In het ondersteunings- of uitbestedingscontract wordt verwezen naar de SLA.

7.2 Inhuur derden
Bij incidentele inhuur, bijvoorbeeld in het geval van verstoringen en calamiteiten, werkt een externe onder verantwoordelijkheid van de verantwoordelijke teamleider. Deze dient te waarborgen dat activiteiten binnen het kader van het informatieveiligheidsbeleid worden uitgevoerd.

7.3 Toegang
- Bij toegang van derden tot de gemeentelijke ICT voorzieningen gelden de onderstaande uitgangspunten:
- Informatiebeveiliging is aantoonbaar (op basis van een risicoafweging) meegewogen bij het besluit een externe partij wel of niet in te schakelen;
- Voorafgaand aan het afsluiten van een contract voor uitbesteding of externe inhuur is bepaald;
  - welke toegang (fysiek, netwerk of tot gegevens) de externe partij(en) moet(en) hebben om de in het contract overeen te komen opdracht uit te voeren en welke noodzakelijke beveiligingsmaatregelen hiervoor nodig zijn;
  - welke waarde en gevoeligheid de informatie heeft waarmee de derde partij in aanraking kan komen en of hierbij eventueel aanvullende beveiligingsmaatregelen nodig zijn;
  - hoe geauthentiseerde en geautoriseerde toegang vastgesteld wordt;

- Indien externe partijen systemen beheren waarin persoonsgegevens verwerkt worden, wordt een Standaard Verwerkersovereenkomst conform artikel 14) afgesloten;
- Er is in contracten met externe partijen vastgelegd welke beveiligingsmaatregelen vereist zijn, dat deze door de externe partij zijn getroffen en worden nageleefd en dat beveiligingsincidenten onmiddellijk worden gerapporteerd;
- Ook wordt beschreven hoe die beveiligingsmaatregelen door de uitbestedende partij te controleren zijn (bijv. audits en penetratietests) en hoe het toezicht is geregeld;
- Over het naleven van de afspraken van de externe partij wordt jaarlijks gerapporteerd.

7.4 Grote projecten
Voor grote ICT-projecten gelden specifieke, op centraal niveau vastgestelde, richtlijnen, met name ten aanzien van (Europese) aanbesteding, screening van bedrijven en juridische aspecten.

NB in een aparte bijlage staan de namen vermeld van de toegewezen rollen in de beveiligingsorganisatie. De toewijzing van de rollen wordt door het DT vastgesteld.