BASELINE INFORMATIEBEVEILIGING OVERHEID 2

BIO 2

9 januari 2026, versie 1.3 definitief

BIO | Baseline Informatiebeveiliging Overheid

Rijksoverheid VNG ip Interprovinciaal Overleg van, voor en door provincies UNIE VAN WATERSCHAPPEN

COPYRIGHT-NOTITIE

Deel 1 BIO2-kader van de Baseline Informatiebeveiliging Overheid 2 (BIO2) is gestructureerd volgens NEN-EN-ISO/IEC 27001:2023, en deel 2 BIO-overheidsmaatregelen van de BIO2 is gestructureerd volgens NEN-EN-ISO/IEC 27002:2022. Entiteiten kunnen kosteloos beschikken over deze normen via NEN connect, het digitale platform van het Nederlands Normalisatie Instituut (NEN).

Forum Standaardisatie heeft deze normen opgenomen in de 'pas-toe-of-leg-uit'-lijst met verplichte standaarden voor de publieke sector. Dit betekent dat de overheid deze normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen. De BIO2 beschrijft de invulling van NEN-EN-ISO/IEC 27001:2023 en NEN-EN-ISO/IEC 27002:2022 voor de overheid. De BIO2 vervangt deze twee normen niet, maar vult ze aan.

NEN-EN-ISO/IEC 27001 en NEN-EN-ISO/IEC 27002 beschrijven de details voor implementatie (richtlijnen) en eisen voor de procesinrichting (onder andere het ISMS uit NEN-EN-ISO/IEC 27001). ISO 27001 is verplicht voor het inrichten van het managementsysteem voor informatiebeveiliging. Daar waar de BIO2 niet expliciet iets voorschrijft, worden beide ISO-normen gebruikt, om te komen tot een goede inrichting voor risicomanagement. Deze ISO-normen geven dus de details voor de toepassing, die niet in de BIO2 zijn beschreven en die nodig blijven voor een goede implementatie van de BIO2.

Het gebruik van informatie uit NEN-EN-ISO/IEC 27001 en NEN-EN-ISO/IEC 27002 in de BIO is auteursrechtelijk beschermd. Het gebruik van teksten uit deze normen in de BIO geschiedt met toestemming van NEN. Voor meer informatie over de NEN en het gebruik van hun producten zie: www.nen.nl.

WIJZIGINGSBEHEER

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is stelselverantwoordelijke voor de BIO. Zij heeft het beheer van de BIO bij het Centrum Informatiebeveiliging en Privacybescherming (CIP) belegd.

Versie	Datum	Wijziging	Door
1.0 concept	05-03-2025	Eerste online gepubliceerde conceptversie met instemming van het kern-IBO.	BZK
1.1 concept	14-04-2025	Tweede online gepubliceerde conceptversie: • Versie en status toegevoegd. • Enters tussen overheidsmaatregelen toegevoegd als er meerdere maatregelen binnen één nummer bestaan. • Diverse tekstuele verbeteringen.	CIP
1.1.1 concept	05-08-2025	Versie voor goedkeuring door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO): • Herstel onvolkomenheden in kolom 'draagt bij aan'. • Verduidelijken paragraaf risico-identificatie. • Consistentie in termgebruik. • Overbodige overheidsmaatregel 7.07.02 verwijderd.	CIP

Versie	Datum	Wijziging	Door
1.2 definitief	24-09-2025	• Door het OBDO vastgestelde versie. • Opmaak in huisstijl. • Toevoeging wijzigingsbeheertabel. • Overheidsmaatregel 5.18.1 verwijderd vanwege maatregel 5.18.2 en 5.18.3. • Overheidsmaatregel 7.07.02 verwijderd vanwege maatregel 7.07.01.	CIP
1.3 definitief	09-01-2026	• Aanpassingen vanwege BIO2 als wetgeving. • Overheidsmaatregelen buiten Cbw-reikwijdte grijs gemarkeerd. • 5.24.08 toegevoegd en vanuit 8.08.06 ernaar verwezen. Verwijderd: • Derde alinea van 2. Doel van de BIO is in § Cyberbeveiligingswet (Cbw) beschreven. • Eerste alinea van 3. Toepasing BIO is beschreven in 1. Leeswijzer. • Typen hygiënen en overheidsrisico. • 5.21.01 is beschreven in 5.21.03. • Nationale in 5.24.07 vanwege Cbw. • 5.35.01 is beschreven in Deel 1 BIO2-kader. • 7.01.01 is onvoldoende concreet. • Eerste alinea van 7.10.02 is beschreven bij 7.10.01. • 8.24.03 is indirect beschreven bij 8.24.01. Verplaatste overheidsmaatregelen: • Eerste deel van 5.01.01 naar 5.02.01. • 5.04.02 naar 5.10.02. • 5.04.03 naar 5.10.03. • 5.24.06 naar 5.21.05. • 5.25.01 naar 5.26.01. • 5.26.01 naar 5.25.01. • Eerste bullet van 8.01.02 naar 6.03.04. • 08.08.06 met een verwijzing naar 5.24.02.	CIP

DANKWOORD

Wij danken iedereen die direct of indirect heeft bijgedragen aan de totstandkoming van de BIO2. In willekeurige volgorde danken wij de vertegenwoordigers van de koepelorganisaties (Vereniging van Nederlandse Gemeenten, Interprovinciaal Overleg en Unie van Waterschappen), Chief Information Security Officers (CISO's) van overheidseniteiten, de Auditdienst Rijk (ADR), de Rijksinspectie Digitale Infrastructuur (RDI), het Nationaal Cyber Security Centrum (NCSC), het Centrum Informatiebeveiliging en Privacybescherming (CIP), de informatiebeveiligingsdienst voor gemeenten (IBD), de leden van de werkgroep BIO, bestuurders en functionarissen van overheden en alle anderen die hebben bijgedragen.

INHOUD

Copyright-notitie ***2***

Wijzigingsbeheer ***2***

Dankwoord ***3***

Inhoud ***4***

Deel 1 BIO2-kader ***5***

1. Leeswijzer **5**

2. Doel van de BIO **5**

3. Toepassing BIO **5**

4. Verplichtingen BIO **6**

5. Het managementsysteem voor informatiebeveiliging **6**

5.1. Reikwijdte managementsysteem 7

5.2. Samenhang managementsystemen 7

6. Risicomanagement **7**

6.1. Contextbepaling 7

6.2. Kiezen risicomanagementmethodiek 7

6.3. Risico-identificatie 7

6.4. Risicoanalyse 8

6.5. Risicobehandeling en maatregelenselectie 8

7. Verklaring van toepasselijkheid (VvT) **8**

8. Monitoring en continue verbetering **8**

9. Transparantie en verantwoording **8**

10. Toezicht **9**

11. Toepasselijke overige normen, wet- en regelgeving **9**

11.1. Cyberbeveiligingswet (Cbw) 9

12. Governance **10**

12.1. Bestuurder 10

12.2. Lijnmanagement 10

12.3. CISO 10

12.4. Interne toezichthouder 11

13. Leveranciers **11**

14. Informatiebeveiligingsprincipes **11**

15. Operationaliseren maatregelen/balans in de maatregelenset **11**

16. Treffen aanvullende maatregelen **11**

17. Impact van risico's **11**

18. Relatie BIO en andere onderwerpen **12**

Deel 2 BIO–overheidsmaatregelen ***13***

DEEL 1 BIO2-KADER

De overheid vervult een essentiële rol in de samenleving door bij te dragen aan de democratische rechtsstaat en het bieden van diensten aan burgers en bedrijven. Deze verantwoordelijkheden vereisen een zorgvuldige omgang met informatie en gegevens. Om deel te kunnen nemen aan de samenleving moeten burgers en bedrijven informatie met de overheid delen en zijn zij afhankelijk van de overheid om informatie te ontvangen. De overheid heeft vanuit deze unieke rol de plicht om zorgvuldig om te gaan met deze informatie.

De Baseline Informatiebeveiliging Overheid (BIO) is het normenkader voor informatiebeveiliging binnen alle overheidsentiteiten. Het biedt richtlijnen, algemene principes en verplichte overheidsmaatregelen voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen de overheid en haar ketens.

1. Leeswijzer

De Baseline Informatiebeveiliging Overheid 2 (BIO2) is opgebouwd uit twee delen:

1. **Deel 1 BIO2-kader** - de context en het belang van informatiebeveiliging voor entiteiten, evenals de structuur en toepasselijkheid van de BIO.
2. **Deel 2 BIO-overheidsmaatregelen** - verplichte maatregelen, gebaseerd op de internationale norm NEN-EN-ISO/IEC 27001, bijlage A (normatief) Referentie voor beheersmaatregelen voor informatiebeveiliging, aangevuld met specifieke overheidseisen.

Deze twee delen vormen een compleet kader voor informatiebeveiliging binnen de overheid. Er worden voor de ISO-normen in dit document alleen jaartallen vermeld als dit van belang is. Daar waar gerefereerd wordt aan een andere norm is geen jaartal vermeld en wordt de meest actuele versie bedoeld.

2. Doel van de BIO

Het doel van de BIO is om de informatieveiligheid overheidsbreed op een gemeenschappelijk basisniveau te brengen en daardoor ook de ketenpartners een basis van vertrouwen te geven bij gegevensuitwisseling.

Daarnaast biedt de BIO een basis voor entiteiten om zowel intern als extern transparant te zijn over de wijze waarop informatiebeveiliging is ingericht. Met de BIO hanteert de overheid één gezamenlijke taal en een gezamenlijk doel voor informatiebeveiliging.

3. Toepassing BIO

De BIO is van toepassing op de informatiebeveiliging van alle typen omgevingen, onder andere operationele technologie (OT) en zorginformatie. De BIO brengt deze op het noodzakelijke niveau met behulp van normen en richtlijnen zoals NEN 7510 Informatiebeveiliging in de zorg en Cybersecurity implementatierichtlijn (CSIR).

Deel 1 BIO2-kader en het bijbehorende deel 2 BIO-overheidsmaatregelen hebben een verplichtend karakter en worden altijd gevolgd.

Een informatiesysteem is '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.' Het gaat dus expliciet niet alleen om technische (ICT-)systemen, maar informatie en organisatie.

4. Verplichtingen BIO

De BIO stelt de volgende verplichtingen aan entiteiten:

- **NEN-EN-ISO/IEC 27001 wordt toegepast op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatiebeveiliging en het vaststellen van het toepassingsgebied van dit managementsysteem**. De BIO schrijft voor dat het managementsysteem van een entiteit voldoet aan NEN-EN-ISO/IEC 27001. Voor het bepalen van de context van de entiteit neemt de entiteit minimaal de bedrijfsprocessen en informatiesystemen op die kritisch zijn voor haar dienstverlening bij het inrichten, implementeren, in stand houden en continu verbeteren van het managementsysteem voor informatiebeveiliging.
- **NEN-EN-ISO/IEC 27002 en de verplichte overheidsmaatregelen uit de BIO worden toegepast op het formuleren van passende beheersmaatregelen**. Hierbij wordt rekening gehouden met de omgeving(en) waarin de informatiebeveiligingsrisico's gelden, gebaseerd op de scope en de onderkende risico's. De beheersmaatregelen uit NEN-EN-ISO/IEC 27002 en de BIO kunnen, waar nodig én gelijkwaardig worden vervangen of gecombineerd met beheersmaatregelen uit andere normen en richtlijnen, zoals voor zorginformatie NEN 7510 en voor Operationele Technologie (OT) de CSIR en IEC 62443 Industriële cybersecurity.
- **Entiteiten tonen opzet, bestaan en werking van maatregelen aan**. Dit vereiste volgt ook uit de Cbw/Network and Information Security directive 2 (NIS2). De BIO omvat overheidsmaatregelen op tactisch niveau. Dit betekent dat deze maatregelen door de entiteit eerst geoperationaliseerd worden voordat ze geïmplementeerd kunnen worden. Deze implementatie is risicogericht en voldoet aan best practices en marktstandaarden. Onderdeel van de operationalisatie is het kunnen detecteren of de maatregel goed functioneert. Over het hele ontwerp wordt geborgd dat uitval van één maatregel niet leidt tot een directe kwetsbaarheid in het hele systeem.
  Hoe de maatregelen zijn geoperationaliseerd, wordt via verwijzingen vastgelegd. Hiermee toont een entiteit de 'opzet' van maatregelen aan. Al dan niet met behulp van externe partijen en/of via self-assessments, audits, pentesten, redteam-testen en dergelijke toont een entiteit het 'bestaan' en de 'werking' aan van maatregelen aan.

5. Het managementsysteem voor informatiebeveiliging

Het managementsysteem voor informatiebeveiliging (information security management system, ook wel ISMS) is een werkwijze om informatiebeveiliging op een gestructureerde manier toe te passen binnen de entiteit. Zo wordt de entiteit, en een bestuurder in het bijzonder, in staat gesteld om de juiste afwegingen te maken.

Om een veelvoorkomend misverstand te voorkomen: een managementsysteem is géén applicatie. Een applicatie kan wel ondersteunen bij het toepassen van een managementsysteem.

Het managementsysteem voor informatiebeveiliging borgt de beschikbaarheid, integriteit en vertrouwelijkheid van informatie door een risicomanagementproces toe te passen. Dit geeft belanghebbenden het vertrouwen dat risico's adequaat worden beheerd.

Het is belangrijk dat het managementsysteem voor informatiebeveiliging deel uitmaakt van en geïntegreerd is met de procedures van de entiteit en met de algehele managementstructuur, en dat informatiebeveiliging in aanmerking wordt genomen bij het ontwerpen van processen, informatiesystemen en beheersmaatregelen.

5.1. Reikwijdte managementsysteem

Bij het bepalen van de reikwijdte van het managementsysteem neemt een entiteit minimaal de bedrijfsprocessen en informatiesystemen op die kritisch zijn voor haar dienstverlening. Zij bepaalt in welke mate de ondersteunende processen worden opgenomen in het managementsysteem.

Waar overheden gelijkwaardige processen hanteren, is het aanbevolen om, waar beschikbaar, gebruik te maken van het ondersteuningsaanbod van de koepelorganisatie.

5.2. Samenhang managementsystemen

De BIO sluit aan op de Harmonized Structure (HS), wat een consistente en uniforme structuur biedt voor managementsystemen, waardoor de integratie van verschillende (ISO-)normen voor managementsystemen wordt vereenvoudigd. Hierdoor wordt dubbel werk voorkomen en middelen efficiënter gebruikt. Het biedt uniformiteit bij de implementatie van verschillende managementsystemen en vereenvoudigt de integratie van deze systemen.

6. Risicomanagement

Risicomanagement is een kernonderdeel van NEN-EN-ISO/IEC 27001 en vormt ook de basis van de BIO-aanpak binnen de overheid. De processen zijn ontworpen om risico's systematisch te identificeren, beoordelen, beheersen en continu te monitoren. Het risicomanagementproces verloopt in hoofdlijnen als volgt:

1. Contextbepaling
2. Kiezen risicomanagementmethodiek
3. Risico-identificatie
4. Risicoanalyse
5. Risicobehandeling en maatregelenselectie

6.1. Contextbepaling

NEN-EN-ISO/IEC 27001 vereist dat een entiteit eerst haar context vaststelt om relevante informatiebeveiligingsrisico's te identificeren. Dit omvat zowel interne als externe factoren die invloed hebben op de beveiliging van informatie(systemen), en de daarmee samenhangende wettelijke verplichtingen uit de Cbw.

6.2. Kiezen risicomanagementmethodiek

Een entiteit kiest een risicomanagementmethodiek en past deze toe die aansluit bij NEN-EN-ISO/IEC 27001. Een risicomanagementmethodiek omvat ten minste de volgende onderdelen:

- een quickscan om te bepalen of het basisniveau toereikend is of dat aanvullende maatregelen noodzakelijk zijn en waarin de classificatie van een proces en een informatiesysteem wordt uitgevoerd
- een methode voor een volledige risicoanalyse om te komen tot aanvullende maatregelen
- een risicoregister met daarin de tijdelijk geaccepteerde risico's
- een proces voor opvolging van risico's om tijdelijk geaccepteerde risico's structureel op te lossen

6.3. Risico-identificatie

De entiteit:

- stelt vast welke waardevolle informatie(verwerkende) middelen aanwezig zijn;
- brengt de relevante bedreigingen in kaart die daarop van invloed kunnen zijn;
- identificeert kwetsbaarheden;

- bepaalt wat de potentiële consequenties zijn als deze bedreigingen zich daadwerkelijk manifesteren.

Hierbij worden uiteenlopende dreigingen en mogelijke scenario's systematisch geïnventariseerd. Verschillende hulpmiddelen zoals NEN-ISO/IEC 27005 of het Cybersecurity Framework (CSF) en SP 800-30 van National Institute of Standards and Technology (NIST) kunnen gebruikt worden. Voorbeelden hiervan zijn dreigingen die voortkomen uit ketenafhankelijkheden, op OT, of gegevensuitwisseling met zorginstellingen.

6.4. Risicoanalyse

De geïdentificeerde risico's worden vervolgens geanalyseerd en geclassificeerd op basis van hun waarschijnlijkheid en impact. De entiteit gebruikt in dit proces NEN-EN-ISO/IEC 27001 voor het uitvoeren van risicoanalyses, ondersteund door richtlijnen uit de BIO. Het classificeren van risico's draagt bij aan een consistent beeld van de risicoprioriteiten binnen de entiteit en de overheid als geheel.

6.5. Risicobehandeling en maatregelenselectie

Er worden na de risicoanalyse passende beheersmaatregelen geselecteerd om risico's te beheersen. NEN-EN-ISO/IEC 27001, bijlage A (normatief) Referentie voor beheersmaatregelen voor informatiebeveiliging, biedt een reeks beheersmaatregelen, die nader uitgewerkt zijn in NEN-EN-ISO/IEC 27002. De BIO vult deze aan met verplicht toe te passen overheidsmaatregelen die aansluiten op de context van de overheid. Deze overheidsmaatregelen zijn altijd verplicht en kunnen ongeacht de risico-inschatting van de entiteit niet geaccepteerd worden, tenzij ze niet van toepassing kunnen zijn.

7. Verklaring van toepasselijkheid (VvT)

NEN-EN-ISO/IEC 27001 vereist dat entiteiten een VvT opstellen, waarin zij de geselecteerde beheersmaatregelen vastleggen en toelichten welke maatregelen zijn geïmplementeerd. Voor entiteiten geldt dat zij hierin ook de overheidsmaatregelen expliciet opnemen. Eventuele afwijkingen of niet-toepasbare beheersmaatregelen worden in een bijlage 'Uitzonderingen op de VvT' opgenomen.

8. Monitoring en continue verbetering

De implementatie van de BIO kan niet afgedaan worden met een eenmalig project. Informatiebeveiliging is een cyclisch proces. NEN-EN-ISO/IEC 27001 en de BIO leggen de nadruk op een continu verbeterproces. Door het toepassen van een managementsysteem blijft een entiteit continu ontwikkelen en verbeteren. Een entiteit onderhoudt haar managementsysteem en evalueert regelmatig om de effectiviteit van beheersmaatregelen te waarborgen. Wijzigingen in wetgeving of nieuwe bedreigingen kunnen aanleiding geven tot het bijwerken van de risicoanalyse en beheersmaatregelen. Met interne audits, managementbeoordelingen en gestroomlijnde documentatie binnen het ISMS houdt de entiteit haar risicomanagement actueel.

9. Transparantie en verantwoording

Burgers moeten erop kunnen vertrouwen dat de overheid uiterst zorgvuldig met gegevens omgaat. Dit wordt ook bereikt door transparant te zijn over de inrichting en de staat van informatieveiligheid en daar verantwoording over af te leggen.

Iedere overheidsorganisatie legt verantwoording af over de staat van de informatieveiligheid via de geldende verantwoordingskaders en aan de relevante toezichthoudende instanties. Informatieveiligheid is een standaard onderdeel van het jaarverslag van de organisatie. Voor veilige onderlinge samenwerking tussen

overheidsorganisaties, geven overheidsorganisaties elkaar inzicht in de getroffen maatregelen. Hierbij wordt gebruik gemaakt van de VvT.

10. Toezicht

De BIO-aanpak is de basis voor het invullen van de zorgplicht uit de Cbw door overheidsentiteiten. NEN-EN-ISO/IEC 27001 en NEN-EN-ISO/IEC 27002 vormen de basis van de BIO. Het is aangeraden voor toezichthouders om deze standaarden te hanteren. De elementen uit het ISMS vormen de basis om het managementsysteem te toetsen, inclusief de verplichte overheidsmaatregelen uit de BIO.

De BIO verplicht geen NEN-EN-ISO/IEC 27001-certificering. Certificering draagt wel bij aan het vereenvoudigen van de verantwoording en geeft op basis van een onafhankelijke beoordeling aan dat de entiteit in staat is om informatiebeveiliging procesmatig uit te voeren.

11. Toepasselijke overige normen, wet- en regelgeving

De BIO bevat overheidsmaatregelen die in lijn zijn met andere wet- en regelgeving, maar is daarin zeker niet uitputtend. De BIO is expliciet niet bedoeld om alle beveiligingseisen van de overheid af te dekken. De verschillende overheidslagen hebben te maken met specifieke dreigingen. Overheidslagen kunnen specifieke aanvullende maatregelen benoemen en die, afhankelijk van de interne besluitvorming, verplichtend of adviserend door te voeren. Daarnaast is elke entiteit zelf verantwoordelijk om vast te stellen welke interne en externe eisen, waaronder ook wet- en regelgeving, van toepassing zijn.

Binnen de overheid gelden meerdere normen voor informatiebeveiliging. Naast de BIO zijn er bijvoorbeeld de Nederlandse normen NEN 7510 Informatiebeveiliging in de zorg voor verwerkers van zorginformatie, NEN-EN-ISO 22301 Managementsystemen voor bedrijfscontinuïteit en crisismanagement en de CSIR voor OT. De basis van deze normen is NEN-EN-ISO/IEC 27001 en NEN-EN-ISO/IEC 27002. Managementsystemen en beheersmaatregelen volgens deze normen kunnen worden geïntegreerd in een managementsysteem voor informatiebeveiliging op basis van NEN-EN-ISO/IEC 27001. Daarmee vallen de twee onderdelen samen: risicomanagement en maatregelen die specifiek passen bij de context.

11.1. Cyberbeveiligingswet (Cbw)

Voor overheden is in de Cbw vastgelegd op welke wijze de zorgplicht voor de beveiliging van netwerk- en informatiesystemen wordt ingevuld. Hieronder volgt een samenvatting van de belangrijkste punten die betrekking hebben op het toepassen van de BIO:

- **Verplichting BIO**: het toepassen van de BIO voor de beveiliging van netwerk- en informatiesystemen is via de Cbw verplicht voor alle entiteiten die vallen onder de sector ‘Overheid’.
  Voor overheidsentiteiten die niet onder de Cbw vallen, is de BIO verplichtende zelfregulering per besluit in van het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). Ook waar beheers- en overheidsmaatregelen zijn uitgezonderd van de Cbw-verplichting of waar informatiebeveiliging over iets anders gaat dan de beveiliging van netwerk- en informatiesystemen, bijvoorbeeld de beveiliging van informatie op papier, geldt de BIO als verplichtende zelfregulering voor alle overheidsentiteiten.
- **Verantwoordelijkheid bestuurder**: De bestuurder is verantwoordelijk voor:
  - het treffen van passende en evenredige technische, operationele en organisatorische maatregelen om de risico’s te beheren en afgestemd op de voor de entiteit relevante risico’s en deze beheersen;
  - het goedkeuren van te nemen maatregelen voor het beheer van cyberbeveiligingsrisico’s;

    - het toezien op de kwaliteit van de uitvoering en het beheer van de maatregelen.
- **Opleiding**: bestuurders zijn opgeleid en hebben kennis om te kunnen sturen op informatiebeveiligingsrisico's. Ze zorgen ervoor dat hun werknemers regelmatig opleiding/training volgen over het onderwerp. Dit betekent dat de opleiding voldoet aan de eisen uit de Cbw.
- **Meldplicht**: de entiteit is verantwoordelijk voor het tijdig melden van significante incidenten. Overheden maken binnen de doorlooptijden een melding van een meldplichtig incident.
- **Toezicht en verantwoording**: de toezichthouder zal toezicht houden op de invulling van de zorgplicht volgens de Cbw. De RDI is als toezichthouder aangewezen voor de sector 'Overheid'.

12. Governance

De bestuurder van een entiteit is verantwoordelijk voor het beheersen van informatiebeveiligingsrisico's. De bestuurder kan dat niet alleen. Om informatiebeveiliging gedegen in te regelen, is een structuur nodig. Het is aan de entiteit om deze structuur aan te brengen volgens NEN-EN-ISO/IEC 27001.

Voor overheden zijn er een aantal rollen die standaard deel uitmaken van informatiebeveiliging van een entiteit. Deze rollen komen ook terug in de uitwerking van overheidsmaatregelen.

12.1. Bestuurder

De aangewezen bestuurders zijn verantwoordelijk voor het treffen van passende en evenredige technische, operationele en organisatorische maatregelen en ziet toe op de naleving daarvan. Kortgezegd zij zijn verantwoordelijk voor risicomanagement, dat gericht is op het borgen van digitale weerbaarheid van de entiteit.

Voor de sector 'Overheid' is in artikel 24 twaalfde lid van de Cbw gedefinieerd welke bestuurders worden bedoeld.

De bestuurder laat zich daarbij adviseren door een Chief Information Security Officer (CISO), Chief Information Officer (CIO), functionaris gegevensbescherming (FG) en dergelijke.

12.2. Lijnmanagement

Het lijnmanagement:

- is de eigenaar van informatie(systemen) en is daarmee verantwoordelijk voor het identificeren van dreigingen en risico's van deze informatie(systemen);
- is verantwoordelijk voor het toepassen van de verplichte beheersmaatregelen en overheidsmaatregelen uit de BIO voor het informatiesysteem;
- vraagt de CISO om advies, in alle gevallen waar het afwijkt van overheidsmaatregelen, ook waar dat expliciet als bevoegdheid genoemd is.

12.3. CISO

De CISO:

- is verantwoordelijk voor de coördinatie van informatiebeveiliging;
- ondersteunt de bestuurder en geeft gevraagd en ongevraagd advies aan de bestuurder;
- vertaalt wetgeving en bedrijfsdoelstellingen naar een informatiebeveiligingsbeleid;
- rapporteert aan het bestuur hoe het lijnmanagement het informatiebeveiligingsbeleid implementeert en op welke wijze wordt voldaan aan

de BIO, om ervoor zorg te dragen dat de bestuurder geïnformeerde besluiten kan maken over de behandeling van informatiebeveiligingsrisico's;
- is uitdrukkelijk niet verantwoordelijk voor informatiebeveiliging door het lijnmanagement.

12.4. Interne toezichthouder

Een bestuurder ziet toe op de toepassing van informatiebeveiliging binnen de entiteit. Een interne toezichthouder kan helpen bij dit toezicht.

13. Leveranciers

Leveranciers bieden diensten en/of producten aan entiteiten. Een entiteit blijft zelf verantwoordelijk voor het behandelen van risico's die betrekking hebben op de uitbestede of ingekochte dienst of product.

Afhankelijk van het risico behoren daarom verplichtingen van de overheid die volgen uit de BIO of uit andere richtlijnen te worden meegenomen bij het samenstellen van inkoopeisen aan leveranciers.

14. Informatiebeveiligingsprincipes

Overheidsmaatregelen worden risicogericht toegepast en geoperationaliseerd. Daarbij is het praktisch om informatiebeveiligingsprincipes te definiëren en toe te passen zoals security by design & default, toegang op basis van need to know, assume breach, zero trust, dingen gaan fout, defense in depth et cetera.

15. Operationaliseren maatregelen/balans in de maatregelenset

De BIO bevat maatregelen op tactisch niveau, die geoperationaliseerd worden. Hierbij is het belangrijk om in de maatregelenset balans te houden tussen:

- Beschikbaarheids-, integriteits- en vertrouwelijkheidsmaatregelen
- Organisatorische/proces-, menselijke/gedrags- en applicatieve/technische maatregelen
- Identificeren, beschermen, detecteren, reageren en herstellen

16. Treffen aanvullende maatregelen

Overheden kennen verschillende soorten informatie. Het is aan de entiteit zelf om te bepalen welk typen informatie zij verwerkt en welke aanvullende beveiligingsmaatregelen getroffen moeten worden. Bij deze afweging worden in ieder geval - en niet uitsluitend - de volgende typen gegevens afgewogen:

- Open data
- (Bijzondere) persoonsgegevens
- Gevoelige of interne informatie
- Gerubriceerde informatie

17. Impact van risico's

De impact van een informatiebeveiligingsincident hangt sterk af van de context. Entiteiten ondervinden vaak specifieke gevolgen door hun rol in de samenleving en democratie, hun bestuursstijl en hun verhouding tot de burgers. Bij het bepalen van de impact worden minimaal onderstaande impactsgebieden afgewogen:

- Politieke schade aan een bestuurder
- Diplomatieke schade

- Financiële gevolgen
- Directe imagoschade
- Verlies van publiek respect of vertrouwen
- Organisatiebrede negatieve publiciteit
- Significant verlies van motivatie van medewerkers
- Belangrijk verlies van management control

De impactgebieden kunnen ook bijdragen aan begrip bij de uitwisseling van impact met ketenpartners.

18. Relatie BIO en andere onderwerpen

De BIO richt zich op informatiebeveiliging. Onderwerpen zoals privacybescherming, informatievoorziening, beheersprocessen, bedrijfscontinuïteit zijn aanpalend aan informatiebeveiliging. Voor deze onderwerpen zijn vaak aparte standaarden opgezet. Deze onderwerpen worden daarom niet uitgewerkt in de BIO. Daar waar nuttig wordt verwezen naar deze separate standaarden.

DEEL 2 BIO–OVERHEIDSMAATREGELEN

Deel 2 van de BIO bevat alle overheidsmaatregelen. Deze maatregelen zijn gekoppeld aan de beheersmaatregelen uit NEN-EN-ISO/IEC 27002:2022. De eerste drie cijfers uit elke overheidsmaatregelnummer verwijst naar de bijbehorende beheersmaatregel uit deze norm. De navolgende nummers zijn het unieke volgnummer van de overheidsmaatregel.

Grijs gemarkeerde overheidsmaatregelen met bijbehorende beheersmaatregelen vallen niet onder de reikwijdte van de Cbw. Hiervoor geldt verplichtende zelfregulering.

Er bestaan beheersmaatregelen zonder overheidsmaatregelen.

Als een dergelijke beheersmaatregel van toepassing is, wordt gebruik gemaakt van de bijbehorende implementatierichtlijn uit NEN-EN-ISO/IEC 27002. Afwijken of niet toepassen van de bovenliggende beheersmaatregel wordt onderbouwd met een risicoanalyse. De referentie naar deze analyse is in een bijlage uitzonderingen opgenomen in de Verklaring van Toepasselijkheid (VvT).

Een beheersmaatregel kan een of meerdere overheidsmaatregelen hebben.

Deze overheidsmaatregelen vormen de verplichte minimale invulling van de beheersmaatregel. Uit een risicoanalyse blijkt of deze voldoende zijn om het risico te beheersen en tot een acceptabel niveau verlagen.

Overheidsmaatregel-nummer	**Overheidsmaatregel**
5.01.01	De entiteit heeft een informatiebeveiligingsbeleid opgesteld en vastgesteld door het bestuur van de entiteit. Dit beleid bevat ten minste de volgende punten: • De strategische uitgangspunten en randvoorwaarden die de entiteit hanteert voor informatiebeveiliging en in het bijzonder de inbedding in en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid. • De organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden. • De toewijzing van de verantwoordelijkheden en samenhang van informatiebeveiliging voor ketens van informatiesystemen, de beveiliging van OT, privacybescherming en de verantwoordelijkheden voor de continuïteit van de taakuitvoering van entiteit (BCM) aan lijnmanagers. • De gemeenschappelijke betrouwbaarheidseisen en normen die op de entiteit van toepassing zijn. • De frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd. • De bevordering van het beveiligingsbewustzijn.
5.01.02	Het informatiebeveiligingsbeleid wordt minimaal jaarlijks en in aansluiting bij de bestuurs- en Planning & Control (P&C)-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.

Overheidsmaatregel-nummer	Overheidsmaatregel
5.02.01	Het bestuur van de entiteit heeft vastgelegd en vastgesteld: • wat de verantwoordelijkheden en rollen zijn voor informatiebeveiliging, privacybescherming, operationele technologie (OT), bedrijfscontinuïteitsmanagement (BCM) binnen haar entiteit; • de samenhang voor informatiebeveiliging, de beveiliging van OT, de continuïteit van de taakuitvoering en BCM van de entiteit. Bij het definiëren en toewijzen van rollen en verantwoordelijkheden is specifieke aandacht voor het adequaat afhandelen van incidenten. Lijnmanagers en proceseigenaren die verantwoordelijk zijn voor bedrijfsmiddelen zijn ook verantwoordelijk voor de behandeling van risico's die op die bedrijfsmiddelen van toepassing zijn.
5.02.02	Er is een CISO aangesteld die bevoegd is om onafhankelijk en zelfstandig te adviseren en te rapporteren aan het bestuur en of het controlerend orgaan over informatiebeveiliging.
5.03.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.04.01	Het bestuur en de werknemers volgen regelmatig scholing, om cyberbeveiligingsrisico's te herkennen en te voorkomen en te weten wat men moet doen als er een informatiebeveiligingsincident is. Daarbij tonen bestuurders aan dat zij voldoende kennis en vaardigheden hebben om de gevolgen van informatiebeveiligingsrisico's te beoordelen op de diensten en/of producten die de entiteit levert.
5.04.02	Verplaatst naar 5.10.02.
5.04.03	Verplaatst naar 5.10.03.
5.05.01	De entiteit heeft uitgewerkt welke functionarissen met welke (overheids)instanties en toezichthouders formele contacten hebben over informatiebeveiliging. Dit overzicht wordt ten minste jaarlijks geactualiseerd.
5.06.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.07.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.08.01	Bij nieuwe informatiesystemen en bij significante wijzigingen op bestaande informatiesystemen wordt een expliciete risicoafweging op basis van een vastgestelde risicomanagementmethodiek uitgevoerd, om risico's te identificeren en in voldoende mate te beheersen en ook voor het vaststellen van de beveiligingseisen.

Overheidsmaatregel-nummer	Overheidsmaatregel
5.09.01	Er is een inventaris van bedrijfsmiddelen die van belang zijn voor informatieverwerking, met inbegrip van OT. De inventaris omvat alle eigenschappen die nodig zijn voor het beheer en onderhoud. In de inventaris zijn ook opgenomen: bedrijfsmiddelen op afstand, cloud-omgevingen en bedrijfsmiddelen die regelmatig zijn verbonden met de netwerkinfrastructuur maar niet onder controle van de entiteit staan. De volledigheid en actualiteit van de inventaris wordt periodiek gecontroleerd met tussenpozen die passend zijn voor de frequentie waarmee wijzigingen optreden.
5.10.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.10.02	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel en vrijwilligers in het contract vastgelegd volgens de huisregels of interne gedragsregels.
5.10.03	Alle medewerkers zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.
5.11.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.12.01	Informatie in alle informatiesystemen wordt met een expliciete risicoafweging geclassificeerd. Hierbij wordt gebruik gemaakt van een vastgestelde impactclassificatiemethodiek die onderdeel is van de vastgestelde risicomanagementmethodiek.
5.13.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.14.01	Internetfacing-informatiesystemen en e-mail-berichtenverkeer blijven voldoen aan de verplichte beveiligingsstandaarden, zie hiervoor de website van het Forum Standaardisatie en het Cyberbeveiligingsbesluit. Hierop wordt gestuurd met de metingen van internet.nl. Daarbij dienen alle onderdelen te worden ingesteld zodat een optimale beveiliging wordt bereikt zonder afbreuk te doen aan de functionaliteit van de geboden dienst.
5.14.02	De entiteit maakt bij openbaar webverkeer van gevoelige gegevens gebruik van ten minste publiek vertrouwde Organization Validated (OV)-certificaten. De entiteit maakt bij intern webverkeer voor gevoelige gegevens gebruik van ten minste publieke vertrouwde OV-certificaten of private PKIo-certificaten. Hogere eisen aan certificaten vloeien voort uit een risicoanalyse, aansluitvoorwaarden of wetgeving.

Overheidsmaatregel-nummer	Overheidsmaatregel
5.14.03	Geavanceerde en/of gekwalificeerde elektronische handtekeningen voldoen aan de Advanced Electronic Signatures (AdES Baseline Profiles), zoals opgenomen in de Lijst open standaarden van Forum Standaardisatie.
5.14.04	Van alle internetfacing-informatiesystemen, webapplicaties, IP-adressen en API's is er een actuele registratie.
5.14.05	Publiek toegankelijke websites worden bekend gemaakt via het Register Internetdomeinen Overheid (RIO). Deze informatie wordt ten minste iedere zes maanden geactualiseerd.
5.15.01	Toegang tot een vertrouwde zone is toegestaan in twee situaties: 1. vanaf geauthentiseerde apparatuur of; 2. vanuit programmatuur die draait binnen een veilige schil.
5.16.01	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.
5.16.02	Het gebruiken van groepsaccounts is niet toegestaan, tenzij de proceseigenaar dit motiveert, vastlegt en afstemt met de CISO.

Overheidsmaatregel-nummer	Overheidsmaatregel
5.17.01	De entiteit past multi-factorauthenticatie (MFA) ten minste toe voor het primaire aanloggen op de digitale werkomgeving, bij accounts voor via het internet bereikbare voorzieningen en accounts die beheerrechten hebben en in andere situaties waar uit de risicoanalyse blijkt dat dit een passende oplossing is. De entiteit past MFA toe in deze twee vormen: 1. Wachtwoordloze toegang, zoals een pincode in combinatie met een hardware token of persoonlijk uniek certificaat (passkey). 2. Wachtwoordtoegang in combinatie met minimaal een tweede factor. Indien MFA niet mogelijk is voor deze accounts, worden andere mitigerende maatregelen genomen. Bij het nemen van mitigerende maatregelen wordt de CISO betrokken. De proceseigenaar keurt de mitigerende maatregelen goed. Waar mogelijk en veilig wordt MFA met federatieve authenticatievoorzieningen zoals Single Sign On en een Stepping Stone-oplossing worden gecombineerd toegepast. Voor beheer en monitoring van authenticatiegegevens: • wordt authenticatie-informatie uitgegeven met formele vastgestelde procedures, nadat de identiteit van de gebruiker met voldoende zekerheid is vastgesteld; • worden Use Cases voor misbruik van authenticatiegegevens gedefinieerd, worden deze gemonitord en wordt passende actie ondernomen bij het optreden ervan. Deze Use Cases omvatten in ieder geval inlogpogingen van ongebruikelijke plekken en pieken in mislukte inlogpogingen.
5.17.02	De entiteit biedt aan alle medewerkers een wachtwoordmanager of vergelijkbare oplossing aan.
5.17.03	De eisen aan wachtwoorden worden geautomatiseerd afgedwongen.
5.18.01	Het maken en aanpassen van accounts met bijzondere rechten wordt gemonitord. Indien deze wijzigingen ongeautoriseerd zijn, is dit een informatiebeveiligingsincident en wordt dat als zodanig vastgelegd en afgehandeld.
5.18.02	Alle uitgegeven toegangsrechten worden minimaal eenmaal per jaar beoordeeld. Een risicoafweging bepaalt of dit sneller moet.

Overheidsmaatregel-nummer	Overheidsmaatregel
5.19.01	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, zijn informatiebeveiligingseisen waaronder de beschikbaarheid, integriteit en vertrouwelijkheid, onderdeel van het hele pakket aan inkoopeisen. De informatiebeveiligingseisen zijn gebaseerd op een expliciete risicoafweging.
5.20.01	De beveiligingseisen uit de offerteaanvraag worden expliciet opgenomen in (inkoop)contracten waar de verwerking van informatie een rol speelt.
5.20.02	Waar mogelijk worden algemene voorwaarden van leveranciers expliciet uitgesloten en worden eventueel aanvullende voorwaarden opgenomen. Als uitsluiten niet mogelijk is, worden risico's beoordeeld. Expliciet is gemaakt welke consequenties geaccepteerd worden, welke gemitigeerd zijn en welke voorwaarden niet of nooit geaccepteerd worden bij het aangaan van de overeenkomst.
5.20.03	In het inkoopcontract wordt opgenomen dat de leverancier aantoont dat hij aan alle gestelde eisen voldoet in opzet, bestaan en werking, op basis van onderzoeken van onafhankelijke derden. Deze onderzoeken hebben een scope die dekkend is voor de gecontracteerde dienstverlening. Hierbij is expliciet aandacht voor de toeleveringsketen en hoe de leverancier zijn leveranciersmanagement ingeregeld heeft, zie overheidsmaatregel 5.21.01. Dit toont de leverancier jaarlijks opnieuw aan.
5.20.04	De entiteit voert zelfstandig onderzoek uit, ook ter validatie van de rapportages die de leverancier aanlevert. Om dit mogelijk te maken, wordt expliciet opgenomen dat er een mogelijkheid is voor een externe audit. Indien uit het voorgaande restrisico's volgen, beheerst de entiteit deze door het toepassen van zijn vastgestelde risicomanagementmethodiek.
5.20.05	Onderdeel van de afspraken is dat de leverancier transparant is over kwetsbaarheden in de dienstverlening en informatiebeveiligingsincidenten waaronder datalekken. Dit stelt de entiteit in staat om passend te reageren onder meer door te rapporteren en mitigerende maatregelen te nemen.
5.20.06	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.
5.21.01	Vervallen.

Overheidsmaatregel-nummer	Overheidsmaatregel
5.21.02	Voorafgaand aan het afsluiten van de overeenkomst geeft de leverancier inzicht in de keten van toeleveranciers en eventuele risico's daarin. De entiteit beoordeelt of de risico's acceptabel zijn.
5.21.03	De entiteit borgt dat de beveiligingseisen aan de leverancier onverminderd van toepassing zijn op de keten van toeleveranciers, tenzij die eisen niet relevant zijn gezien de aard van de dienstverlening door de toeleverancier. Indien informatiebeveiligingseisen zijn uitgesloten, maakt de leverancier dat inzichtelijk, inclusief een onderbouwing.
5.21.04	Gedurende de looptijd geeft de leverancier veranderingen in de keten van toeleveranciers door, inclusief risico's daarin. Dit omvat minimaal kwetsbaarheden en informatiebeveiligingsincidenten die de dienstverlening aan de entiteit kunnen raken.
5.21.05	De beveiliging van toeleveringsketens is onderdeel van de risicoanalyse voor de entiteit. In de risicoanalyse wordt rekening gehouden met: • specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener; • de algemene kwaliteit van de producten; • de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures.
5.22.01	Op basis van het door de leverancier aangeleverde bewijsmateriaal, zie overheidsmaatregel 5.20.03, is de proceseigenaar verantwoordelijk voor: • het jaarlijks beoordelen dat de leverancier voldoet aan de gestelde informatiebeveiligingseisen; • het vaststellen van eventuele beveiligingsrisico's; • het (laten) nemen van mitigerende maatregelen en het accepteren van rest-risico's.
5.22.02	De entiteit heeft een actuele registratie van leveranciers en afgesloten contracten.
5.23.01	De entiteit stelt beleid op dat toeziet op het inventariseren, classificeren, selecteren, beoordelen en managen van Cloud Service Providers (CSP) en het beëindigen van dienstverlening door CSP's en past dat toe. Dit beleid wordt minimaal eens per drie jaar herzien. In de inkoopcontracten wordt opgenomen welke situaties aanleiding kunnen geven tot ontbinding van het contract. Wanneer zich belangrijke wijzigingen bij de leverancier optreden, beoordeel de risico's daarvan en neem passende maatregelen.
5.24.01	Er is voor alle interne en externe medewerkers een toegankelijk meldloket waar informatiebeveiligingsincidenten kunnen worden gemeld en geregistreerd.

Overheidsmaatregel-nummer	Overheidsmaatregel
5.24.02	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
5.24.03	De proceseigenaar is verantwoordelijk voor het oplossen van informatiebeveiligingsincidenten.
5.24.04	De proceseigenaar rapporteert maandelijks de opvolging van informatiebeveiligingsincidenten aan de eindverantwoordelijke voor de bedrijfsvoering.
5.24.05	In de procedure voor informatiebeveiligingsincidenten is er een verwijzing gemaakt naar de procedure voor crisisbeheersing.
5.24.06	Verplaatst naar 5.21.05.
5.24.07	De incidentprocedure bevat tenminste: • dat binnen de wettelijke termijn informatiebeveiligingsincidenten worden gemeld bij het Cyber Security Incident Response Team (CSIRT); • dat meldingen van het CSIRT worden ontvangen, beoordeeld en opgenomen in de risicobehandeling; • dat betrokkenen binnen de wettelijke termijn op de hoogte gesteld worden van het incident.
5.24.08	Een Coordinated Vulnerability Disclosure (CVD)-procedure is ingericht en gepubliceerd volgens de NCSC-leidraad of NEN-EN-ISO/IEC 29147:2020 Vulnerability disclosure. Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD)-meldingen is onderdeel van de incidentrapportage.
5.25.01	Verplaatst naar 5.26.02.
5.25.02	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.26.01	Verplaatst naar 5.25.02.
5.26.02	Informatiebeveiligingsincidenten worden afgedaan via het incidentbeheerproces. In het incidentbeheerproces is opgenomen dat incidenten indien relevant gemeld worden bij de in wet- en regelgeving aangewezen toezichthouders.
5.27.01	Informatiebeveiligingsincidenten worden geanalyseerd om achterliggende oorzaken vast te stellen, verbeteringen te realiseren, om zo toekomstige incidenten te voorkomen.
5.27.02	De analyses van informatiebeveiligingsincidenten, inclusief de achterliggende oorzaken en de verbeteringen worden breed gedeeld met relevante partners om herhaling en toekomstige incidenten te voorkomen.

Overheidsmaatregel-nummer	Overheidsmaatregel
5.28.01	De bewaartermijn van een (vermoedelijk) informatiebeveiligingsincident en alle informatie om het incident te analyseren en op te lossen, is minimaal drie jaar. Dit betreft onder meer de informatie benodigd voor de analyse waaronder logging, de oplossing en het advies.
5.29.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.30.01	De proceseigenaar test jaarlijks continuïteitsplannen op werking, volledigheid en actualiteit, om de plannen te verbeteren.
5.30.02	Binnen de inventarisatie van beheersmaatregel 5.12 uit NEN-EN-ISO/IEC 27002:2022, identificeert de proceseigenaar kritieke systemen op basis van de vastgestelde risicomanagementmethodiek en een expliciete risicoafweging. De proceseigenaar actualiseert dit overzicht ten minste eens per drie jaar.
5.31.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.32.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.33.01	De proceseigenaar heeft voor alle informatie(systemen) in selectielijsten de bewaartermijn vastgelegd, rekening houdend met de eigen bedrijfsdoelstellingen en wet- en regeling, zoals de archiefwet en privacywetgeving. De proceseigenaar heeft deze termijnen ook praktisch ingeregeld en toetst periodiek de werking hiervan.
5.34.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
5.35.01	Vervallen.
5.35.02	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.
5.36.01	In de P&C-cyclus en als onderdeel van de plan-do-check-act (PDCA)-cyclus wordt gerapporteerd over informatiebeveiliging onder coördinatie van de CISO. Dit resulteert in een jaarlijks af te geven In Control Verklaring (ICV), of een vergelijkbaar instrument, over de gehele informatiebeveiliging van de entiteit. De ICV of het vergelijkbare instrument kan ook onderdeel zijn van de formele verantwoording.
5.37.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
6.01.01	Elke entiteit heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan op basis van een risicoafweging een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.

Overheidsmaatregel-nummer	Overheidsmaatregel
6.02.01	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden voor informatiebeveiliging. De voor hen geldende regelingen en instructies voor informatiebeveiliging zijn eenvoudig toegankelijk.
6.03.01	Alle medewerkers, lijnmanagers en bestuurders hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels van en verplichtingen voor informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.
6.03.02	Alle medewerkers en contractanten die gebruikmaken van informatiesystemen en -diensten hebben binnen drie maanden na indiensttreding aantoonbaar een training I-bewustzijn succesvol gevolgd.
6.03.03	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 voor informatiebeveiliging. Het management stimuleert hen actief deze periodiek te volgen.
6.03.04	In bewustwordingsprogramma's komen gedragsaspecten van veilig mobiel werken aan de orde.
6.04.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
6.05.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
6.06.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
6.07.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
6.08.01	Alle medewerkers (intern en extern) hebben aantoonbaar kennisgenomen van de meldingsprocedure van informatiebeveiligingsincidenten.
7.01.01	Vervallen.
7.01.02	Kritieke informatie of informatiesystemen zijn nooit via één beveiligde zone te bereiken.
7.02.01	In geval van concrete beveiligingsrisico's worden waarschuwingen, volgens onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.
7.03.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
7.04.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.

Overheidsmaatregel-nummer	Overheidsmaatregel
7.05.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
7.06.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
7.07.01	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingsvergrendeling automatisch geactiveerd.
7.08.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
7.09.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
7.10.01	In de verwijderinstructie is opgenomen dat van verwijderbare media, die herbruikbaar zijn en de entiteit verlaten, de bedrijfsgevoelige inhoud onherstelbaar verwijderd is.
7.10.02	Er wordt gecontroleerd of alle data op het medium onherstelbaar verwijderd is. Hiervan wordt verslag gemaakt. Er wordt waar mogelijk gebruik gemaakt van producten waarvoor de Unit Weerbaarheid van het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) een positief inzetadvies afgegeven heeft.
7.10.03	Het gebruik van koeriers of transporteurs voor transport van geclassificeerde informatie voldoet aan vooraf opgestelde betrouwbaarheidseisen.
7.11.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
7.12.01	Geen overheidsmaatregel, zie inleiding deel 2BIO-overheidsmaatregelen.
7.13.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
7.14.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.01.01	Mobiele apparatuur is zo ingericht dat bedrijfsinformatie niet standaard op het gebruikersdevice wordt opgeslagen (‘zero footprint’). Als (near) zero footprint (nog) niet realiseerbaar is, biedt een mobiel apparaat de mogelijkheid om de toegang te beschermen met een toegangsbeveiligingsmechanisme met minimaal versleuteling van de gegevens. Op mobiele apparatuur is ‘wissen op afstand’ mogelijk.

Overheidsmaatregel-nummer	Overheidsmaatregel
8.01.02	Bij de inzet van mobiele apparatuur zijn minimaal de volgende aspecten geïmplementeerd: • Het apparaat maakt deel uit van patchmanagement en hardening. • Er wordt gebruik gemaakt van Mobile Device Management (MDM)- of Mobile Application Management (MAM)-oplossingen. • Gebruikers tekenen een gebruikersovereenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen. Deze verklaring heeft betrekking op alle mobiele apparatuur die de medewerker zakelijk gebruikt. Periodiek wordt getoetst of deze drie aspecten worden nageleefd.
8.02.01	De toegewezen of gebruikte speciale bevoegdheden worden in opzet, bestaan en werking minimaal ieder kwartaal beoordeeld.
8.03.01	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.
8.03.02	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.
8.04.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.05.01	Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden en voor hoelang de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.
8.06.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.07.01	Het downloaden van bestanden is beheerst en beperkt op basis van het risico en need-of-use. De antimalware-software beoordeelt altijd alle downloads.
8.07.02	Gebruikers zijn voorgelicht over de risico's van surfgedrag en het klikken op onbekende links.
8.07.03	De gebruikte antimalware-software en bijbehorende herstelsoftware zijn actueel en wordt ondersteund door periodieke updates.

Overheidsmaatregel-nummer	Overheidsmaatregel
8.07.04	De malwarescan wordt uitgevoerd op: • alle omgevingen, bijvoorbeeld op (mail)servers, (desktop)computers en bij de toegangsverlening tot het netwerk van de entiteit; • alle gedownloade content voorafgaand aan executie of opslag; • alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik of opslag in de eigen omgeving.
8.08.01	Als van een kwetsbaarheidswaarschuwing de kans op misbruik en de verwachte schade beide hoog zijn, worden passende mitigerende maatregelen zo snel mogelijk, maar uiterlijk binnen een week getroffen.
8.08.02	Op basis van een expliciete risicoafweging wordt bepaald op welke wijze mitigerende maatregelen getroffen worden.
8.08.03	In de tussentijd of als installatie binnen een week niet mogelijk is, worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.
8.08.04	Informatiesystemen worden waar mogelijk jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses, penetratietesten of red-teamingstesten. Internetfacing-informatiesystemen worden waar mogelijk continue getest op zwakheden en kwetsbaarheden.
8.08.05	Internetfacing-informatiesystemen hebben een verplichte waar mogelijk geautomatiseerde penetratietest bij iedere nieuwe release of major update. Als daar bevindingen met een hoog risico uitkomen die niet op een andere manier gemitigeerd kunnen worden, mag het systeem niet in productie. Alle internetfacing-informatiesystemen worden minimaal jaarlijks getest op zwakheden en kwetsbaarheden.
8.08.06	Zie overheidsmaatregel 5.24.08.
8.09.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.10.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.11.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.12.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.

Overheidsmaatregel-nummer	Overheidsmaatregel
8.13.01	Er is een back-upbeleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld. Er is speciale aandacht voor het beschermen van de back-up tegen ransomware-aanvallen en genomen maatregelen om de integriteit van de back-up te behouden.
8.13.02	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een incident.
8.13.03	Het back-upproces voorziet in de opslag van de back-up op een locatie, waarbij een incident op de ene locatie niet kan leiden tot schade op de andere.
8.13.04	De herstelprocedure wordt minimaal jaarlijks getest of na een grote wijziging, om de goede werking te waarborgen als deze in noodgevallen uitgevoerd wordt.
8.14.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.15.01	Een logregel bevat minimaal: • Actie: de gebeurtenis of handeling die heeft plaatsgevonden. • Object: waarop de gebeurtenis of handeling effect had (bijvoorbeeld welk bestand, proces of systeem). • Resultaat: het resultaat van de gebeurtenis of handeling. • Oorsprong: het apparaat of de netwerklocatie van waaruit de gebeurtenis of handeling in gang is gezet. • Actor: identificatie van de persoon die of het proces dat de gebeurtenis in gang heeft gezet. • Tijdstempel: datum en tijdstip waarop de gebeurtenis of handeling plaatsvond.
8.15.02	Een logregel bevat nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden.
8.15.03	Er is een overzicht van logbestanden die worden gegenereerd.
8.15.04	De bewaartermijn van logbestanden en gegevens in het Security Incident en Event Monitoring (SIEM) worden risicogericht bepaald, rekening houdend met het scenario dat aanvallers langdurig binnen zijn.
8.15.05	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als informatiebeveiligingsincident via de procedure voor informatiebeveiligingsincidenten volgens beheersmaatregel 5.24 uit NEN-EN-ISO/IEC 27002:2022.
8.15.06	Op basis van een expliciete risicoafweging bepaalt de entiteit de periodieke toetsing op het ongewijzigd bestaan van logbestanden gedurende de bewaartermijn. Toetsing wordt uitgevoerd door een ten opzichte van de uitvoering onafhankelijke functionaris.

Overheidsmaatregel-nummer	Overheidsmaatregel
8.16.01	Bij ontdekte nieuwe dreigingen (aanvallen) via overheidsmaatregel 8.16.3 worden deze binnen geldende juridische kaders verplicht gedeeld met de daarvoor aangewezen Computer Emergency Response Team (CERT).
8.16.02	Het SIEM- en/of het SOC-monitoringsproces hebben eenduidige regels over wanneer een incident wordt gerapporteerd aan het verantwoordelijke management.
8.16.03	De informatieverwerkende omgeving wordt gemonitord met een detectie- en response-oplossing, waarmee aanvallen kunnen worden gedetecteerd en afwijkingen adequaat en tijdig worden behandeld.
8.16.04	Actieve netwerkcomponenten zijn voorzien van logging en monitoring van die logging om afwijkende gebeurtenissen te kunnen waarnemen en daarop te reageren.
8.17.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.18.01	Alleen bevoegd personeel heeft op die momenten dat toegang strikt noodzakelijk is toegang tot systeemhulpmiddelen.
8.18.02	Het gebruik van systeemhulpmiddelen wordt gelogd. De logging is een halfjaar beschikbaar voor onderzoek.
8.19.01	Het risico van installatie door gebruikers van niet geautoriseerde software wordt beheerst.
8.20.01	Netwerkcomponenten voldoen minimaal aan het vertrouwelijkheidsniveau van het netwerk waarvan ze onderdeel zijn.
8.20.02	Toegang tot beheerinterfaces van netwerkcomponenten zijn zo veel als mogelijk gescheiden van het gebruikersnetwerk.
8.21.01	In koppelpunten met externe of onvertrouwde zones en vanwege netwerksegmentatie zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden te signaleren en te mitigeren.
8.21.02	Het dataverkeer van of naar de vertrouwde omgeving, wordt bewaakt en geanalyseerd op verdacht verkeer met detectievoorzieningen.
8.21.03	Bij ontdekte nieuwe dreigingen vanuit overheidsmaatregel 8.21.02 worden deze doorgeleid, rekening houdend met de geldende juridische kaders gedeeld binnen de overheid.

Overheidsmaatregel-nummer	Overheidsmaatregel
8.21.04	Bij transport van gegevens over draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied worden gegevens versleuteld met uitzondering van metagegevens die noodzakelijk zijn om het transport tot stand te laten komen. De inrichting van de versleuteling is risicogericht en houdt rekening met de noodzakelijke beschermingstermijn en het noodzakelijke beschermingsniveau. Hierbij wordt waar mogelijk gebruik gemaakt van encryptiemiddelen waarvoor de Unit Weerbaarheid van het NBV van de AIVD een positief inzetadvies heeft afgegeven. Als de Unit Weerbaarheid geen encryptiemiddelen heeft geadviseerd, wordt in overleg met de CISO een andere geschikte versleutelingsmethodiek gekozen en ingericht.
8.22.01	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.
8.23.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.24.01	In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: • Wanneer cryptografie ingezet wordt. • Wie verantwoordelijk is voor de implementatie. • Wie verantwoordelijk is voor het sleutelbeheer. • Hoe geregistreerd wordt waar welke cryptografie toegepast wordt. • Welke normen als basis dienen voor cryptografie en de wijze waarop de passende normen van het Forum Standaardisatie worden toegepast. • De wijze waarop het beschermingsniveau vastgesteld wordt. • Bij communicatie tussen entiteiten wordt het beleid onderling vastgesteld.
8.24.02	Cryptografische beheersmaatregelen zijn opgenomen in de inventaris van de bedrijfsmiddelen. Voor alle cryptografische beheersmaatregelen is vastgesteld waar ze worden ingezet, wie ervoor verantwoordelijk is en hoe ze actueel worden gehouden.
8.24.03	Vervallen.
8.24.04	De sterkte van de cryptografie wordt gebaseerd op de actuele adviezen van het NCSC en de Unit Weerbaarheid van het NBV van de AIVD.
8.24.05	Er zijn afspraken over reservecertificaten van een alternatieve leverancier als uit de risicoafweging blijkt dat deze noodzakelijk zijn als onderdeel van gereedheid voor bedrijfscontinuïteit (zie beheersmaatregel 5.30 uit NEN-EN-ISO/IEC 27002:2022).

Overheidsmaatregel-nummer	Overheidsmaatregel
8.25.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.26.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.27.01	Architectuurprincipes zoals 'security by design' en 'security by default' voor het ontwerpen van de beveiliging van informatiesystemen worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten over het ontwikkelen van informatiesystemen.
8.28.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.29.01	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden waar mogelijk geautomatiseerd uitgevoerd. Van de resultaten van de testen wordt verslag gemaakt.
8.30.01	Interne maatregelen voor systeemontwikkeling zijn onverkort van toepassing op uitbestede ontwikkeling, aangevuld met maatregelen die volgen vanuit uitbestedingen.
8.31.01	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.
8.31.02	Significante wijzigingen in de productieomgeving worden altijd getest voordat zij in productie gebracht worden. Alleen met voorafgaande goedkeuring door de proceseigenaar kan hiervan worden afgeweken.
8.32.01	In het wijzigingsbeheerproces is minimaal aandacht besteed aan: • het administreren van wijzigingen, met de resultaten van het testplan; • een risicoafweging van mogelijke gevolgen van de wijzigingen, inclusief een beschreven rollback-plan; • de goedkeuringsprocedure voor wijzigingen.
8.32.02	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerraamwerk.
8.33.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.
8.34.01	Geen overheidsmaatregel, zie inleiding deel 2 BIO-overheidsmaatregelen.