Bijlage 3 PVE

Excel Export ICO Wizard tbv Inkoopafdeling/opdrachtgever/budgethouder

Inkooponderdelen	Algemeen Ketenpartners, Clouddiensten, Communicatievoorzieningen
Proceseis	ja
Producteis	ja
Eis voor de opdrachtgever	nee
Eis voor de opdrachtnemer	ja
Ook eisen meegeven die alleen te maken hebben met schaalgrootte	nee
Waardering	MUST, NEED,
Basispakket	ja
Privacy-supplement	ja
Toon BIO-O maatregelen	ja
Toon ABRO-eisen TBB4	ja
Toon ABRO-eisen TBB3	nee
Toon ABRO-eisen TBB2	nee
Toon ABRO-eisen TBB1	nee
Aantal geselecteerde eisen	293

Nr	**Naam Eis**	**Referentie brondocument:**	**Referentie code norm:**	**BIO-O-maatregel:**	**Samenvatting eis:**
0	Voldoen aan BIO Hoofdstuk 1	n.v.t.	Ketenpartnereis 1		De organisatie van de Opdrachtnemer en zijn dienstverlening dienen in opzet, bestaan en werking te voldoen aan hoofdstuk 1 van de Baseline Informatiebeveiliging Overheid (BIO, versie 1.04, te downloaden op www.bio-overheid.nl) en toont dat jaarlijks aan middels onafhankelijke onderzoeken.
1	ABRO-maatregel. Voldoen aan ABRO	ABRO 2026	1.1.13		Opdrachtnemer heeft bij het inrichten van beveiligingsmaatregelen rekening gehouden met vigerende wetgeving om te zorgen dat het welzijn en de veiligheid van medewerkers niet in het geding komt. Indien vigerende wetgeving, zoals de Arbowet, maakt dat bepaalde beveiligingsmaatregelen niet volledig kunnen worden geïmplementeerd, heeft Opdrachtnemer in afstemming met NBIV passende mitigerende maatregelen genomen.
2	PDCA-cyclus	n.v.t.	Ketenpartnereis 2		Informatiebeveiliging en privacy zijn dynamische onderwerpen en de maatregelen dienen vanwege toenemende risico’s en bedreigingen via een PDCA-cyclus actueel te worden gehouden.
3	Recht op audit	n.v.t.	Ketenpartnereis 3		De Opdrachtgever heeft het recht om maximaal een maal per jaar een audit te laten uitvoeren. Deze audit wordt in overleg met de Opdrachtnemer ingepland.
4	Onderaannemers	n.v.t.	Ketenpartnereis 4	Ja	De eisen van het inkooponderdeel 'Algemeen Ketenpartners' zijn ook van toepassing op onderaannemers van de Opdrachtnemer.
6	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.1		Opdrachtnemer legt voorgenomen Uitbesteding van werkzaamheden in het kader van een Bijzondere Opdracht aan een Onderaannemer vooraf ter goedkeuring voor aan de Opdrachtgever en NBIV conform formulier 'Aanvraag Onderaannemer'.
7	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.2		Opdrachtnemer heeft in afstemming met Opdrachtgever en NBIV een opdrachtspecifiek overzicht van Te Beschermen Belangen voor elke bij de Bijzondere Opdracht betrokken Onderaannemer en eventuele achterliggende Onderaannemers opgesteld, zodanig dat voor Opdrachtgever en NBIV inzichtelijk is welke Onderaannemer toegang heeft tot welke Te Beschermen Belangen, zie ook bijlage 4.

8	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.3		Na goedkeuring van Opdrachtgever en NBIV tot Uitbesteding heeft Opdrachtnemer in het contract met Onderaannemer die op enigerwijze in aanraking komen met een Te Beschermen Belang de vigerende ABRO bedongen.
9	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.4		Na toestemming van NBIV op basis van een door een Buitenlandse partner verstrekte Facility Security Clearance, heeft Opdrachtnemer in het contract met de buitenlandse Onderaannemer(s) de in het betrokken land geldende beveiligingseisen bedongen. Een overzicht van Te Beschermen Belangen is hierbij verstrekt aan NBIV.
10	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.5		Opdrachtnemer bepaalt in afstemming met Opdrachtgever op basis van een Risicoanalyse of de door (Toe)leverancier(s) geleverde producten en/of diensten een risico vormen voor de Bijzondere Opdracht. Indien dit het geval is wordt de (Toe)leverancier als Onderaannemer aangemerkt en heeft Opdrachtnemer de vigerende ABRO contractueel bedongen.
11	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.6		Opdrachtnemer draagt de verantwoordelijkheid voor het voldoen aan de eisen uit ABRO 2026 door Onderaannemer(s).
12	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.7		Opdrachtnemer heeft een proces vastgesteld en geïmplementeerd om veranderingen in en naleving van gemaakte beveiligingsafspraken met Onderaannemer(s) doorlopend te beheren, controleren en te evalueren. In geval van geconstateerde tekortkomingen die invloed hebben op een Te Beschermen Belang informeert Opdrachtnemer NBIV conform de Incident Response Procedure.
13	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.8		Wanneer binnen een samenwerkingsverband met andere bedrijven wordt gewerkt aan de Bijzondere Opdracht zijn de werkzaamheden aan een Te Beschermen Belang zoveel mogelijk gecentraliseerd.
14	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.9		Opdrachtnemer verstrekt een overzicht aan NBIV van de gehele keten van Onderaannemer(s) en (Toe)leverancier(s) en de landen waarin zij gevestigd zijn voor alle bedrijfsactiviteiten die van toepassing zijn op de Bijzondere Opdracht(en) en werkzaamheden die raken aan een Te Beschermen Belang.
15	ABRO-maatregel. Onderaannemers	ABRO 2026	1.5.10		Wanneer een Te Beschermen Belang wordt ondergebracht bij een door Opdrachtnemer gekozen Escrow Agent, is de vigerende ABRO contractueel bedongen en beschikt de Escrow Agent over een ABRO-Verklaring voor de Bijzondere Opdracht voordat een Te Beschermen Belang wordt overgedragen.
16	ABRO-maatregel. Onderaannemers	ABRO 2026	4.2.1		Voorafgaand aan de overdracht of uitwisseling van Bijzondere Informatie is door de Beveiligingsfunctionaris vastgesteld dat de ontvangende partij de Bijzondere Informatie conform het vastgestelde beveiligingsniveau kan behandelen en geautoriseerd is om te beschikken over de Bijzondere Informatie.
17	Beheer van informatiebeveiligingsincidenten	BIO 2019	Ketenpartn ereis 5	Ja	Op de inrichting van het beheer van Informatiebeveiligingsincidenten is hoofstuk 16 van de BIO 2019 van toepassing.
18	O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen	BIO 2019	16.1.2.1	Ja	Er is een meldloket waar beveiligingsincidenten kunnen worden gemeld.
19	O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen	BIO 2019	16.1.2.2	Ja	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
20	O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen	BIO 2019	16.1.2.3	Ja	Alle medewerkers en contractanten hebben aantoonbaar kennis genomen van de meldingsprocedure van incidenten.
21	O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen	BIO 2019	16.1.2.4	Ja	Incidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.
22	O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen	BIO 2019	16.1.2.5	Ja	De proceseigenaar is verantwoordelijk voor het oplossen van beveiligingsincidenten.
23	O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen	BIO 2019	16.1.2.6	Ja	De opvolging van incidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.

24	O-maatregel. Rapportage van informatiebeveiligingsgebeurtenissen	BIO 2019	16.1.2.7	Ja	Informatie afkomstig uit de Coordinated Vulnerability Disclosure (CVD) procedure is onderdeel van de incidentrapportage.
25	O-maatregel. Rapportage van zwakke plekken in de informatiebeveiliging	BIO 2019	16.1.3.1	Ja	Een Coördinated Vulnerability Disclosure (CVD) procedure is gepubliceerd en ingericht.
30	Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	BIO 2019	Ketenpartn ereis 6	Ja	Op het bedrijfscontinuïteitsbeheer zijn de Informatiebeveiligingsaspecten van hoofstuk 17 van de BIO 2019 van toepassing.
34	Inrichting van verantwoordelijkheden bij informatiebeveiliging	BIO 2019	Ketenpartn ereis 7	Ja	Op de inrichting van verantwoordelijkheden bij informatiebeveiliging is paragraaf 6.1. van de BIO 2019 van toepassing
35	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.1	Ja	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
36	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.2	Ja	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
37	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.3	Ja	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.
38	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.4	Ja	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
39	O-maatregel. Scheiding van taken	BIO 2019	6.1.2.1	Ja	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.
42	Sturen op veilig personeel	BIO 2019	Ketenpartn ereis 8	Ja	Bij het sturen op veilig personeel is hoofdstuk 7 van de BIO 2019 van toepassing.
43	O-maatregel. Screening	BIO 2019	7.1.1.1	Ja	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.
44	O-maatregel. Arbeidsvoorwaarden	BIO 2019	7.1.2.1	Ja	Alle medewerkers (intern en extern) zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.
45	O-maatregel. Directieverantwoordelijkheden	BIO 2019	7.2.1.1	Ja	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen anoniem en veilig beveiligingsissues kan melden.
46	O-maatregel. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	BIO 2019	7.2.2.1	Ja	Alle medewerkers hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.
47	O-maatregel. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	BIO 2019	7.2.2.2	Ja	Alle medewerkers en contractanten die gebruikmaken van de informatiesystemen- en diensten hebben binnen drie maanden na indiensttreding een training I-bewustzijn succesvol gevolgd.
48	O-maatregel. Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	BIO 2019	7.2.2.3	Ja	Het management benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij haar medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.

49	O-maatregel. Speciale systeemhulpmiddelen gebruiken	BIO 2019	9.4.4.1	Ja	Alleen bevoegd personeel heeft toegang tot systeemhulpmiddelen.
63	Transport en verzenden	BIO 2019	Ketenpartn ereis 10	Ja	Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.
66	ABRO-maatregel. Bediening van ICT	ABRO 2026	1.1.10		Opdrachtnemer voert op verzoek van NBIV voor het verkrijgen van een ABRO-Verklaring een Zelfinspectie uit met behulp van de zelfinspectielijst om in te schatten in welke mate Opdrachtnemer voldoet aan de op grond van ABRO 2026 vereiste maatregelen en verstrekt deze aan NBIV.
67	ABRO-maatregel. Bediening van ICT	ABRO 2026	4.12.2		Procedures (inclusief rollen en verantwoordelijkheden) voor het beheer van de IT-voorzieningen waarin Bijzondere Informatie wordt verwerkt (o.a. ten aanzien van back-up en herstel, afhandelen van fouten en noodprocedures) zijn vastgesteld en beschikbaar gesteld aan Beheerders en worden minimaal jaarlijks geëvalueerd en waar nodig aangepast.
68	ABRO-maatregel. Beschermen bedrijfsinformatie	ABRO 2026	1.6.1		Opdrachtnemer maakt het bestaan van, of opgedane kennis tijdens, de Bijzondere Opdracht op geen enkele wijze bekend buiten de geautoriseerde personen of organisaties. Dit geldt voor alle informatie waarvan Opdrachtnemer het vertrouwelijk karakter kent of redelijkerwijs kan vermoeden. Enkel na voorafgaand, uitdrukkelijk en schriftelijke goedkeuring van Opdrachtgever of organisatie aan wie de informatie toebehoort, mag over de Bijzondere Opdracht buiten de geautoriseerde personen of organisaties worden gecommuniceerd.
69	ABRO-maatregel. Beschermen bedrijfsinformatie	ABRO 2026	1.6.2		Het maken van Opnamen van een Te Beschermen Belang en/of het Compartiment, anders dan noodzakelijk voor het uitvoeren van de Bijzondere Opdracht, is niet toegestaan. Tenzij in afstemming met NBIV voorafgaande schriftelijke goedkeuring van Opdrachtgever is verkregen.
70	ABRO-maatregel. Beschermen bedrijfsinformatie	ABRO 2026	1.6.3		Opdrachtnemer maakt contactgegevens van en afspraken met NBIV op geen enkele wijze (publiekelijk) bekend.
71	ABRO-maatregel. Beschermen bedrijfsinformatie	ABRO 2026	4.2.6		Data Leak Prevention (DLP) maatregelen zijn geïmplementeerd in Systemen, Netwerken en andere apparaten waarop of waarmee Bijzondere Informatie wordt gegenereerd, verwerkt of opgeslagen ter voorkoming van het onbedoeld delen (bijvoorbeeld per e-mail) van Bijzondere Informatie.
72	ABRO-maatregel. Capaciteitsbeheer	ABRO 2026	4.14.2		Er zijn voorzieningen ingesteld om voortdurend de Beschikbaarheid van de componenten die betrokken zijn bij de verwerking en opslag van Bijzondere Informatie te monitoren. Op basis van voorspellende analyses van het gebruik worden tijdig maatregelen genomen om de capaciteit indien nodig uit te breiden.
73	ABRO-maatregel. Capaciteitsbeheer	ABRO 2026	4.14.3		Er zijn beperkingen opgelegd aan Gebruikers en Systemen ten aanzien van het gebruik van gemeenschappelijke Middelen, zodat een enkele Gebruiker (of Systeem) de Beschikbaarheid van Systemen voor andere Gebruikers (of Systemen) niet in gevaar kan brengen.
74	ABRO-maatregel. Classificatie van informatie	ABRO 2026	1.1.2		Opdrachtnemer voert een Risicoanalyse uit voor de Bijzondere Opdracht(en) en neemt daarbij de resultaten van de door Opdrachtgever uitgevoerde Risicoanalyse mee. De Risicoanalyse wordt minimaal jaarlijks door Opdrachtnemer geëvalueerd en indien nodig herzien. Hierin is ten minste: - uitgewerkt met welke soort dreigingen Opdrachtnemer rekening moet houden bij het uitvoeren van de Bijzondere Opdracht(en); - geïdentificeerd, geanalyseerd en geëvalueerd welke risico's van toepassing zijn op het uitvoeren van de Bijzondere Opdracht(en) inclusief het Te Beschermen Belang.
75	ABRO-maatregel. Classificatie van informatie	ABRO 2026	1.1.3		Opdrachtnemer heeft een risicomanagementproces vastgesteld en geïmplementeerd in relatie tot de Bijzondere Opdracht(en) en het Te Beschermen Belang.

76	ABRO-maatregel. Classificatie van informatie	ABRO 2026	4.2.3		Verwijderbare gegevensdragers zijn voorzien van een fysiek label conform bijlage 8 op basis van de hoogste Rubricering van hetgeen opgeslagen is op de betreffende Verwijderbare gegevensdrager.
77	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.1.1		Opdrachtnemer beschikt over een door het Hoogste bestuursorgaan van de Opdrachtnemer bekrachtigd integraal beveiligingsbeleid dat organisatorische, personele, fysieke en cybersecurity-aspecten beschrijft. Dit beleid kent geen belemmeringen om te kunnen voldoen aan de vanuit ABRO 2026 vereiste maatregelen.
78	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.1.4		Opdrachtnemer draagt een medewerker aan voor de rol van Beveiligingsfunctionaris bij NBIV conform formulier 'Aanstelling Beveiligingsfunctionaris'. Na goedkeuring wordt de Beveiligingsfunctionaris benoemd door NBIV. Afhankelijk van de aard en omvang van de Bijzondere Opdracht(en), het aantal betrokken locaties en specialismen kunnen zo nodig één of meerdere sub-Beveiligingsfunctionarissen worden benoemd.
79	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.1.5		Afhankelijk van de aard en omvang van de Bijzondere Opdracht(en), kan Opdrachtnemer een medewerker aandragen voor de rol van Cyber-Beveiligingsfunctionaris bij NBIV conform formulier 'Aanstelling Beveiligingsfunctionaris'. Na goedkeuring wordt de Cyber-Beveiligingsfunctionaris benoemd door NBIV. Zo nodig kunnen één of meerdere sub-Cyber-Beveiligingsfunctionarissen worden benoemd, zie ook bijlage 2.
80	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.1.6		De Beveiligingsfunctionaris fungeert als primair contactpersoon voor NBIV. De Beveiligingsfunctionaris: - is in loondienst van het betreffende bedrijf; - heeft een directe rapportagelijn met het Hoogste bestuursorgaan van Opdrachtnemer; - beschikt over voldoende mandaat, senioriteit, uitvoeringsvermogen en controle over relevante uitvoerende medewerkers om zonder tussenkomst van superieuren de verantwoordelijkheden uit te voeren; - beschikt over een VOG of een VGB op het hoogst geldende Rubriceringsniveau van de Bijzondere Opdracht(en).
81	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.1.7		Indien bij de Bijzondere Opdracht gebruik wordt gemaakt van Cryptografische beveiligingsoplossingen draagt Opdrachtnemer een medewerker aan voor de rol van Cryptobeheerder bij NBIV conform formulier 'Aanstelling Cryptobeheerder'. Na goedkeuring wordt de Cryptobeheerder benoemd door NBIV. Zo nodig kunnen meerdere Cryptobeheerders worden benoemd, zie ook bijlage 3.
82	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.1.8		Opdrachtnemer beschikt over een Beveiligingsplan opgesteld door de Beveiligingsfunctionaris, conform bijlage 1. Het Beveiligingsplan is goedgekeurd door het Hoogste bestuursorgaan van Opdrachtnemer, geaccordeerd door NBIV en eenduidig geïmplementeerd.
83	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.1.9		Het Beveiligingsplan is alleen toegankelijk voor Geautoriseerde Medewerkers en bij het opstellen en behandelen van het Beveiligingsplan zijn maatregelen getroffen om de Integriteit en Vertrouwelijkheid te waarborgen, waaronder het toepassen van 'Need-to-Be' en 'Need-to-Know'.
84	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.2.6		De Beveiligingsfunctionaris houdt een actuele registratie bij van alle medewerkers met een VGB, VOG en ondertekende Geheimhoudingsverklaring(en).
85	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.2.7		De Beveiligingsfunctionaris beschikt over een actueel overzicht van alle Te Beschermen Belangen die in beheer zijn van Opdrachtnemer.
87	ABRO-maatregel. Formele vastlegging handelen verwerker	ABRO 2026	1.2.9		De Beveiligingsfunctionaris houdt een actuele registratie bij van wie welke Bijzondere Informatie in zijn bezit heeft.

90	ABRO-maatregel. Fysieke opslag	ABRO 2026	3.9.2		Gegevensdragers waarop Bijzondere Informatie wordt verwerkt of opgeslagen, zijn voorzien van een kenmerk (labeling) conform bijlage 8, waarbij verschillende Rubriceringsdomeinen en -niveaus duidelijk te onderscheiden zijn.
92	ABRO-maatregel. Fysieke opslag	ABRO 2026	3.9.4		Er zijn niet meer reproducties gemaakt dan noodzakelijk voor de uitvoering van de Bijzondere Opdracht.
95	ABRO-maatregel. Fysieke opslag	ABRO 2026	3.9.8		Beveiligingsmaatregelen voor reproductiemiddelen worden in afstemming met NBIV vastgesteld.
96	ABRO-maatregel. Fysieke opslag	ABRO 2026	3.9.9		Het vernietigen van Bijzondere Informatie geschiedt na toestemming van Opdrachtgever conform de in bijlage 8 gespecificeerde vernietigingsmethode door een Geautoriseerde Medewerker.
100	ABRO-maatregel. Geheimhouding	ABRO 2026	1.1.15		Toegang tot een Te Beschermen Belang of Systeem uit hoofde van controles of audits door anderen dan wettelijke toezichthouders of andere bij wet gemandateerde instanties, is vooraf goedgekeurd door NBIV.
101	ABRO-maatregel. Geheimhouding	ABRO 2026	1.1.16		In het geval van controles, audits en onderzoeken in relatie tot de Bijzondere Opdracht door derden (zoals NAVO, EU of ESA), stemt Opdrachtnemer op voorhand af met NBIV.
102	ABRO-maatregel. Geheimhouding	ABRO 2026	1.1.17		Bij beëindiging van de Bijzondere Opdracht dient Opdrachtnemer alle door Opdrachtgever verstrekte of tijdens de Bijzondere Opdracht gegenereerde Te Beschermen Belangen te retourneren conform een met Opdrachtgever vastgesteld proces, tenzij Opdrachtgever in afstemming met NBIV, voorafgaand schriftelijk goedkeuring heeft verleend het Te Beschermen Belang te vernietigen middels goedgekeurde procedures en methodes.
103	ABRO-maatregel. Geheimhouding	ABRO 2026	2.1.1		Betrokken Medewerkers beschikken over een VOG op basis van het door Opdrachtgever vastgestelde screeningsprofiel voor het uitvoeren van de betreffende functie. Een VOG is niet ouder dan de door Opdrachtgever gestelde termijn.
105	ABRO-maatregel. Geheimhouding	ABRO 2026	2.1.3		Opdrachtnemer houdt een actuele registratie bij van de Bijzondere Opdracht(en) en de Betrokken Medewerker(s) met daarbij de VOG of VGB en afgiftedatum.
106	ABRO-maatregel. Geheimhouding	ABRO 2026	2.1.4		Indien bij een internationale opdracht nationaliteitseisen worden vastgesteld door Opdrachtgever, worden deze door Opdrachtnemer nageleefd.
107	ABRO-maatregel. Geheimhouding	ABRO 2026	2.1.5		Opdrachtnemer heeft in afstemming met NBIV vastgesteld of er medewerkers zijn die voor de uitvoering van hun functie beschikken over Buitengewone bevoegdheden of toegangsrechten (bijvoorbeeld Beheerders) en daarmee een bovengemiddeld risico vormen voor een Te Beschermen Belang.
108	ABRO-maatregel. Geheimhouding	ABRO 2026	2.1.6		Voor Betrokken Medewerkers met Buitengewone bevoegdheden of toegangsrechten, zoals Beheerders, facilitair medewerkers, servicedeskmedewerkers en securityanalisten, heeft Opdrachtnemer in afstemming met Opdrachtgever en NBIV additionele beveiligingsmaatregelen getroffen.

109	ABRO-maatregel. Geheimhouding	ABRO 2026	2.1.7		Indien Opdrachtgever periodieke vernieuwing van een VOG van Betrokken Medewerkers vereist, vraagt de Beveiligingsfunctionaris minimaal 1 maand voor het verstrijken van de afgesproken termijn een nieuw VOG aan.
111	ABRO-maatregel. Geheimhouding	ABRO 2026	2.2.1		Betrokken Medewerkers hebben een Geheimhoudingsverklaring ondertekend conform formulier 'Geheimhoudingsverklaring'. Deze verklaringen worden bewaard door de Beveiligingsfunctionaris en op verzoek worden specifieke Geheimhoudingsverklaringen verstrekt aan NBIV.
112	ABRO-maatregel. Geheimhouding	ABRO 2026	2.2.2		De Cryptobeheerder is als Vertrouwensfunctionaris aangemerkt en heeft een Geheimhoudingsverklaring getekend conform formulier 'Geheimhoudingsverklaring Cryptobeheerder'. Deze verklaring wordt bewaard door de Beveiligingsfunctionaris en op verzoek worden specifieke verklaringen verstrekt aan NBIV.
113	ABRO-maatregel. Geheimhouding	ABRO 2026	2.3.1		Wanneer een medewerker door Opdrachtnemer ontheven wordt als Vertrouwensfunctionaris meldt de Beveiligingsfunctionaris dit aan NBIV. Dit gebeurt bijvoorbeeld bij of gelijktijdig met de volgende aanleidingen: - functiewijziging van een Vertrouwensfunctionaris; - ontslag van een Vertrouwensfunctionaris; - intrekken van de VGB; - overtreding van beveiligingsregels door een Vertrouwensfunctionaris.
114	ABRO-maatregel. Geheimhouding	ABRO 2026	2.3.2		De Beveiligingsfunctionaris heeft aan de medewerker een toelichting gegeven op de ontheffingsverklaring, de VOG en VGB-registratie bijgewerkt, en zeker gesteld dat de medewerker geen toegang meer heeft tot of beschikt over een Te Beschermen Belang. Bij ontheffing uit een Vertrouwensfunctie ontvangt NBIV van de Beveiligingsfunctionaris een door de medewerker getekende ontheffingsverklaring conform formulier 'Ontheffing uit Vertrouwensfunctie'.
115	ABRO-maatregel. Geheimhouding	ABRO 2026	2.3.3		Er is een procedure voor veranderingen op personeelsvlak (o.a. verandering of beëindiging van functie of dienstverband) of in de contractuele relatie tussen Opdrachtnemer en Opdrachtgever. Deze omvat minimaal: - het intrekken van toegangsrechten; - het innemen van ICT-bedrijfsmiddelen; - de verantwoordelijkheden en taken met betrekking tot beveiliging van de Bijzondere Opdracht die ook na de beëindiging van het dienstverband van kracht blijven, zoals bijvoorbeeld de geheimhouding; - hoe uitgevoerde handelingen naar aanleiding van de verandering of beëindiging worden vastgelegd.
116	ABRO-maatregel. Geheimhouding	ABRO 2026	2.4.1		Opdrachtnemer verleent medewerking bij het ontheffen van een (Cyber-)Beveiligingsfunctionaris of Cryptobeheerder op aangeven van NBIV. Dit gebeurt bijvoorbeeld bij of gelijktijdig met de volgende aanleidingen: - overtreding van beveiligingsregels of -beleid; - handelen in strijd met ABRO 2026; - geen uitvoering geven aan instructies van NBIV; - niet naleven van wetgeving aangaande de Bijzondere Opdracht.
117	ABRO-maatregel. Geheimhouding	ABRO 2026	2.4.2		Bij ontheffing van de (Cyber-)Beveiligingsfunctionaris ontvangt NBIV een door de medewerker getekende ontheffingsverklaring conform formulier 'Ontheffing Beveiligingsfunctionaris'.
118	ABRO-maatregel. Geheimhouding	ABRO 2026	2.4.3		Bij ontheffing van de Cryptobeheerder ontvangt NBIV een door de medewerker getekende ontheffingsverklaring conform formulier 'Ontheffing Cryptobeheerder'.
119	ABRO-maatregel. Recht op audit	ABRO 2026	1.1.11		Opdrachtnemer overlegt zo snel als mogelijk en uiterlijk binnen 48 uur na een daartoe strekkend verzoek van NBIV een actuele registratie van Bedrijfsmiddelen die worden gebruikt voor de Bijzondere Opdracht(en).

120	ABRO-maatregel. Recht op audit	ABRO 2026	1.1.12		Minimaal jaarlijks en op verzoek van NBIV verstrekt de Beveiligingsfunctionaris een overzicht aan NBIV met alle door de Opdrachtnemer gebruikte externe IP-adressen, Internet Service Provider(s) en domeinnamen, conform formulier 'IP-adressen en domeinnamen'.
121	ABRO-maatregel. Recht op audit	ABRO 2026	1.1.14		Opdrachtnemer geeft volledige medewerking bij nalevingscontroles en onderzoeken in relatie tot de Bijzondere Opdracht bij Opdrachtnemer door NBIV.
122	ABRO-maatregel. Reizen naar het buitenland	ABRO 2026	2.6.1		Bij een zakelijke reis van een Vertrouwensfunctionaris naar een Risicoland meldt de Beveiligingsfunctionaris dit bij NBIV conform formulier 'Melding bezoek Risicoland'.
123	ABRO-maatregel. Reizen naar het buitenland	ABRO 2026	2.6.2		Indien voor een zakelijke reis in het kader van de Bijzondere Opdracht een Request for Visit (RfV) benodigd is, dient de Vertrouwensfunctionaris tijdig via de Beveiligingsfunctionaris een RfV ter goedkeuring in bij NBIV. Zonder goedgekeurde RfV kan de reis niet plaatsvinden.
124	ABRO-maatregel. Reizen naar het buitenland	ABRO 2026	2.6.3		De Beveiligingsfunctionaris brieft en debrieft de Vertrouwensfunctionaris ten aanzien van de zakelijke reis naar een Risicoland. Van de debriefing wordt een verslag opgesteld en op verzoek overhandigd aan NBIV.
125	ABRO-maatregel. Reizen naar het buitenland	ABRO 2026	2.6.4		Bij een zakelijke reis van een Betrokken Medewerker naar een Risicoland wordt gebruik gemaakt van dedicated Mobiele apparatuur die alleen voor deze reis wordt ingezet en na terugkomst wordt gewist.
126	ABRO-maatregel. Rubreceringsaanduiding	ABRO 2026	1.4.1		Opdrachtnemer beschikt over een actueel, door Opdrachtgever ingevuld en geaccordeerd, opdrachtspecifiek overzicht van Te Beschermen Belangen, zie bijlage 4.
127	ABRO-maatregel. Rubreceringsaanduiding	ABRO 2026	1.4.2		Indien de Bijzondere Opdracht met een buitenlandse Opdrachtgever aanvullende of afwijkende specifieke beveiligingsmaatregelen vereist, beschikt Opdrachtnemer over een actuele Project Security Instruction (PSI) of Security Aspect Letter (SAL).
128	ABRO-maatregel. Rubreceringsaanduiding	ABRO 2026	1.4.3		E-mailverkeer tussen Opdrachtgever en Opdrachtnemer is, ook wanneer het geen Bijzondere Informatie bevat, zodanig beveiligd (zoals middels Forced TLS) dat de Vertrouwelijkheid en Integriteit gewaarborgd is.
129	ABRO-maatregel. Rubreceringsaanduiding	ABRO 2026	1.4.4		Opdrachtnemer treft maatregelen om te waarborgen dat Bijzondere Informatie met verschillende Rubriceringsdomeinen en -niveaus gescheiden wordt verwerkt en opgeslagen.
130	ABRO-maatregel. Rubreceringsaanduiding	ABRO 2026	1.4.5		Voorafgaand aan het genereren van informatie in het kader van de Bijzondere Opdracht waarop redelijkerwijs een Rubricering van toepassing is, doet de Beveiligingsfunctionaris een verzoek tot Rubricering aan Opdrachtgever. Na vaststelling door Opdrachtgever wordt deze informatie als zodanig gegenereerd, geregistreerd en behandeld door Opdrachtnemer.
131	ABRO-maatregel. Rubreceringsaanduiding	ABRO 2026	1.4.6		In geval van onvoorziene situaties, bijvoorbeeld door een gewijzigd dreigingsbeeld, nieuwe aanvalsmethodieken, uitvoering van meerdere Bijzondere Opdrachten op een locatie of Systeem, of kennisaggregatie, kunnen binnen redelijke grenzen additionele organisatorische, personele, fysieke of Cyber beveiligingsmaatregelen worden voorgeschreven. Opdrachtnemer geeft invulling aan deze beveiligingsmaatregelen.
133	ABRO-maatregel. Transport en verzenden	ABRO 2026	3.5.1		Een Te Beschermen Belang wordt uitsluitend buiten het Compartiment gebracht als dit voor de voortgang van de werkzaamheden absoluut noodzakelijk is.

134	ABRO-maatregel. Transport en verzenden	ABRO 2026	3.5.3		De Beveiligingsfunctionaris beschrijft in het Beveiligingsplan op welke wijze om wordt gegaan met het Transport en Verzenden van een Te Beschermen Belang in het kader van de Bijzondere Opdracht conform bijlage 7. Dit wordt in afstemming met NBIV ter goedkeuring voorgelegd aan Opdrachtgever.
135	ABRO-maatregel. Transport en verzenden	ABRO 2026	3.5.4		Voorafgaand aan een Transport of Verzenden van een Te Beschermen Belang wordt door de Beveiligingsfunctionaris vastgesteld dat de ontvangende partij het Te Beschermen Belang conform het vastgestelde beveiligingsniveau kan behandelen en geautoriseerd is om te beschikken over het Te Beschermen Belang.
136	ABRO-maatregel. Transport en verzenden	ABRO 2026	3.6.1		Voorafgaand aan Verzenden wordt het Te Beschermen Belang verpakt zodat de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.
137	ABRO-maatregel. Transport en verzenden	ABRO 2026	3.6.2		Verzenden van een Te Beschermen Belang is uitsluitend toegestaan wanneer dit aangetekend wordt verzonden met track en trace nummer en met onmiddellijke ontvangstbevestiging.
139	ABRO-maatregel. Transport en verzenden	ABRO 2026	3.7.1		Het fysiek Transport van een Te Beschermen Belang (zoals goederen en materieel) wordt uitgevoerd conform de door Opdrachtgever vastgestelde beveiligingsmaatregelen.
142	ABRO-maatregel. Transport en verzenden	ABRO 2026	3.8.3		Bijzondere Informatie wordt getransporteerd in een afsluitbaar Transportmiddel waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.
145	ABRO-maatregel. Transport en verzenden	ABRO 2026	3.8.6		Transport van Bijzondere Informatie vindt op één van onderstaande manieren plaats: - handcarried, al dan niet met eigen vervoer, door een Geautoriseerde Medewerker; - door een koeriersbedrijf.
149	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.1		Opdrachtnemer heeft ten behoeve van de ABRO-Verklaring een verklaring van eigendom, Zeggenschap en bedrijfsstructuur opgesteld conform formulier 'Verklaring van eigendom, Zeggenschap en bedrijfsstructuur' en verstrekt aan NBIV.
150	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.2		Opdrachtnemer legt elke voorgenomen wijziging in eigendom, Zeggenschap (inclusief bestuurders), bedrijfsstructuur of aandeelhouderschap (inclusief wijzigingen naar aanleiding van voorgenomen (her)financiering) van Opdrachtnemer onmiddellijk conform formulier 'Wijziging van eigendom, Zeggenschap en bedrijfsstructuur' schriftelijk ter goedkeuring voor aan NBIV, zodanig dat NBIV de voorgenomen wijziging tijdig kan beoordelen.
151	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.3		Opdrachtnemer meldt elke voorgenomen samenwerking met buitenlandse bedrijven of overheden onmiddellijk schriftelijk aan NBIV.
152	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.4		Opdrachtnemer meldt elk van de volgende gebeurtenissen onmiddellijk conform formulier 'Wijziging van eigendom, Zeggenschap en bedrijfsstructuur' schriftelijk aan NBIV: voorgenomen splitsing, strategische samenwerking, Uitbesteding, sourcing, fusie, verandering in Significante invloed, dreigende gedeeltelijke of volledige overname (inclusief binding en 'non-binding offers'), bedrijfsbeëindiging, surseance van betaling of faillissement.

153	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.5		Managementbeslissingen aangaande voorgenomen splitsing, strategische samenwerking, Uitbesteding, sourcing, fusie, veranderingen in Significante invloed en dreigende gedeeltelijke of volledige overname (inclusief binding en 'non-binding offers') worden onmiddellijk conform formulier 'Wijziging van eigendom, Zeggenschap en bedrijfsstructuur' schriftelijk ter goedkeuring voorgelegd aan NBIV, zodanig dat NBIV de voorgenomen wijziging tijdig kan beoordelen.
154	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.6		Opdrachtnemer meldt elke voorgenomen wijziging van bedrijfsactiviteiten, locaties of veranderende omgevingsfactoren rond bestaande locaties die (in)direct betrekking hebben op een Bijzondere Opdracht, onmiddellijk schriftelijk aan NBIV conform formulier 'Wijziging van eigendom, Zeggenschap en bedrijfsstructuur'.
155	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.7		Het verplaatsen van een Te Beschermen Belang of werkzaamheden in het kader van een Bijzondere Opdracht anders dan opgenomen in het Beveiligingsplan, gebeurt alleen na schriftelijke goedkeuring van NBIV en in afstemming met Opdrachtgever.
156	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.8		Opdrachtnemer verschaft duidelijkheid bij welk (onderdeel van het) bedrijf en op welke locatie de Bijzondere Opdracht wordt belegd en streeft maximaal naar onderbrenging van alle Bijzondere Opdrachten bij één duidelijk herkenbaar en juridisch en organisatorisch af te schermen (onderdeel van het) bedrijf.
157	ABRO-maatregel. Zeggenschap en bedrijfsstructuur	ABRO 2026	1.3.9		Opdrachtgever kan op basis van een Risicoanalyse, in afstemming met NBIV vaststellen dat er additionele risico's zijn waarvoor aanvullende beveiligingsmaatregelen moeten worden getroffen door Opdrachtnemer. Voorbeelden van aanvullende beveiligingsmaatregelen zijn verplichte verwerking of behandeling op Nederlands grondgebied door een in Nederland gevestigde rechtspersoon.
158	Privacybeleid	Privacy-supplement Algemeen	ALG P.01		De organisatie heeft privacybeleid en procedures ontwikkeld en vastgesteld, waarin de verantwoordelijkheid is vastgelegd op welke wijze persoonsgegevens worden verwerkt, invulling wordt gegeven aan de wettelijke beginselen en hoe in een cyclisch proces wordt vastgelegd op welke wijze transparant aan de wet- en regelgeving wordt voldaan en afwijkingen worden opgelost.
159	Privacy-organisatie	Privacy-supplement Algemeen	ALG P.02		De verdeling van de taken en verantwoordelijkheden, de benodigde middelen en de rapportagelijnen, zijn door de organisatie vastgelegd en vastgesteld , inclusief die bij uitwisseling van persoonsgegevens tussen organisaties, zodat ook bij doorgifte van persoonsgegevens de privacybelangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, zijn gewaarborgd.
160	Privacy-bewustzijn	Privacy-supplement Algemeen	ALG P.03		De organisatie waarborgt dat eenieder die persoonsgegevens verwerkt of een verwerking voorbereidt zich bewust is van de belangen van de betrokkenen, waarvan de persoonsgegevens worden verwerkt, en beschouwt dit conform de verwachtingen als hoogste prioriteit om deze overtuiging toe te passen; deze betrokkenen hebben daarvoor de benodigde kennis en zijn op de hoogte van grote veranderingen in de verwachtingen.
161	Formele vastlegging handelen verwerker	Privacy-supplement Algemeen	ALG P.04		De organisatie heeft van eenieder, die persoonsgegevens verwerkt of een verwerking voorbereidt, een actuele VOG, een actuele verklaring terzake het naleven en de kennisname van de regels omtrent privacy en het bewijs van op de hoogte zijn van de disciplinaire procedure; hiervan bestaat een overzicht.
162	Privacy in de levenscyclus	Privacy-supplement Algemeen	ALG P.05		Vooraf aan het ontwerp van een gegevensverwerking en bij een verandering wordt een inschatting gemaakt van de privacyrisico’s en wordt bepaald welke passende maatregelen nodig zijn; hiervoor zijn de verantwoordelijkheden duidelijk en is een proces ingeregeld voor het kunnen aantonen van het passend zijn van deze maatregelen.
163	Register van verwerkingsactiviteiten	Privacy-supplement Algemeen	ALG P.06		De verwerkingsverantwoordelijke(n) en de verwerker(s) hebben hun gegevens over de gegevensverwerkingen in een register vastgelegd, daarbij biedt het register een actueel en samenhangend beeld van de gegevensverwerkingen, processen en technische systemen die betrokken zijn bij het verzamelen, verwerken en doorgeven van persoonsgegevens en dat voldoet aan de vereisten van de AVG.

164	Datalekken	Privacy-supplement Algemeen	ALG P.07		De organisatie heeft de kennis georganiseerd om de oorzaak van een datalek te kunnen vaststellen en te onderzoeken, heeft daarvoor de benodigde loggegevens om herhaling te voorkomen en heeft de stakeholders vastgesteld om ze te kunnen informeren.
453	Beleid en procedures voor informatietransport	Thema Communicatievoorzieningen	B.01		Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.
455	ABRO-maatregel. Beleid en procedures voor informatietransport	ABRO 2026	4.5.28		Ontsluiting van een Te Beschermen Belang op een Netwerk tussen verschillende locaties van de Opdrachtnemer (WAN) is niet toegestaan.
457	Cryptografiebeleid voor communicatie	Thema Communicatievoorzieningen	B.03	Ja	Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.
458	ABRO-maatregel. Cryptografiebeleid voor communicatie	ABRO 2026	4.5.20		De gebruikte versleutelingsprotocollen zijn de meest recente conform (inter)nationale beveiligingsstandaarden. Nieuw gepubliceerde standaarden dienen binnen de minimaal haalbare termijn geïmplementeerd te worden. Aansluitvoorwaarden van Opdrachtgever prevaleren en afwijkingen worden gemeld aan NBIV.
459	ABRO-maatregel. Cryptografiebeleid voor communicatie	ABRO 2026	4.5.21		Netwerken voor verschillende Rubriceringsdomeinen zijn gescheiden en toegang is beveiligd middels Goedgekeurde Middelen.
462	Organisatiestructuur netwerkbeheer	Thema Communicatievoorzieningen	B.04		In het beleid behoort te zijn vastgesteld dat een centrale organisatiestructuur gebruikt wordt voor het beheren van netwerken (onder andere Local Area Network (LAN) en Virtual Local Area Network (VLAN)) en zo veel mogelijk van de hardware en softwarecomponenten daarvan.
463	Richtlijnen voor netwerkbeveiliging	Thema Communicatievoorzieningen	U.01		Organisaties behoren hun netwerken te beveiligen op basis van richtlijnen voor ontwerp, implementatie en beheer.
464	ABRO-maatregel. Richtlijnen voor netwerkbeveiliging	ABRO 2026	1.7.3		Beveiligingsincidenten worden na constatering geverifieerd en direct aan NBIV gemeld conform formulier 'Melding Beveiligingsincident'.

465	ABRO-maatregel. Richtlijnen voor netwerkbeveiliging	ABRO 2026	1.7.4		Gegevens ten aanzien van toegang tot en inzicht in een Te Beschermen Belang zijn vastgelegd en worden 3 maanden bewaard om achteraf onderzoek naar vermoede Beveiligingsincidenten mogelijk te maken.
467	ABRO-maatregel. Richtlijnen voor netwerkbeveiliging	ABRO 2026	1.7.6		Alle beschikbare informatie die direct gerelateerd is aan een Beveiligingsincident wordt bewaard voor een periode die na Melding in afstemming met NBIV wordt bepaald.
468	ABRO-maatregel. Richtlijnen voor netwerkbeveiliging	ABRO 2026	4.5.7		Alle beveiligingsmechanismes maken gebruik van actuele indicatoren, zoals virusdefinities en Signatures.
469	ABRO-maatregel. Richtlijnen voor netwerkbeveiliging	ABRO 2026	4.5.8		Beveiligingsmechanismes ten behoeve van de Bijzondere Opdracht mogen niet voortkomen uit een land dat een Offensief cyberprogramma tegen de Nederlandse belangen heeft.
470	ABRO-maatregel. Richtlijnen voor netwerkbeveiliging	ABRO 2026	4.5.9		Minimaal jaarlijks worden de geïmplementeerde beveiligingsmaatregelen op een Koppelvlak getest op de werking. Bevindingen worden opgevolgd en gedocumenteerd.
472	ABRO-maatregel. Richtlijnen voor netwerkbeveiliging	ABRO 2026	4.5.18		TOR (The Onion Router)/Darknet verkeer is geblokkeerd.
473	Beveiligde inlogprocedure	Thema Communicatievoorzieningen	U.02	Ja	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.

474	O-maatregel. Beveiligde inlogprocedures	BIO 2019	9.4.2.1	Ja	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.
476	Netwerkbeveiligingsbeheer	Thema Communicatievoorzieningen	U.03		Netwerken en netwerkapparaten behoren te worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
477	ABRO-maatregel. Netwerkbeveiligngsbeheer	ABRO 2026	4.4.5		Het interne en externe dataverkeer wordt op basis van een Risicoanalyse beperkt tot de noodzakelijke protocollen en sessies.
478	ABRO-maatregel. Netwerkbeveiligngsbeheer	ABRO 2026	4.4.6		Software, servers, gebruikers-, netwerk- en opslagapparatuur worden middels een vastgesteld proces voorzien van veilige configuraties. Deze configuraties zijn vastgelegd, worden minimaal jaarlijks beoordeeld en waar nodig aangepast en op verzoek gedeeld met NBIV.
479	ABRO-maatregel. Netwerkbeveiligngsbeheer	ABRO 2026	4.5.17		Technische en procedurele maatregelen zijn getroffen om te waarborgen dat alleen geïdentificeerde en geauthentiseerde apparatuur kan worden verbonden met het Netwerk. Wanneer onbekende apparatuur wordt aangesloten vindt er alarmering plaats.
480	Vertrouwelijkheids- en of geheimhoudingsovereenkomst	Thema Communicatievoorzieningen	U.04		Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.
481	ABRO-maatregel. Vertrouwelijkheids- en of geheimhoudingsovereenkomst	ABRO 2026	1.7.9		Opdrachtnemer heeft in haar beveiligingsbeleid vastgelegd hoe wordt omgegaan met medewerkers die bewust of onbewust een Beveiligingsincident veroorzaken, welke disciplinaire maatregelen mogelijk zijn en dat in het geval van strafbare feiten aangifte wordt gedaan.
482	Beveiliging van netwerkdiensten	Thema Communicatievoorzieningen	U.05	Ja	Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.
486	O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.4	Ja	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.
487	Zonering en filtering	Thema Communicatievoorzieningen	U.06	Ja	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).
489	ABRO-maatregel. Zonering en filtering	ABRO 2026	4.5.5		In geval van een Externe (netwerk) koppeling is een DMZ toegepast.
490	ABRO-maatregel. Zonering en filtering	ABRO 2026	4.5.6		Voor in- en uitgaand dataverkeer van en naar een onvertrouwde omgeving, zowel intern als extern, zijn beveiligingsmaatregelen getroffen zoals een DMZ, Proxy-server en/of sandbox.
491	Elektronische berichten	Thema Communicatievoorzieningen	U.07	Ja	Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.
492	O-maatregel. Elektronische berichten	BIO 2019	13.2.3.1	Ja	Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen phishing en afluisteren op pas-toe-of-leg-uit lijst van het forum standaardisatie.

496	Toepassingen via openbare netwerken	Thema Communicatievoorzieningen	U.08		Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.
497	Gateways en firewalls	Thema Communicatievoorzieningen	U.09		De filterfuncties van gateways en firewalls behoren zo te zijn geconfigureerd, dat inkomend en uitgaand netwerkverkeer wordt gecontroleerd en dat daarbij in alle richtingen uitsluitend het vanuit beveiligingsbeleid toegestaan netwerkverkeer wordt doorgelaten.
498	Virtual Private Networks	Thema Communicatievoorzieningen	U.10		Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie, is voorbehouden aan tot de organisatie die de VPN gebruikt.
499	ABRO-maatregel. Virtual Private Networks	ABRO 2026	4.5.34		Bij de toepassing van Virtualisatie in het kader van de Bijzondere Opdracht wordt een Risicoanalyse uitgevoerd door de (Cyber-) Beveiligingsfunctionaris en een Beheerder. Hierbij gelden ten minste de volgende voorwaarden: - beveiligingsfunctionaliteiten draaien op fysiek gescheiden virtualisatieplatforms; - alleen systeemcomponenten met hetzelfde Rubriceringsdomein en -niveau worden gecombineerd; - het ontwerp en de implementatie zijn vooraf goedgekeurd door NBIV; - de management interface is enkel bereikbaar vanuit het beheersegment; - het Virtualisatie platform is gehardend conform de instructie van de leverancier.
500	ABRO-maatregel. Virtual Private Networks	ABRO 2026	4.5.35		Het toepassen van VLAN's is alleen toegestaan in Netwerken met hetzelfde Rubriceringsdomein en -niveau. Het ontwerp en de implementatie zijn vooraf goedgekeurd door NBIV. Hierbij gelden ten minste de volgende voorwaarden: - een firewall wordt gebruikt om ongewenst verkeer te filteren; - marktstandaarden voor de configuratie van VLAN's zijn toegepast; - netwerkpoorten worden statisch of op basis van een certificaat toegewezen aan een VLAN.
501	Cryptografische services	Thema Communicatievoorzieningen	U.11	Ja	Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.
502	O-maatregel. Voorschriften voor het gebruik van cryptografische beheersmaatregelen	BIO 2019	18.1.5.1	Ja	Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de pas-toe-of-leg-uit lijst van het forum standaardisatie.
503	Draadloze toegang	Thema Communicatievoorzieningen	U.12		Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.
504	ABRO-maatregel. Draadloze toegang	ABRO 2026	4.5.3		Alle Draadloze communicatie wordt behandeld als Externe (netwerk) koppeling.
506	Netwerkconnecties	Thema Communicatievoorzieningen	U.13		Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.
507	ABRO-maatregel. Netwerkconnecties	ABRO 2026	4.4.7		Een mechanisme controleert de instellingen van informatiebeveiligingsfuncties (zoals securitysoftware) op het Koppelvlak tussen verschillende Netwerken op ongeautoriseerde wijzigingen.

508	ABRO-maatregel. Netwerkconnecties	ABRO 2026	4.5.2		Continue real-time Monitoring en Logging van al het inkomende en uitgaande netwerkverkeer en netwerkkoppelingen zijn ingericht, waarbij wordt gelet op afwijkingen van het normaalbeeld en waar nodig (geautomatiseerd) wordt ingegrepen.
509	ABRO-maatregel. Netwerkconnecties	ABRO 2026	4.5.12		In Koppelvlakken met externe of onvertrouwde Netwerken zijn maatregelen getroffen om mogelijke aanvallen die de Betrouwbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld (D)DoS-aanvallen) te signaleren en hierop te reageren.
510	ABRO-maatregel. Netwerkconnecties	ABRO 2026	4.5.23		Internationale Netwerkkoppelingen maken gebruik van door NBIV goedgekeurde producten en procedures.
511	ABRO-maatregel. Netwerkconnecties	ABRO 2026	4.5.25		Netwerken van verschillende juridische entiteiten waarop een Te Beschermen Belang is opgeslagen zijn alleen gekoppeld na goedkeuring van Opdrachtgever. Alle entiteiten beschikken over de vereiste ABRO-Verklaring, de koppeling maakt gebruik van Goedgekeurde Middelen en door NBIV goedgekeurde procedures, en er is voldaan aan de aansluitvoorwaarden van de betreffende Netwerken.
512	ABRO-maatregel. Netwerkconnecties	ABRO 2026	4.5.26		Bij Koppelvlakken tussen Netwerken van verschillende Rubriceringsniveaus is informatie-uitwisseling alleen mogelijk van een Netwerk met een lager Rubriceringsniveau naar een Netwerk met een hoger Rubriceringsniveau. De koppeling maakt gebruik van Goedgekeurde Middelen. Uitgewisselde informatie wordt behandeld conform het Rubriceringsniveau van het Segment waarop de informatie zich bevindt.
514	ABRO-maatregel. Netwerkconnecties	ABRO 2026	4.13.4		Er zijn maatregelen getroffen (zoals IDS, Intrusion Prevention System (IPS) en Security Information & Event Management (SIEM)) om afwijkingen van het normbeeld (anomalies) en ongebruikelijke creaties, aanwezigheid en/of beëindiging van processen te detecteren en te onderzoeken op dreigingen.
515	Netwerkauthenticatie	Thema Communicatievoorzieningen	U.14		Authenticatie van netwerkknooppunten behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.
516	Netwerkbeheeractiviteiten	Thema Communicatievoorzieningen	U.15		Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.
517	Logging en monitoring	Thema Communicatievoorzieningen	U.16	Ja	Netwerken behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren; logbestanden worden geregistreerd en bewaard.
518	ABRO-maatregel. Logging binnen communicatievoorzieningen	ABRO 2026	4.4.8	Ja	De instellingen van logmechanismen zijn zodanig beschermd dat deze niet onopgemerkt aangepast of gemanipuleerd kunnen worden. Wijzigingen worden gecontroleerd middels het vier-ogen principe.
519	ABRO maatregel. Logging en monitoring	ABRO 2026	4.5.1	Ja	Netwerken, Systemen en applicaties worden gemonitord en beheerd zodat aanvallen, storingen en/of fouten ontdekt en hersteld kunnen worden en de Beschikbaarheid niet onder het afgesproken minimum niveau komt. Dit minimum is opgenomen in het Beveiligingsplan.
520	ABRO maatregel. Logging en monitoring	ABRO 2026	4.5.19	Ja	Op verzoek van NBIV wordt door Opdrachtnemer medewerking verleend aan: - het plaatsen van een detectiemiddel; - het monitoren van netwerkverkeer en hosts door gebruik van een detectiemiddel; - het uitvoeren en aanleveren van specifieke Logging verzoeken voor de lokale- en Cloud omgevingen (inclusief telemetrie); - het installeren van host based detectie; - het gebruik maken van een door de Rijksoverheid geleverde DNS-dienst.

521	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.1	Ja	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.
522	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.2	Ja	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
526	Netwerk beveiligingsarchitectuur	Thema Communicatievoorzieningen	U.17		De beveiligingsarchitectuur behoort de samenhang van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende principes en de geldende normen en standaarden.
527	ABRO-maatregel. Netwerkbeveiligngsarchitectuur	ABRO 2026	4.5.24		Netwerken van eenzelfde juridische entiteit waarop een Te Beschermen Belang is opgeslagen zijn alleen gekoppeld middels Goedgekeurde Middelen en door NBIV goedgekeurde procedures.
528	Naleving richtlijn netwerkbeveiliging en evaluaties	Thema Communicatievoorzieningen	C.01		De effectiviteit van de richtlijnen voor de netwerkbeveiliging behoort periodiek getoetst en geëvalueerd te worden.
529	Compliance-toets netwerkbeveiliging	Thema Communicatievoorzieningen	C.02		De naleving van een, volgens het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliancy-toetsen).
530	Evalueren robuustheid netwerkbeveiliging	Thema Communicatievoorzieningen	C.03		De robuustheid van de beveiligingsmaatregelen en de naleving van het netwerkbeveiligingsbeleid behoren periodiek getest en aangetoond te worden.
531	Evalueren netwerkgebeurtenissen (monitoring)	Thema Communicatievoorzieningen	C.04		Toereikende logging en monitoring behoren te zijn ingericht, om detectie, vastlegging en onderzoek van gebeurtenissen mogelijk te maken van gebeurtenissen, die mogelijk van invloed op of relevant kunnen zijn voor de informatiebeveiliging.
532	ABRO-matregel. Evalueren netwerkgebeurtenissen (monitoring)	ABRO 2026	1.7.1		Opdrachtnemer heeft een Incident Response Procedure vastgesteld en geïmplementeerd voor het afhandelen en evalueren van Beveiligingsincidenten. Deze is bekend bij alle medewerkers die werken aan of toegang hebben tot een Te Beschermen Belang.
533	ABRO-matregel. Evalueren netwerkgebeurtenissen (monitoring)	ABRO 2026	1.7.2		In geval van een geconstateerde Compromittatie van een Te Beschermen Belang wordt de Beveiligingsfunctionaris onmiddellijk geïnformeerd.
534	ABRO-matregel. Evalueren netwerkgebeurtenissen (monitoring)	ABRO 2026	1.7.7		Er is een evaluatiemechanisme gedefinieerd waarmee men specifieke lessen identificeert, bijvoorbeeld naar aanleiding van een Beveiligingsincident, en waar nodig deze verwerkt in het beveiligingsbeleid en implementeert.

535	ABRO-matregel. Evalueren netwerkgebeurtenissen (monitoring)	ABRO 2026	1.7.8		In geval van grove nalatigheid of bewuste Compromittatie van een Te Beschermen Belang door een medewerker informeert de Beveiligingsfunctionaris NBIV direct.
536	Beheersorganisatie netwerkbeveiliging	Thema Communicatievoorzieningen	C.05	Ja	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.
537	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.1	Ja	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
538	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.2	Ja	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
539	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.3	Ja	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.
540	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.4	Ja	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
541	ABRO-maatregel. Scheiden binnen communicatievoorzieningen	ABRO 2026	4.5.14		Netwerken zijn voorzien van beheersmaatregelen voor routering gebaseerd op mechanismen ter verificatie van bron- en bestemmingsadressen.
542	ABRO-maatregel. Scheiden binnen communicatievoorzieningen	ABRO 2026	4.5.15		Er zijn technische maatregelen getroffen om te voorkomen dat interne netwerkadressen naar buiten toe routeren, zoals het toepassen van Outbound Traffic Filtering.
544	ABRO-maatregel. Scheiden binnen communicatievoorzieningen	ABRO 2026	4.5.29		De Technische infrastructuur is ingedeeld in Segmenten. Opdrachtnemer draagt zorg dat binnen één Segment alleen Bijzondere Informatie wordt verwerkt van hetzelfde Rubriceringsdomein en -niveau. Opdrachtnemer evalueert dit minimaal jaarlijks en herziet Segmenten indien nodig.
545	ABRO-maatregel. Scheiden binnen communicatievoorzieningen	ABRO 2026	4.5.30		Elk Segment heeft een gedefinieerd Rubriceringsdomein en -niveau. Bij Koppelvlakken tussen Segmenten vindt controle plaats op protocol, inhoud en richting van de communicatie.
546	ABRO-maatregel. Scheiden binnen communicatievoorzieningen	ABRO 2026	4.5.31		Segmenten zijn alleen ingericht met voorzieningen die strikt noodzakelijk zijn voor de functionaliteit. Beheer en audit van Segmenten vindt plaats vanuit een logisch gescheiden Segment.
548	ABRO-maatregel. Scheiden binnen communicatievoorzieningen	ABRO 2026	4.5.33		Segmentering is toegepast om groepen van Systemen, diensten en Gebruikers te scheiden in het Netwerk. Bijvoorbeeld door middel van een firewall of DMZ.

549	Scheiden binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.01		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.
550	Verbergen binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.02		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruikt wordt, waarbij het verbergen van verwerkingen het uitgangspunt is.
551	Logging binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.03		De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.
858	Wet en Regelgeving	Thema Clouddiensten	B.01		Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de CSP om aan deze eisen te voldoen behoren voor elke clouddienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.
860	ABRO-maatregel. Wet en regelgeving	ABRO 2026	5.1.2		Het gebruik van een Public Cloud-dienst (computing, opslag, transport) voor Bijzondere Informatie van de NAVO, EU of ESA is niet toegestaan zonder voorafgaande goedkeuring van NBIV.
861	ABRO-maatregel. Wet en regelgeving	ABRO 2026	5.1.3		CSP is niet gelieerd aan, niet gevestigd in, noch voert beheerwerkzaamheden uit in een land dat een Offensief cyberprogramma tegen Nederlandse belangen heeft.
862	ABRO-maatregel. Wet en regelgeving	ABRO 2026	5.1.6		Opdrachtnemer voldoet aan de voor Cloud-diensten relevante eisen uit ABRO 2026 hoofdstuk 3 en 4 zoals vermeld in bijlage 11.
863	ABRO-maatregel. Wet en regelgeving	ABRO 2026	5.5.1		CSP geeft volledige medewerking bij nalevingscontroles en onderzoeken in relatie tot de Bijzondere Opdracht door Opdrachtgever of NBIV, al dan niet uitgevoerd door een gecertificeerde derde partij.
864	Cloudbeveiligingsstrategie	Thema Clouddiensten	B.02		De CSP behoort een cloud-beveiligingsstrategie te hebben ontwikkeld die samenhangt met de strategische doelstelling van de CSP en die aantoonbaar de informatieveiligheid ondersteunt.
865	ABRO-maatregel. Cloudbeveiligingsstrategie	ABRO 2026	5.3.4		CSP richt de Cloud-dienst en -infrastructuur in volgens het concept Secure by default.
866	Exit-strategie	Thema Clouddiensten	B.03		In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exitstrategie te zijn opgenomen waarbij zowel een aantal bepalingen6 over exit zijn opgenomen, als een aantal condities6 die aanleiding kunnen geven tot een exit.
867	ABRO-maatregel. Exit-strategie	ABRO 2026	5.5.3		CSP heeft maatregelen getroffen en processen ingeregeld om invulling te geven aan de exit-strategie van Opdrachtgever en daaruit volgende bepalingen, zoals opgenomen in het contract met Opdrachtgever.

868	Clouddienstenbeleid	Thema Clouddiensten	B.04		De CSP behoort haar informatiebeveiligingsbeleid uit te breiden met een cloud-beveiligingsbeleid om de voorzieningen en het gebruik van cloudservices te adresseren.
869	Transparantie	Thema Clouddiensten	B.05		De CSP voorziet de CSC in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.
870	Risicomanagement	Thema Clouddiensten	B.06		De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.
871	ABRO-maatregel. Risicomanagement	ABRO 2026	5.2.1		Opdrachtnemer heeft een Risicoanalyse uitgevoerd op het gebruik van de Cloud-dienst op basis van de resultaten van de door Opdrachtgever uitgevoerde Risicoanalyse en relevante dreigingen inclusief statelijke actoren. Deze Risicoanalyse is in afstemming met NBIV goedgekeurd door Opdrachtgever en opgenomen in het Beveiligingsplan.
872	IT-functionaliteit	Thema Clouddiensten	B.07		IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.
873	Bedrijfscontinuïteitsmanagement	Thema Clouddiensten	B.08		De CSP behoort haar BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.
874	Privacy en bescherming persoonsgegevens	Thema Clouddiensten	B.09		De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labelen, eigenaarschap en locatie.
875	Beveiligingsorganisatie	Thema Clouddiensten	B.10	Ja	De CSP behoort een beveiligingsfunctie te hebben benoemd en een beveiligingsorganisatie te hebben ingericht, waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.
876	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.1	Ja	De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
877	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.2	Ja	De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.
878	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.3	Ja	De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.

879	O-maatregel. Rollen en verantwoordelijkheden bij informatiebeveiliging	BIO 2019	6.1.1.4	Ja	Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.
880	Clouddienstenarchitectuur	Thema Clouddiensten	B.11		De CSP heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.
881	ABRO-maatregel. Clouddienstenarchitectuur	ABRO 2026	5.3.1		CSP heeft een opdrachtspecifieke architectuur verstrekt aan NBIV waarin ten minste is gespecificeerd: - welke IT-services, functionaliteit en bedrijfsprocessen van toepassing zijn; - op welke locaties (ondersteunende) werkzaamheden, computing, opslag en transport plaatsvinden; - welke infrastructuur, netwerk- en systeemcomponenten worden gebruikt voor de ontwikkeling en de werking van de clouddienst(en); - of, en zo ja welke, IT-functies door de CSP zijn toegewezen of uitbesteed aan (Toe)leveranciers.
882	Standaarden voor clouddiensten	Thema Clouddiensten	U.01		De CSP past aantoonbaar relevante, nationale standaarden en internationale standaarden toe voor de opzet en exploitatie van de diensten en de interactie met de CSC.
883	Risico-assessment	Thema Clouddiensten	U.02		De CSP behoort een risico-assessment uit te voeren, bestaande uit een risico-analyse en risico-evaluatie met de criteria en de doelstelling voor clouddiensten van de CSP.
884	Bedrijfscontinuïteitsservices	Thema Clouddiensten	U.03		Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.
885	Herstelfunctie voor data en clouddiensten	Thema Clouddiensten	U.04		De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.
886	Dataprotectie	Thema Clouddiensten	U.05		Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.
887	ABRO-maatregel. Dataprotectie	ABRO 2026	5.1.4		Data van Opdrachtgever (inclusief Metadata en telemetrie) blijven at-rest, in-transit en in-use binnen Nederland of, indien goedgekeurd door Opdrachtgever, het grondgebied van de Europese Economische Ruimte (EER).
888	ABRO-maatregel. Dataprotectie	ABRO 2026	5.1.5		Beheer en onderhoud van de Cloud-dienst en -infrastructuur in het kader van de Bijzondere Opdracht vindt plaats binnen het grondgebied van de EER.
889	Dataretentie en gegevensvernietiging	Thema Clouddiensten	U.06	Ja	Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van de CSC/data-eigenaar te kunnen worden vernietigd.
891	Datascheiding	Thema Clouddiensten	U.07		CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.

892	Scheiding dienstverlening	Thema Clouddiensten	U.08		De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.
893	Malware-protectie	Thema Clouddiensten	U.09	Ja	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.
894	O-maatregel. Beheersmaatregelen tegen malware	BIO 2019	12.2.1.1	Ja	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.
895	O-maatregel. Beheersmaatregelen tegen malware	BIO 2019	12.2.1.2	Ja	Gebruikers zijn voorgelicht over de risico's ten aanzien van surfgedrag en het klikken op onbekende links.
896	O-maatregel. Beheersmaatregelen tegen malware	BIO 2019	12.2.1.3	Ja	De gebruikte antimalwaresoftware en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.
897	O-maatregel. Beheersmaatregelen tegen malware	BIO 2019	12.2.1.4	Ja	Computers en media worden als voorzorgsmaatregel routinematig gescand. De uitgevoerde scan behoort te omvatten: (a) Alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, vóór gebruik op malware scannen. (b) Bijlagen en downloads vóór gebruik.
898	O-maatregel. Beheersmaatregelen tegen malware	BIO 2019	12.2.1.5	Ja	De malwarescan wordt op verschillende omgevingen uitgevoerd, bijvoorbeeld op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.
899	Toegang IT-diensten en data	Thema Clouddiensten	U.10	Ja	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.
900	ABRO-maatregel. Toegang IT-diensten en data	ABRO 2026	5.5.2		CSP heeft en verstrekt procedures voor de afhandeling van onderzoeksvragen van overheidsinstanties die toegang tot Tenants of gegevens van Opdrachtgever vereisen. De procedures omvatten minimaal: - verificatie van de rechtsgrond van de onderzoeksvraag; - naar vermogen Opdrachtgever en NBIV informeren over de onderzoeksvraag en betrekken bij de afhandeling ervan; - mogelijkheden voor Opdrachtgever om in beroep te gaan tegen de onderzoeksvraag.
901	O-maatregel. Toegang tot netwerken en netwerkdiensten	BIO 2019	9.1.2.1	Ja	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.
902	O-maatregel. Toegang tot netwerken en netwerkdiensten	BIO 2019	9.1.2.2	Ja	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.
903	Cryptoservices	Thema Clouddiensten	U.11	Ja	Gevoelige data van CSC's behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld
904	ABRO-maatregel. Cryptoservices	ABRO 2026	5.4.1		CSP ondersteunt sleutelbeheer dat volledig wordt uitgevoerd door Opdrachtgever, of ondersteunt dat Opdrachtgever op basis van een met NBIV afgestemde Risicoanalyse een derde partij met ABRO-Verklaring kan inschakelen, niet zijnde de CSP.
905	ABRO-maatregel. Cryptoservices	ABRO 2026	5.4.2		Data van Opdrachtgever at-rest en in-transit is versleuteld conform de meest recente markstandaarden.
910	Koppelvlakken	Thema Clouddiensten	U.12	Ja	De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.
914	O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.4	Ja	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld DDoS-aanvallen, Distributed Denial of Service attacks) te signaleren en hierop te reageren.

915	Service-orkestratie	Thema Clouddiensten	U.13		Service-orkestratie biedt coördinatie, aggregatie en samenstelling van de servicecomponenten van de cloud-service die aan de CSC wordt geleverd.
916	ABRO-maatregel. Service-orkestratie	ABRO 2026	5.3.2		De verdeling van rollen en verantwoordelijkheden tussen CSP en Opdrachtgever voor de implementatie en uitvoering van de beveiligingsmaatregelen die van toepassing zijn op de Cloud-dienst zijn vastgelegd in een SLA en DAP. Een afschrift hiervan is opgenomen in het Beveiligingsplan.
917	Interoperabiliteit en portabiliteit	Thema Clouddiensten	U.14		Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende ITplatforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit) naar andere CSP's.
918	Logging en monitoring	Thema Clouddiensten	U.15	Ja	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
919	ABRO-maatregel. Logging en monitoring	ABRO 2026	5.3.3		CSP heeft op basis van de Risicoanalyse, indien van toepassing, in afstemming met NBIV additionele Monitoring en Logging ingeregeld, gericht op detectie van statelijke actoren.
920	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.1	Ja	Een logregel bevat minimaal: (a) de gebeurtenis; (b) de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; (c) het gebruikte apparaat; (d) het resultaat van de handeling; (e) een datum en tijdstip van de gebeurtenis.
921	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.2	Ja	Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.
925	Clouddienstenarchitectuur	Thema Clouddiensten	U.16		De clouddienstenarchitectuur specificeert de samenhang en beveiliging van de services en de interconnectie tussen de CSC en de CSP en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.
926	Multi-tenantarchitectuur	Thema Clouddiensten	U.17		Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines
927	Servicemanagementbeleid en evaluatierichtlijn	Thema Clouddiensten	C.01		De CSP heeft voor clouddiensten een servicemanagementbeleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.
928	Risico-control	Thema Clouddiensten	C.02		Risicomanagement en het risico-assessmentproces behoren continu te worden gemonitord en gereviewd en zo nodig te worden verbeterd.
929	ABRO-maatregel. Risico-control	ABRO 2026	5.2.3		CSP heeft op basis van de meest recente CSA Cloud Control Matrix (CCM) maatregelen geïmplementeerd en kan opzet, bestaan en werking aantonen, of heeft op basis van een door Opdrachtgever goedgekeurde Risicoanalyse onderbouwd waarom een of meerdere controls niet van toepassing zijn. Dit is opgenomen in het Beveiligingsplan. Wijzigingen hierin worden direct gemeld bij NBIV.
930	ABRO-maatregel. Risico-control	ABRO 2026	5.2.4		Wijzigingen in een voor de Bijzondere Opdracht relevante Assuranceverklaring of wijzigingen van maatregelen die raken aan de CSA CCM controls worden voorafgaand aan implementatie ter goedkeuring voorgelegd aan NBIV.

931	Compliance en assurance	Thema Clouddiensten	C.03	Ja	De CSP behoort regelmatig de naleving van de cloudbeveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een assurance-verklaring aan de CSC uit te brengen en te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.
932	ABRO-maatregel. Compliance en assurance	ABRO 2026	5.2.2		CSP beschikt gedurende de gehele contractperiode over een SOC2 type 2 verklaring op basis van alle trusted services criteria of een door NBIV als gelijkwaardig beoordeelde Assuranceverklaring, voor de volledige scope van de werkzaamheden. Deze verklaring is verstrekt aan NBIV.
933	ABRO-maatregel. Compliance en assurance	ABRO 2026	5.2.5		CSP heeft een opdracht specifiek Cloud-beveiligingshoofdstuk opgenomen in het Beveiligingsplan waarin is vastgelegd: - hoe de CSA CCM controls geïmplementeerd zijn en waar eventuele afwijkingen zijn van de controls; - welke aanvullende maatregelen van toepassing zijn op basis van de Risicoanalyse. Aanvullende maatregelen zijn vastgesteld in afstemming met NBIV en goedgekeurd door Opdrachtgever.
934	O-maatregel. Beoordeling van het informatiebeveiligingsbeleid	BIO 2019	5.1.2.1	Ja	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting bij de (bestaande) bestuurs- en P en C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.
937	O-maatregel. Naleving van beveiligingsbeleid en -normen	BIO 2019	18.2.2.1	Ja	In de P en C cyclus wordt gerapporteerd over informatiebeveiliging, resulterend in een jaarlijks af te geven In Control Verklaring (ICV) over de informatiebeveiliging. Indien voldoende herkenbaar kan de ICV voor informatiebeveiliging onderdeel zijn van de reguliere, generieke verantwoording.
939	Technische kwetsbaarhedenbeheer	Thema Clouddiensten	C.04	Ja	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.
940	O-maatregel. Beheer van technische kwetsbaarheden	BIO 2019	12.6.1.1	Ja	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.
941	Security-monitoringsrapportage	Thema Clouddiensten	C.05		De performance van de informatiebeveiliging van de cloud-omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan verschillende stakeholders.
942	Beheersorganisatie clouddiensten	Thema Clouddiensten	C.06		De CSP heeft een beheersorganisatie ingericht waarin de processtructuur en de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.
943	Testdata	Privacy-supplement Applicatieontwikkeling Algemeen	APO P.01		Waar mogelijk wordt als testdata gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data, wanneer op basis van de resultaten van een risico-analyse gebruik gemaakt wordt van persoonsgegevens, worden passende maatregelen ter bescherming van de persoonsgegevens genomen.

944	Privacy by Default binnen applicaties	Privacy-supplement SSD	SSD P.01		De applicatie vraagt bij elke verzameling van persoonsgegevens vrijelijk en ondubbelzinnig toestemming aan betrokkene, waarvan de persoonsgegevens worden verwerkt, om de gegevens te mogen verwerken, waarbij standaard zo min mogelijk persoonsgegevens worden verwerkt
945	Correcte en gewenste verwerking met applicaties	Privacy-supplement SSD	SSD P.02		De applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.
946	Informatieverstrekking aan betrokkene met applicaties	Privacy-supplement SSD	SSD P.03		Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, geïnformeerd betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens.
947	Toegang op taakniveau met applicaties	Privacy-supplement SSD	SSD P.04		Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
948	Logging met applicaties	Privacy-supplement SSD	SSD P.05		De applicatie behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.
949	Dataminimalisatie binnen applicaties	Privacy-supplement SSD	SSD P.06		De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.
950	Generalisatie binnen applicaties	Privacy-supplement SSD	SSD P.07		De applicatie behoort, indien de functionele eisen aan de applicatie van de opdrachtgever dit toelaten, gegeneraliseerde gegevens te gebruiken.
951	Scheiden binnen applicaties	Privacy-supplement SSD	SSD P.08		Iedere applicatie kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst.
952	Verbergen binnen applicaties	Privacy-supplement SSD	SSD P.09		Een applicatie, en iedere Functie binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de applicatie en verwerking binnen een taak alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de middleware. Het implementatiemodel is getoetst.
953	DataminimalisatieDataminimalisatie door serverplatformen	Privacy-supplement Serverplatform	SVP P.01		De organisatie behoort een proces te hebben ingericht en afspraken te hanteren, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en verwijdering van persoonsgegevens mogelijk is.
954	Scheiden door serverplatformen	Privacy-supplement Serverplatform	SVP P.02		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.
955	Verbergen door serverplatformen	Privacy-supplement Serverplatform	SVP P.03		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.
956	Scheiden binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.01		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij de scheiding van verwerkingen het uitgangspunt is.
957	Verbergen binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.02		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij het verbergen van verwerkingen het uitgangspunt is.

958	Logging binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.03		De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.
959	Uitvallen van een dienst	Privacy-supplement Huisvesting-IV	HVI P.01		De organisatie heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.
960	Het stelsel van toegangsbeheer	Privacy-supplement Toegangsbeveiliging	TBV P.01		Het doel van de verwerking van persoonsgegevens en van de toegang zijn welbepaald, gerechtvaardigd en uitdrukkelijk omschreven, waarbij de toegang naar keuze rol gebaseerd en waar nodig taak gebaseerd wordt verstrekt. Aanvullend vindt logging en monitoringplaats.
961	Doelbinding op rolniveau	Privacy-supplement Toegangsbeveiliging	TBV P.02		De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.
962	Toegang op taakniveau	Privacy-supplement Toegangsbeveiliging	TBV P.03		Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.
963	Logging en monitoring uitgeven toegangsrechten	Privacy-supplement Toegangsbeveiliging	TBV P.04		De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.
964	Toegang tot fysieke omgevingen	Privacy-supplement Toegangsbeveiliging	TBV P.05		De organisatie behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op passende wijze ingericht te hebben, zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd.
965	Toegang buiten beveiligde omgevingen	Privacy-supplement Toegangsbeveiliging	TBV P.06		Er is een procedure ingericht voor het transporteren van persoonsgegevens buiten een beschermde omgeving, waarbij door versleuteling de kans op een datalek is verkleind en door minimalisatie de omvang van een datalek wordt beperkt.
966	Toegang in het buitenland	Privacy-supplement Toegangsbeveiliging	TBV P.07		De organisatie hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.
967	Beëindiging (verwerkers)overeenkomst	Privacy-supplement Toegangsbeveiliging	TBV P.08		De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd.