Vertrouwelijk

Strategisch Informatiebeveiligingsbeleid

Nationale Ombudsman 2020 t/m 2023

Document classificatie

Vertrouwelijk

Referentie documenten en informatie uit systemen

- Baseline Informatiebeveiliging Overheid
- ISO/IEC 27002:2013
- Algemene Verordening Gegevensbescherming
- Bevindingenrapport Nationale ombudsman
- Algemene Rekenkamerrapportage
- Governance Risk & Control-tool

Versiebeheer

Naam document	Strategisch Informatiebeveiligingsbeleid Nationale Ombudsman 2020 t/m 2023
Verantwoordelijke	Matthijs Kerkvliet
Auteur	Matthijs Kerkvliet
Review	Carlos Hernandez (extern adviseur)
Versienummer	1.0 (DEFINITIEF)
Datum eerste versie	6 juli 2020
Laatst bijgewerkt	2 oktober 2020

Wijzigingen			
Datum	**Versie**	**Door**	**Wijzigingen**
22 juli 2020	0.1	Matthijs Kerkvliet	Opgesteld
27 juli 2020	0.2	Edwin Valentijn	
27 juli 2020	0.2	Marjan Volgelpoel	
3 augustus 2020	0.3	Matthijs Kerkvliet	
4 augustus 2020	0.4	Matthijs Kerkvliet	
11 augustus 2020	0.5	Carlos Hernandez	i-Visie aangepast, Begrippenlijst toegevoegd Definitie informatiebeveiliging verplaatst naar begrippenlijst Paragraaf doel aangepast naar doel en scope Paragraaf standaarden verwijderd (BIO is al benoemd) Strategische doelen verplaats naar paragraaf doel en scope Informatiesystemen worden naast persoonsgegevens en overige informatie ook benoemd als belangrijke onderdeel om te beveiliging/beschermen.
	0.6	Matthijs Kerkvliet	Aanpassingen n.a.v. feedback Carlos. Verwijzingen naar privacybeleid en risicomanagement Risicomanagementparagraaf toegevoegd
24 augustus 2020	07	Carlos Hernandez	Commentaar gegeven m.b.t: • KPI's • Doelstelling ongeautoriseerde toegang • Informatieclassificatie
27 augustus 2020	0.8	Matthijs Kerkvliet	Aanpassingen n.a.v. feedback Carlos. - KPI's moeten nog geformuleerd worden. Suggesties worden daarbij meegenomen.

			- Doelstelling toegang is aangevuld met 'fysiek'. - Informatieclassificatie is aangevuld met toelichting op BBN's Versie voor BVO
21 september 2020	0.9	Matthijs Kerkvliet	Aanpassingen n.a.v. bespreking in BVO Kleine aanpassingen in rol ambtsdrager, MT-leden en vaststelling IB-beleid. Versie voor MT
2 oktober 2020	1.0	Matthijs Kerkvliet	Versie vastgesteld in MT van 1 oktober 2020

Inhoud

1 Inleiding

Informatiebeveiliging is een onderwerp die elk jaar meer aandacht krijgt dankzij technologische ontwikkelingen, dreigingen en incidenten die dagelijks plaatsvinden in de digitale wereld. In het belang van alle organisaties wordt informatiebeveiliging in alle bedrijfsprocessen geïntegreerd, zodat deze met passende maatregelen worden beschermd. Een van de passende maatregelen is het informatiebeveiligingsbeleid, waarin op strategisch niveau bepaald wordt hoe de Nationale Ombudsman met informatiebeveiliging wil omgaan. Dit beleid is richtinggevend en kaderstellend en wordt aangevuld met onderwerp specifieke beleidsdocumenten voor informatiebeveiliging op tactisch niveau en werkinstructies op operationeel niveau. Dit strategisch informatiebeveiligingsbeleid is vastgesteld in het Managementteam (MT) van <datum volgt>.

Met dit 'Strategisch Informatiebeveiligingsbeleid 2020-2023' zet de Nationale Ombudsman een volgende stap om de beveiliging van persoonsgegevens, andere informatie en informatiesystemen binnen de organisatie 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).

1.1 Ambitie en visie Nationale Ombudsman op het gebied van informatiebeveiliging

De ambitie en visie op het gebied van informatiebeveiliging volgen uit de visie van de Nationale ombudsman en die van de Kinderombudsman. Bij deze visies geldt dat het van groot belang is dat informatie en kennis goed en veilig onderling gedeeld kan worden binnen de Nationale ombudsman. Dit maakt het mogelijk om vroegtijdig nieuwe ontwikkelingen te signaleren en vroegtijdig actie te kunnen ondernemen.

"Burgers (op weg) helpen als het misgaat tussen hen en de overheid: door hen de weg te wijzen naar het juiste loket. Door ze te empoweren met adviezen en tools. En door op een effectieve manier onderzoek te doen."

"Overheden uitdagen anders te kijken naar diensten, processen en innovaties: door met een team van specialisten te kijken naar alles wat de overheid doet. Door na te

denken over manieren waarop het anders en beter kan. Met meer oog voor het perspectief van de burger. Om overheden hier vervolgens op aan te spreken. En ze uit te dagen om zaken te verbeteren."

- Visie Nationale Ombudsman 2020

"Alle kinderrechten van alle kinderen en jongeren in Nederland worden altijd nageleefd. Dit betekent dat alle kinderen en jongeren in Nederland in een geweldvrije en stimulerende omgeving kunnen opgroeien. Bij alle besluiten op alle niveaus staan de ontwikkelingsbelangen van kinderen en jongeren voorop, telt hun mening en worden ze gelijk behandeld ten opzichte van andere kinderen en jongeren."

- Visie Kinderombudsman 2020

Om burgers op weg te kunnen helpen, overheden uitdagen en de kinderrechten te kunnen beschermen, is het noodzakelijk dat wij ook op het gebied van informatiebeveiliging een visie hebben die aansluit op de in het informatiebeleid geformuleerde i-Visie. De visie op informatiebeveiliging moet bijdragen aan de collectieve visie en is als volgt geformuleerd:

"Een veilige en flexibele informatievoorziening inzetten waar men het vertrouwen krijgt dat informatie en systemen tegen kwaadwillende worden bescherm en de continuïteit wordt gewaarborgd."

- Visie op informatiebeveiliging, Nationale Ombudsman 2020

De maatregelen die de Nationale ombudsman treft op het gebied van informatiebeveiliging dienen dus het resultaat te zijn van een afweging van de elementen uit de i-Visie.

i-Visie elementen

De informatievoorziening:

- is flexibel, betrouwbaar en veilig;

- is toegesneden op de werkprocessen;
- maakt slim en optimaal gebruik van gegevens en gegevensbronnen; en
- is beheersbaar, betaalbaar en toekomstbestendig.

1.2 Leeswijzer

In hoofdstuk twee wordt de kern van het strategisch beleid uiteengezet. Dit beleid wordt op tactisch niveau aangevuld met onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid. In het jaarlijks uit te brengen Informatiebeveiligingsplan (vastgesteld door de directeur) worden deze tactische en operationele aspecten van de informatiebeveiliging verder uitgewerkt en geconcretiseerd. Dit wordt gedaan op basis van input van de managers, de CISO, het cybersecuritybeeld Nederland en de uitkomsten van audits en het jaarlijkse rechtmatigheidsonderzoek van de Algemene Rekenkamer. Wij maken hiervoor gebruik van een *Governance, Risk & Control*-tool waarin de doelstellingen op het gebied van informatiebeveiliging en de te treffen maatregelen worden bijgehouden. Hoofdstuk drie beschrijft vervolgens hoe de taken en verantwoordelijkheden in de organisatie belegd zijn en hoofdstuk vier gaat in op bewustwording op het gebied van informatiebeveiliging.

2 Strategisch beleid

Het doel van dit beleid is het presenteren van het ‘Strategisch Informatiebeveiligingsbeleid voor de jaren 2020 tot en met 2023’. De uitwerking van dit beleid in concrete maatregelen vindt plaats in het jaarlijks bij te stellen informatiebeveiligingsplan (IBP).

2.1 Strategische doelen van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid kent een aantal strategische doelen. Onderstaande opsomming beschrijft deze strategische doelen met daarbij een toelichting. De toelichting geeft houvast voor de wijze waarop het beleid in de praktijk kan worden gebracht. Dit maakt het informatiebeveiligingsbeleid ook meetbaar.

1. **Het managen van de informatiebeveiliging**
   Om informatiebeveiliging in goede banen te kunnen leiden is de informatiebeveiligingsorganisatie ingericht, zijn de middelen beschikbaar en worden de beschreven informatiebeveiligingsprocedures gevolgd. Ook hebben wij KPI's bepaald en volgen we deze nauwlettend, waardoor bijsturen snel mogelijk is.

2. **Adequate bescherming van bedrijfsmiddelen**
   Er is een overzicht van alle bedrijfsmiddelen en van deze bedrijfsmiddelen is tenminste vastgelegd wat hiervan de levensduur is en op welke wijze deze dienen te worden beschermd. Regelmatig dient te worden vastgesteld of deze bescherming ook plaatsvindt.

3. **Het minimaliseren van risico’s van menselijk gedrag**
   Er zijn maatregelen ter voorkoming van bewust en onbewust menselijk gedrag dat kan leiden tot risico's in de informatievoorziening. Voorbeelden zijn het awareness programma, maar ook het vier-ogenprincipe bij bepaalde integriteitsgevoelige handelingen of dubbele controles bij bepaalde foutgevoelige handelingen.

4. **Het voorkomen van ongeautoriseerde toegang**
   We hebben aantoonbaar een active directory die op orde is en waarbij het principe geld van 'least privilege' autorisatie. Dit geldt voor logische toegang en fysieke toegang. Dit betekent dat een gebruiker de autorisaties heeft die hij of zij nodig heeft om zijn of haar werk te kunnen doen, maar ook niet meer dan dat.

Deze active directory is gekoppeld aan de in-, door- en uitstroomgegevens van het HR-proces en wordt hier ook regelmatig op gecontroleerd.

5. **Het garanderen van correcte en veilige informatievoorzieningen**
   We werken volgens een goed en gestructureerd changemanagement proces waarbij nieuwe voorzieningen en wijzigingen op bestaande voorzieningen kritisch worden getoetst op vooraf vastgestelde veiligheidseisen. Het is niet mogelijk om buiten dit proces om nieuwe voorzieningen in gebruik te nemen of wijzigingen door te voeren.

6. **Het adequaat reageren op incidenten**
   We werken volgens een goed en gestructureerd incidentmanagementproces. Dit betekent dat alle incidenten worden geregistreerd en volgens de procedure worden afgehandeld. Ook wordt periodiek gerapporteerd aan het management over incidenten die hebben plaatsgevonden.

7. **Het beschermen van kritieke bedrijfsprocessen**
   In overleg met de proceseigenaren stellen we vast welke processen van de Nationale ombudsman kritiek zijn en treffen we maatregelen ter bescherming hiervan. Deze maatregelen dienen ter waarborging dat de juiste mensen binnen het proces de juiste bevoegdheden hebben en enkel en uitsluitend toegang hebben tot de juiste informatiesystemen ter ondersteuning van hun taak.

8. **Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers**
   We hebben beschreven in het privacybeleid en -statement op welke wijze wij persoonsgegevens verwerken en voeren hiertoe een verwerkingenregister. Het privacybeleid gaat in meer detail in op hoe wij met persoonsgegevens van burgers en medewerkers omgaan.

9. **Het waarborgen van de naleving van dit beleid**
   Informatiebeveiliging komt regelmatig terug als gespreksonderwerp in het MT en is onderdeel van de reguliere planning- & controlcyclus van de Nationale ombudsman. Dit betekent dat het beleid wordt bijgesteld bij kleine relevante wijzigingen en meer ingrijpend wordt herzien bij grote wijzigingen in de informatievoorziening én tegen het einde van de looptijd van het informatiebeveiligingsbeleid.

Het informatiebeveiligingsbeleid geldt voor alle processen van de Nationale ombudsman 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 de ambtsdragers, alle medewerkers, burgers, gasten, bezoekers en externe relaties.

Dit strategisch Informatiebeveiligingsbeleid is een algemene basis. Voor bepaalde kerntaken gelden op grond van wet- en regelgeving ook nog enkele specifieke (aanvullende) beveiligingseisen. Indien dit van toepassing is worden deze in aanvullende documenten geformuleerd.

2.2 Ontwikkelingen

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

2.2.1 Cybersecuritybeeld Nederland 2020

Het Cybersecuritybeeld Nederland 2020 (CSBN 2020) biedt inzicht in de digitale dreiging en de belangen die daardoor kunnen worden aangetast. Het gaat ook in op de weerbaarheid tegen de digitale dreiging en op de digitale risico's. Het accent ligt daarbij op de nationale veiligheid. Het CSBN wordt jaarlijks door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) vastgesteld. Dit cybersecuritybeeld is daarmee het ideale document om focus aan te brengen in het actualiseren van beleid en plannen voor informatiebeveiliging.

2.2.2 De 10 principes voor informatiebeveiliging

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

1. Ambtsdragers en de directeur 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. De directeur controleert en evalueert.

De principes gaan vooral over de rol van de ambtsdragers en de directeur bij het borgen van informatiebeveiliging in de organisatie. Deze principes ondersteunen de directeur bij het uitvoeren van goed risicomanagement.

Als er iets verkeerd gaat met betrekking tot het beveiligen van de informatie binnen de bedrijfsprocessen, dan kan dit directe gevolgen hebben voor burgers die een klacht hebben ingediend bij de Nationale ombudsman. Daarmee is informatiebeveiliging

nadrukkelijk gewenst als gespreksonderwerp tussen de ambtsdragers en de directeur van de Nationale ombudsman.

2.2.3 Baseline Informatiebeveiliging Overheid

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

2.2.4 Informatie uit incidenten en inbreuken op de beveiliging

De Nationale ombudsman kent naast het hierboven genoemde cybersecuritybeeld natuurlijk een eigen systeem waarin incidenten worden vastgelegd. Dit systeem geeft ook waardevolle informatie om van te leren en dus zijn incidenten uit het verleden ook nadrukkelijk input bij het actualiseren van het beleid.

2.3 Plaats van het informatiebeveiligingsbeleid

Dit voorliggende document beschrijft op strategisch niveau het informatiebeveiligingsbeleid. Dit beleid zal worden vertaald in tactische en operationele richtlijnen en maatregelen. Deze vertaling is er grotendeels al in de vorm van de BIO. Deze bevat een set aan maatregelen die weliswaar formeel niet verplicht zijn voor de Nationale ombudsman, maar die wij onszelf wel opleggen. Naast de BIO hanteren wij de ISO-27002:2017 standaard voor een nadere invulling van de BIO-maatregelen.

Het privacy beleid <verwijzing volgt> van de Nationale ombudsman hangt nauw samen met het informatiebeveiligingsbeleid. Tussen de maatregelen ten behoeve van het privacy beleid en het informatiebeveiligingsbeleid zit overlap. Daarom hebben de Functionaris Gegevensbescherming (FG) en de Chief Information Security Officer (CISO) regelmatig contact.

2.4 Risicomanagement

In welke mate de BIO-maatregelen afdoende zijn of dat eventueel aanvullende maatregelen nodig zijn bepalen we aan de hand van risicoanalyses. Ook daar waar BIO-maatregelen (nog) niet zijn toegepast moet een risicoanalyse inzicht geven wat de betekenis hiervan is. Risicomanagement staat centraal in informatiebeveiliging en hierbij zijn de volgende onderdelen van belang:

2.4.1 Bepalen van basisbeveiligingsniveau

Een groot deel van het denkwerk dat ten grondslag ligt aan de risicoafweging die je als organisatie moet maken is al gemaakt. Een set van basisbeveiligingsmaatregelen is namelijk al gedefinieerd in de vorm van de BIO. Als organisatie stel je vast of het basisbeveiligingsniveau (BBN) voldoet of dat aanvullend extra maatregelen vereist zijn. Het vaststellen van het vereiste beveiligingsniveau doen we met behulp van een business impactanalyse (BIA), een BIO-quickscan of een andere toets waarbij de betrouwbaarheidseisen '**Beschikbaarheid**', '**Integriteit**' en '**Vertrouwelijkheid**' (BIV) van informatie worden bepaald.

Drie basisbeveiligingsniveaus worden onderscheiden:

BBN 1: Dit is de minimale ondergrens waar alle informatiesystemen binnen de overheid aan dienen te voldoen. Dit niveau geldt dus altijd. Informatie op BBN 1 is informatie die toegankelijk mag of moet zijn voor alle medewerkers van de eigen organisatie(s). Vertrouwelijkheid is gering. Schending van vertrouwelijkheid kan enige (in)directe schade toebrengen.

BBN 2: Informatie op BBN 2 is informatie die alleen toegankelijk mag zijn voor een beperkte groep gebruikers. De informatie wordt ter beschikking gesteld op basis van vertrouwen. Schending van vertrouwelijkheid kan serieuze (in)directe schade toebrengen.

Aanvullend op BBN 1 geldt BBN 2 indien de volgende punten van toepassing zijn:

- Er wordt vertrouwelijke informatie verwerkt
- Mogelijke incidenten leiden tot bestuurlijke commotie
- De veiligheid van andere systemen is afhankelijk van de veiligheid van het eigen systeem

Wanneer een informatiesysteem is geclassificeerd op BBN 2, dan gelden de maatregelen op BBN 1 en de maatregelen op BBN 2 niveau. Het te beschermen belang (TBB) binnen

BBN 2 is maximaal Departement Vertrouwelijk (DepV) zoals gerubriceerd in het Voorschrift Informatiebeveiliging – Bijzondere Informatie (VIR-BI).

BBN 3: Informatie op BBN 3 betreft gevoelige informatie die alleen toegankelijk mag zijn voor de direct geadresseerde. Schending van vertrouwelijkheid kan zeer grote schade toebrengen. BBN 3 richt zich op de bescherming van als Departementaal Vertrouwelijk gerubriceerde informatie, waarbij weerstand geboden moet worden tegen de dreiging, zoals Advanced Persistant Threats (APT's), die uitgaat van statelijke actoren en beroepscriminelen. BBN 3 is van toepassing indien de volgende elementen van toepassing zijn:

- Verlies van informatie heeft een grote impact 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)

Wij verwachten niet dat BBN 3 voor de Nationale ombudsman aan de orde is en de Nationale ombudsman verwerkt ook geen informatie met een rubricering van STG. Confidentieel of hoger. In de risicoanalyses die wij op de informatiesystemen uitvoeren besteden we hier wel aandacht aan. Bijlage B geeft hierop een korte toelichting.

2.4.2 Informatiebeveiligingsplan

De werkzaamheden die voorkomen uit de te implementeren maatregelen van de hiervoor beschreven paragrafen worden uitgewerkt in het jaarlijks te schrijven 'Informatiebeveiligingsplan'. Het informatiebeveiligingsplan wordt vastgesteld in het MT. De voortgang van het informatiebeveiligingsplan wordt door de CISO ingebracht in het BVO en daar besproken. Indien het de voortgang betreft van onderdelen die een bredere impact hebben op de organisatie kan het BVO besluiten deze ook voor te leggen aan het MT ter bespreking. De wijze waarop we invulling geven aan risicomanagement is in meer detail beschreven in het document 'Risicomanagement'.

2.5 Uitgangspunten

De ambtsdragers, de directeur en het management spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Het management maakt een inschatting

van het belang dat de verschillende delen van de informatievoorziening voor de Nationale ombudsman heeft, de risico's die de Nationale ombudsman hiermee loopt en welke van deze risico's onacceptabel hoog zijn.

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

Het gehele management van de Nationale ombudsman geeft een duidelijke richting aan informatiebeveiliging en demonstreert dat zij informatiebeveiliging ondersteunt en zich hierbij betrokken voelt, door het uitdragen en handhaven van een informatiebeveiligingsbeleid van en voor de hele organisatie.

Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van de Nationale ombudsman en de relevante landelijke en Europese wet- en regelgeving.

2.5.1 De belangrijkste uitgangspunten van het beleid

- Alle informatie en informatiesystemen zijn van belang voor de Nationale ombudsman, bepaalde informatie is van vitaal en kritiek belang. De directeur van de Nationale ombudsman is eindverantwoordelijke voor de informatiebeveiliging.
- De uitvoering van de informatiebeveiliging is een verantwoordelijkheid van het lijnmanagement. Alle informatiebronnen en -systemen die gebruikt worden door de Nationale ombudsman hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaalt van de informatie die ze bevatten. De primaire verantwoordelijkheid voor de bescherming van informatie ligt dan ook bij de eigenaar van de informatie.
- Onder het informatiebeveiligingsbeleid liggen de maatregelen uit de BIO. Deze maatregelen vormen de basis voor de informatiebeveiliging. In de informatiebeveiligingsplannen wordt beschreven hoe en wanneer de maatregelen worden geïmplementeerd.
- Het informatiebeveiligingsbeleid vormt samen met het informatiebeveiligingsplan het fundament onder een betrouwbare informatievoorziening. In het informatiebeveiligingsplan wordt de betrouwbaarheid van de informatievoorziening organisatie breed benaderd. Het plan wordt periodiek bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.

- Informatiebeveiliging is een continu verbeterproces. ‘Plan, do, check en act’ vormen samen het managementsysteem van informatiebeveiliging.
- De Nationale ombudsman stelt de benodigde mensen en middelen beschikbaar om haar eigendommen en werkprocessen te kunnen beveiligen volgens de wijze zoals gesteld in dit beleid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

2.5.2 Praktische invulling uitgangspunten

- De directeur van de Nationale ombudsman stelt als eindverantwoordelijke het strategisch informatiebeveiligingsbeleid vast.
- De directeur stelt jaarlijks het informatiebeveiligingsplan vast in het BVO.
- De directeur is verantwoordelijk voor het (laten) uitwerken en uitvoeren van onderwerp specifieke tactische beleidsregels die aanvullend zijn op dit strategisch beleid.
- De directeur is verantwoordelijk voor het vragen om informatie bij de managers en ziet erop toe dat de managers adequate maatregelen genomen hebben voor de bescherming van de informatie die onder hun verantwoordelijkheid valt.
- 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 via het hoofd Bestuursbureau aan de directeur, voorafgaand aan de P&C-gesprekken.
- Tijdens P&C-gesprekken dient er aandacht te zijn voor de informatiebeveiliging n.a.v. de rapportage van de CISO. De onderwerpen, die als risicovol worden gezien, moeten tevens worden opgenomen in de auditplannen.
- De managers zijn verantwoordelijk voor de uitvoering van de informatiebeveiliging voor de processen waarvoor zij verantwoordelijk zijn.
- Alle medewerkers van de Nationale ombudsman worden getraind in het gebruik van beveiligingsprocedures.
- Medewerkers dienen verantwoord om te gaan met persoonsgegevens en andere informatie.

- Managers 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. Managers voeren quickscans informatiebeveiliging uit op basis van de BIO om deze risico-afwegingen te kunnen maken.

2.6 Tijdslijn strategisch informatiebeveiligingsbeleid

Dit strategisch informatiebeveiligingsbeleid heeft een looptijd van drie jaar. In die drie jaar hebben wij de volgende mijlpalen gedefinieerd:

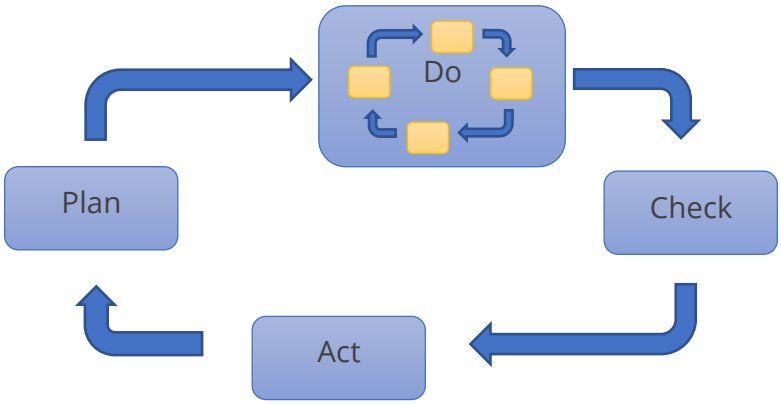
Mijlpaal	**Datum gereed**
In control op informatiebeveiliging en voldoen aan BBN 1	Eind 2020
In compliance met BIO (voldoen aan BBN 1 en 2)	Medio 2021
Informatiebeveiliging awareness programma (meerdere activiteiten)	2021
Informatiebeveiliging gestructureerd proces ondersteund met tooling	Eind 2021
Informatiebeveiliging awareness programma (meerdere activiteiten)	2022
Evaluatie strategisch informatiebeveiligingsbeleid	Eind 2022

3 Organisatie, taken & verantwoordelijkheden

In dit hoofdstuk wordt uiteengezet welke taken en verantwoordelijkheden met betrekking tot informatiebeveiliging op welke plaats belegd zijn binnen de organisatie. De methodiek sluit aan bij de in de bedrijfsvoering bekende Three Lines of Defence (3LoD). In dit model is het lijnmanagement verantwoordelijk voor de eigen processen. De tweede lijn (CISO) ondersteunt, adviseert, coördineert en bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. In de derde lijn wordt het geheel door een (interne) auditor van een objectief oordeel voorzien met mogelijkheden tot verbetering.

3.1 Planning, uitvoering, controle en bijstelling

Informatiebeveiliging voeren we uit volgens de 'Plan-Do-Check-Act' cyclus. Dit betekent dat we het beleid ontwerpen, in uitvoering nemen en vervolgens regelmatig bekijken of het beleid bijstelling behoeft. Het beleid loopt daarom mee in de reguliere planning- & controlcyclus. De uitvoering van het informatiebeveiligingsbeleid, de 'Do', bestaat uit het nemen van informatiebeveiligingsmaatregelen. Ook voor deze informatiebeveiligingsmaatregelen geldt een 'Plan-Do-Check-Act' cyclus in het klein. Immers, een maatregel komt voort uit een risicoanalyse, deze wordt geïmplementeerd en vervolgens stellen we vast of een maatregel werkt. Eventueel stellen we een maatregel bij of komt deze te vervallen als deze niet meer nodig is. Deze kleine PDCA-cyclus is het risicomanagementproces. Onderstaand figuur beschrijft beide PDCA-cycli.



Figuur 1 PDCA-cyclus voor informatiebeveiliging

Het informatiebeveiligingsbeleid heeft een looptijd van drie jaar. In 2023 loopt het beleid af en vindt een evaluatie plaats. Op basis van de evaluatie wordt het beleid bijgesteld of meer ingrijpend vernieuwd voor een nieuwe periode. Indien tussendoor ingrijpende

wijzigingen plaatsvinden in de informatievoorziening is dat ook aanleiding om het informatiebeveiligingsbeleid opnieuw te bekijken of deze nog voldoet.

3.2 Aansturing: directeur

De directeur zorgt dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid vallen van een manager. De directeur zorgt dat de managers zich verantwoorden over de beveiliging van de informatie die onder hen berust.

De directeur zorgt dat de eindverantwoordelijke ambtsdrager gevraagd en ongevraagd geïnformeerd worden over de mate waarin informatiebeveiliging een onderdeel is van het handelen van de bedrijfsvoering. Op die manier kan de Nationale ombudsman zich ook verantwoorden richting het parlement.

De directeur stelt het gewenste niveau van continuïteit en vertrouwelijkheid vast. De directeur draagt zorg voor het uitwerken van tactische informatiebeveiligingsbeleidsonderwerpen en laat zich hierin bijstaan door de CISO. De directeur autoriseert de benodigde procedures en uitvoeringsmaatregelen. Het onderwerp informatiebeveiliging wordt bij de Nationale ombudsman gezien als een integraal onderdeel van risicomanagement.

3.3 Uitvoering: managers

Informatiebeveiliging valt onder de verantwoordelijkheden van alle managers. Om deze verantwoordelijkheid waar te maken dienen zij goed ondersteund te worden vanuit de tweede lijn. Deze verantwoordelijkheid kunnen zij niet delegeren, uitvoerende werkzaamheden wel. De bedoeling is dat alle processen, systemen, data, applicaties altijd minimaal 1 eigenaar hebben; er moet dus altijd iemand verantwoordelijk zijn. Managers rapporteren aan de directeur over de door hen tactisch en operationeel uitgevoerde informatiebeveiligingsactiviteiten. Dit kan plaatsvinden in het managementteam (MT) dat wordt voorgezeten door de directeur. Afstemming met de sectoren en diensten over de inhoudelijke aanpak vindt plaats door minimaal twee keer per jaar het onderwerp Informatiebeveiliging te bespreken in het MT.

Taken van de managers in het kader van informatiebeveiliging zijn:

- het leveren van input voor wijzigingen op maatregelen en procedures;

- het binnen de eigen afdeling uitdragen van het beveiligingsbeleid, de daaraan gerelateerde procedures;
- het vroegtijdig signaleren van de voornaamste bedreigingen waaraan de bedrijfsinformatie is blootgesteld; en
- bespreking van beveiligingsincidenten en de consequenties die dit moet hebben voor beleid en maatregelen.

3.4 Uitvoering: ICT-beheer

De afdeling ICT-beheer van de Nationale ombudsman heeft als taak om de technische informatiebeveiligingsmaatregelen daadwerkelijk te implementeren voor zover dit maatregelen zijn op infrastructuur of informatiesystemen die wij zelf in beheer hebben.

Taken van ICT-beheers in het kader van informatiebeveiliging zijn:

- het implementeren van technische informatiebeveiligingsmaatregelen op de infrastructuur en applicaties die in eigen beheer zijn;
- het monitoren van de werking van technische informatiebeveiligingsmaatregelen op de infrastructuur en de applicaties van de Nationale ombudsman (zowel die in eigen beheer als die door een externe partij worden gehost);
- rapporteren over de werking van de technische informatiebeveiligingsmaatregelen op de infrastructuur en de applicaties van de Nationale ombudsman aan de CISO;
- signaleren van incidenten en hierover rapporteren aan de CISO;
- adviseren van de CISO over te treffen maatregelen op nieuwe of gewijzigde infrastructuur of applicaties van de Nationale ombudsman.

De medewerkers van de ICT-afdeling houden hun kennis op het gebied van informatiebeveiliging op peil door middel van training en opleiding en het bijwonen van bijeenkomsten van leveranciers over informatiebeveiliging.

3.5 Planning en Control: Chief Information Security Officer (CISO)

De CISO is verantwoordelijk voor de totstandkoming van het informatiebeveiligingsbeleid en ziet erop toe dat de organisatie werkt volgens de in dit informatiebeveiligingsbeleid geformuleerde principes en de daaronder ressorterende documenten zoals het informatiebeveiligingsplan en de Baseline Informatiebeveiliging Overheid (BIO). De CISO

rapporteert volgens de PDCA aan de directeur over het gevoerde informatiebeveiligingsbeleid.

Taken van de CISO zijn:

- Het organiseren van een betrouwbare en veilige informatievoorziening is de verantwoordelijkheid van de CISO.

Daartoe:

- stelt de CISO het informatiebeveiligingsbeleid op;
- toetst de CISO de naleving van het informatiebeveiligingsbeleid;
- toetst de CISO op de juiste implementatie van beheersmaatregelen uit de BIO. De CISO heeft hiertoe een tool ter beschikking waarin de voortgang per maatregel is wordt bijgehouden;
- rapporteert de CISO over het gevoerde informatiebeveiligingsbeleid volgens de PDCA via het hoofd Bestuursbureau richting de directeur;
- initieert de CISO elk jaar een informatiebeveiliging awareness programma;
- bereidt de CISO het informatiebeveiligingsoverleg voor en coördineert deze.

Het is voor de Nationale ombudsman van belang dat de kennis over informatiebeveiligingsrisico's en -maatregelen van de CISO actueel is. Daarom houdt de CISO zijn kennis op peil door middel van (online) training en opleiding. Hieruit volgt eventueel nieuwe input voor het jaarlijkse informatiebeveiligingsplan.

3.6 Control en verantwoording

De ambtsdragers en de directeur van de Nationale ombudsman zullen volgens de 10 principes voor informatiebeveiliging richting en sturing geven aan het onderwerp informatiebeveiliging door het geven van voorbeeldgedrag en het vragen om informatie.

De directeur is verantwoordelijk voor het gevraagd en ongevraagd rapporteren over informatiebeveiliging aan de ambtsdragers. De directeur rapporteert daarnaast over de mate waarin zij invulling hebben gegeven aan het uitwerken van tactische (deel) beleidsonderwerpen die aanvullend zijn op dit strategische beleid.

De verantwoording over de informatiebeveiliging komt in het jaarverslag tot uitdrukking in de bedrijfsvoeringsparagraaf. Met deze paragraaf geeft de ambtsdrager aan in hoeverre de Nationale ombudsman en de Kinderombudsman haar voornemens op het

gebied van informatiebeveiliging hebben kunnen waarmaken. Ook worden de eventuele verbetermaatregelen vermeld die de organisatie gaat treffen.

4 Bevorderen van informatiebeveiligingsbewustzijn

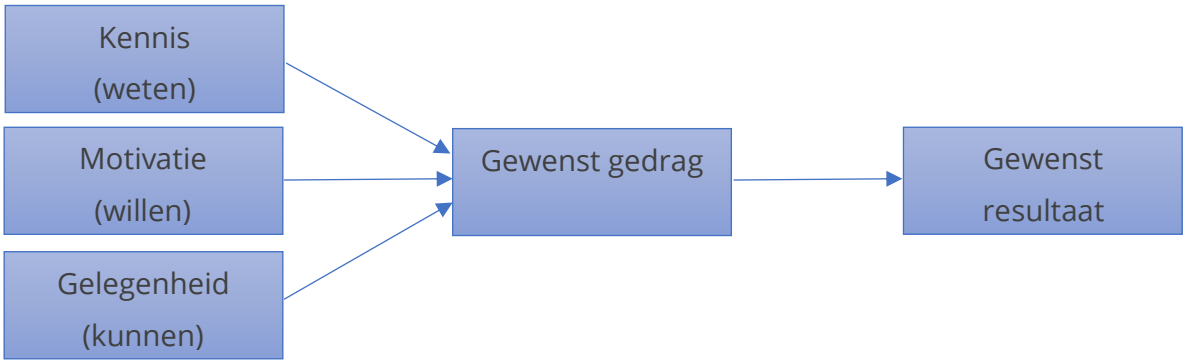
Ten behoeve van een goede informatiebeveiliging is een breed scala aan maatregelen beschikbaar. Een aantal van de maatregelen ligt, naar de aard van het te beveiligen object, op technisch vlak. Een ander deel van de maatregelen is organisatorisch van aard. Maar, het geheel van maatregelen staat of valt bij een organisatie die bewust is van informatiebeveiligingsrisico's en hier ook naar handelt.

Daarom bevat dit informatiebeveiligingsbeleid een apart hoofdstuk over informatiebeveiligingsbewustzijn.

4.1 Doelstelling

Het doel van informatiebeveiligingsbewustzijn is dat medewerkers van de Nationale ombudsman zich bewust zijn van informatiebeveiligingsrisico's en hier ook naar handelen.

Het bereiken van informatiebeveiligingsbewustzijn én het bevorderen van een veilige omgang met informatie gaat verder dan het informeren van medewerkers over informatiebeveiligingsrisico's en -maatregelen. Onderstaand schema beschrijft de determinanten die een rol spelen bij het gewenste gedrag en daarmee het gewenste resultaat.



Figuur 2 Determinanten van gewenste omgang met informatie

Het informatiebeveiligingsbewustzijnsprogramma dient aandacht te besteden aan al deze elementen om het gewenste resultaat, een veilige omgang met informatie, te realiseren. Hieruit blijkt dat voor een goede en veilige omgang met informatie meer nodig

is dan alleen het informeren van medewerkers over risico's. Veel bewustwordingsprogramma's zijn daarin te beperkt.

4.1.1 Kennis

In de eerste plaats is het van belang dat medewerkers weten wat de risico's rond het gebruik van informatie zijn en dat zij weten hoe zij geacht worden met de informatiesystemen en de gegevens daarin dienen om te gaan. Het beleid op informatiebeveiligingsbewustzijn dient daarom aandacht te besteden aan actuele dreigingen en welke rol medewerkers daarbij hebben en tenslotte hoe ze dienen te handelen in welke situatie.

Wanneer de Nationale ombudsman een informatiebeveiligingsbewustwordingscampagne start dienen de op dat moment actuele dreigingen aan bod te komen. Ook de voor de medewerkers relevante maatregelen zijn onderdeel van de campagne. Resultaat van dit onderdeel 'kennis' is dat een medewerker weet welke informatiebeveiligingsrisico's er zijn en wat hij of zij kan doen ter voorkoming van een informatiebeveiligingsincident én, indien een informatiebeveiligingsincident zich tóch voordoet, hoe dan te handelen.

4.1.2 Motivatie

Medewerkers moeten niet alleen het belang van een goede informatiebeveiliging weten, ze moeten dit ook ervaren en zich er verantwoordelijk voor (gaan) voelen. We streven ernaar om informatiebeveiligingsmaatregelen zo min mogelijk een 'last' te laten zijn voor medewerkers, maar indien een maatregel wel een extra handeling vraagt van een medewerker, dan is het bevorderlijk wanneer een medewerker hier ook zelf het nut van ervaart.

4.1.3 Gelegenheid

Wanneer een medewerker weet wat hij of zij moet doen en hier ook toe bereid is, dan moet deze ook in staat zijn om veilig met informatie om te gaan en de eventueel noodzakelijke maatregelen te treffen. De middelen die hiervoor nodig zijn moeten dan ook beschikbaar gesteld worden en eventuele barrières moeten worden weggenomen die deze veilige omgang met informatie in de weg staan.

4.2 Aan de slag met informatiebeveiligingsbewustzijn

Aan informatiebeveiligingsbewustzijn werk je continu. Het is dus een structurele activiteit. Maar, dat neemt niet weg dat het goed is om op momenten extra aandacht te besteden aan informatiebeveiligingsbewustzijn of een aspect daarvan. Dat gebeurt dan in de vorm van een informatiebeveiligingsbewustzijnscampagne. Beide vormen, dus structurele aandacht en campagnes zijn belangrijk en relevant.

4.2.1 Informatiebeveiligingsbewustzijnscampagnes

Niet iedereen is continu bezig met een veilige omgang met informatie. Daarom is het goed om hier af en toe extra aandacht aan te besteden zodat medewerkers zich weer bewust worden van de risico's en weer aandacht kunnen besteden aan hoe zij veilig en verantwoord met informatie kunnen omgaan. Dit kan in de vorm van een grote campagne waar medewerkers voor een iets langere periode regelmatig leren over informatiebeveiliging, hiertoe de middelen krijgen aangereikt en gemotiveerd worden om hiermee aan de slag te gaan.

Een andere vorm is om dit in meerdere kleine campagnes, bijvoorbeeld op een aspect van informatiebeveiliging. Voorbeelden zijn:

- een korte campagne gericht op 'phishing', waarbij medewerkers leren over de risico's, concrete handelingsperspectieven krijgen aangereikt en waar ook een aantal nep-phishingmails verstuurd worden als oefening;
- een campagne gericht op wachtwoorden, eventueel in combinatie met de uitrol van een paswoordenmanager. Medewerkers leren dan het belang van sterke wachtwoorden en krijgen bovendien de middelen aangereikt om dit goed in de praktijk te brengen; en
- een campagne gericht op informatiebeveiliging in combinatie met fysieke beveiliging waarbij medewerkers leren over het veilig en afgesloten achterlaten van een werkplek en wat te doen wanneer zij een onbekend persoon treffen op de afdeling.

4.2.2 Structurele aandacht voor informatiebeveiligingsbewustzijn

Het voordeel van bewustwordingscampagnes is de aandacht die deze genereren. Het nadeel van de bewustwordingscampagnes is dat die aandacht vaak snel genoeg weer wordt ingehaald door de dagelijkse praktijk en uiteindelijk ook door oude gewoontes. Het is daarom van belang dat informatiebeveiliging ook buiten campagnes onder de aandacht komt van medewerkers. Dit kan op meerdere manieren plaatsvinden.

Zo is het mogelijk om via e-learning of fysieke opleiding het kennisniveau op peil te houden en te oefenen met (gesimuleerde) praktijksituaties. Ook moet informatiebeveiliging structureel een plek hebben in het introductieprogramma voor alle nieuwe medewerkers. Maar voor de leidinggevende ligt ook een taak in het aanspreken van de medewerker op informatieveilig gedrag. Dit kan bijvoorbeeld meelopen in de P&O-cyclus, dus een terugkomend aandachtspunt in het functioneringsgesprek.

4.2.3 Informatiebeveiligingsbewustzijn in het informatiebeveiligingsplan

Het informatiebeveiligingsplan beschrijft welke informatiebeveiligingsbewustzijnsactiviteiten plaats zullen vinden. Jaarlijks wordt dus vastgesteld welke activiteiten op dit gebied aan de medewerkers zullen worden aangeboden en in welke mate dit verplicht of vrijwillig is.

Bijlage A: Begrippenlijst

- **Informatiebeveiliging**: onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket van maatregelen om de betrouwbaarheid van de informatievoorziening aantoonbaar te waarborgen. Betrouwbaarheid wordt uitgedrukt in beschikbaarheid, integriteit (juistheid) en vertrouwelijkheid van persoonsgegevens, andere informatie en informatiesystemen.
- **Beschikbaarheid**: Beschikbaarheid beschrijft hoeveel en wanneer data toegankelijk is en gebruikt kan worden.
- **Integriteit**: Integriteit betreft het in overeenstemming zijn van informatie met de werkelijkheid en dat niets ten onrechte is achtergehouden of verdwenen (juistheid, volledigheid en tijdigheid).
- **Vertrouwelijkheid**: Vertrouwelijkheid behelst de bevoegdheden en de mogelijkheden tot muteren, kopiëren, toevoegen, vernietigen of kennisnemen van informatie voor een gedefinieerde groep van gerechtigden.
- **Risico**: Een risico is in het kader van informatiebeveiliging een ongewenste gebeurtenis die we willen voorkomen. In een formule is het risico uit te drukken als: Risico = Kans x Schade.
- **Dreiging**: Een dreiging is een kans op schade.
- **Persoonsgegevens**: Persoonsgegevens zijn alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.
- **Informatiebeveiligingsplan**: het informatiebeveiligingsplan is een onderdeel van het informatieplan en beschrijft de activiteiten die in een bepaald jaar uitgevoerd zullen worden.

Bijlage B: Risicoanalyse en bijzondere informatie

Toelichting op BBN 3

BBN3 bestaat uit de controls- en overheidsmaatregelen uit BBN 2, aangevuld met relevante eisen uit het VIR-BI, relevante bepalingen uit regelingen andere overheidslagen en uit het NAVO-verdrag voor de beveiliging van informatie. Niet alle delen/maatregelen zijn van toepassing voor de nationale context en voor NATO Restricted. In de uitwerking van BBN 3 zal daarom specifiek aangegeven worden welke delen/maatregelen van het NAVO-verdrag specifiek van toepassing zijn.

Uitvoeren risicoanalyse

Wanneer uit de bepaling van het basisbeveiligingsniveau blijkt dat die op BBN 3 of hoger ligt is het uitvoeren van een meer verdiepende risicoanalyse verplicht. Het doel van deze risicoanalyse is om vast te stellen welke risico's er niet worden afgedekt met de basismaatregelen uit de BIO en welke aanvullende maatregelen nodig zijn om die risico's alsnog af te dekken. Voor de risicoanalyse doorlopen we drie stappen.

1. Het bepalen van de scope van de risicoanalyse conform het MAPGOOD-model[1]
2. Het in kaart brengen van de dreigingen en kwetsbaarheden
3. Het bepalen van de risico's
4. Het vertalen van de meest relevante dreigingen naar maatregelen die moeten worden getroffen.

Rubricering van informatie

Het Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIR-BI) beschrijft de maatregelen die een overheid dient te treffen voor de omgang met bijzondere informatie. Bijzondere informatie is informatie die een van de volgende rubriceringen toegekend heeft gekregen:

- **Staatsgeheim ZEER GEHEIM (afgekort Stg.ZG)**

[1] MAPGOOD staat voor Mens, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving, Diensten

Indien kennisname door niet geautoriseerden zeer ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten

- **Staatsgeheim GEHEIM (afgekort Stg.G)**
  Indien kennisname door niet geautoriseerden ernstige schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
- **Staatsgeheim CONFIDENTIEEL (afgekort Stg.C)**
  Indien kennisname door niet geautoriseerden schade kan toebrengen aan een van de vitale belangen van de Staat of zijn bondgenoten
- **Departementaal VERTROUWELIJK (afgekort Dep.V.)**
  Indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries.

Het toekennen van het juiste rubriceringsniveau is aan de eigenaar van de informatie. Deze eigenaar is er dan ook voor verantwoordelijk om de maatregelen te treffen die vereist zijn bij het gekozen rubriceringsniveau.