



Bijlage 6

Beveiliging

IWR2024|Vaste Telefonie

ICT Werkomgeving Rijk

Status: versie 1.0
Referentie: IUC 202303067

Inhoud

1	Inleiding	3
2	Eisen aan Personeel van Opdrachtnemer	4
2.1	Personeel.....	4
2.2	Toegang tot Locatie.....	4
3	Beveiliging bij Diensten	6
3.1	Beveiliging Diensten algemeen	6
3.2	Securitytesten	7
3.3	Afhandeling van Incidenten en Onderhoud op Locatie.....	7
3.4	Penetratietest.....	7
3.5	Remote beheer	7
3.6	Toegang tot het online portaal.....	8
3.7	Logging van gegevens	8
3.8	Beveiligingsinstellingen van Diensten	10
3.9	Infrastructurele beveiligingseisen	10
3.10	Toegangscontrole	11
3.11	Onderhoud en beëindigen Diensten	12
4	Uitvoeringsaspecten	13
4.1	Beveiligingsincidenten.....	13
4.2	Wijziging in beveiliging.....	13
4.3	Controle en audits	13
4.4	Organiseren van informatiebeveiliging.....	13
5	Vertaalslag BIO en AVG naar concrete eisen conform ICO Wizzard	15
6	Bronvermeldingen	23

1 Inleiding

Op het gebied van informatiebeveiliging van de informatievoorziening dienen de Opdrachtgever en de Deelnemers zich te houden aan vastgestelde regels voor de Rijksoverheid. De regels over informatiebeveiliging voor de Rijksoverheid zijn onder meer terug te vinden in:

- Besluit BVA-stelsel Rijksdienst 2021¹;

1 ¹ Zie hoofdstuk 6 Vertaalslag BIO en AVG naar concrete eisen conform ICO Wizzard

De onderstaande eisen zijn van toepassing en zijn een concretisering vanuit de BIO en AVG. Deze zijn opgesteld middels de ICO Wizzard: Communicatievoorzieningen en BIO t/m BBN2, op datum 2 juni 2023.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	BIO 2019: 13.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.	Onveilig versturen van gevoelige informatie.
Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1.		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.

Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
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.	BSI 200-2 2017: 4.2		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Organisaties behoren hun netwerken te beveiligen met richtlijnen voor ontwerp, implementatie en beheer.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	BIO 2019: 9.4.2.	SAML (authenticatie)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van andermans identiteit.
Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onterecht hebben van rechten.
Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onterecht hebben van rechten.
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie, betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	BIO 2019: 13.2.4.		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van andermans identiteit.

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.	BIO 2019: 13.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.	Aanvallen via systemen die niet in eigen beheer zijn.
Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Aanvallen via systemen die niet in eigen beheer zijn.
Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Incidenten worden niet tijdig opgepakt.
Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Onveilig versturen van gevoelige informatie.
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.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Netwerkdiensten raken overbelast.
Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).	BIO 2019: 13.1.3.		Overleg bewijsstukken en/of Verklaring.	Misbruik van speciale bevoegdheden.

Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	BIO 2019: 13.2.3.	* STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-mailphishing/-spoofing)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onveilig versturen van gevoelige informatie.
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.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de pastoe-of-leg-uit lijst, gebruik gemaakt van de actuele versie van Digikoppeling.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontleen.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
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.	BIO 2019: 14.1.2.		Overleg bewijsstukken en/of Verklaring.	Onveilig versturen van gevoelige informatie.

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.	ISO 27033-4 2014: 6		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie die over een VPN wordt getransporteerd, is ingeperkt tot de organisatie die de VPN gebruikt.	ISO 27033-5 2013: 6.1	TLS	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruiken van zwakheden in netwerkbeveiliging.
Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.	BIO 2019: 18.1.5, ISO 27033-1 2015: 7.2.2.2.	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekenen de domeinnaam) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de pas-toe-of-leg-uit lijst van het forum standaardisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.	CIP-netwerk	* WPA2 Enterprise (Beveiligde WiFi-netwerken)	Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Authenticatie van netwerk-nodes behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Logbestanden van informatiebeveiligingsgebeurtenissen in netwerken, behoren te worden gemaakt en bewaard en regelmatig te worden beoordeeld (op de ernst van de risico's).	BIO 2019: 12.4.1.		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
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.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatie-systemen, zodat aanvallen kunnen worden gedetecteerd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken	Incidenten worden niet

gerapporteerd aan het verantwoordelijk management.			en/of Verklaring.	tijdig opgepakt.
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.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Richtlijnen voor de naleving van het netwerkbeveiligingsbeleid behoren periodiek getoetst en geëvalueerd te worden.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De naleving van een, conform het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliance-toetsen).	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De robuustheid van de beveiligingsmaatregelen en de naleving van het netwerkbeveiligingsbeleid behoren periodiek getest en aangetoond te worden.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
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.	ISO 27033-1 2015: 8.5		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	BIO 2019: 6.1.1.		Overleg bewijsstukken en/of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.

- Baseline Informatiebeveiliging Overheid (BIO)¹;
- Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007)¹;
- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI 2013)¹;
- de Algemene Verordening Gegevensbescherming (AVG)¹;

De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoorde lijkheid voor informatiebev eiliging niet.
De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoorde lijkheid voor informatiebev eiliging niet.
Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoorde lijkheid voor informatiebev eiliging niet.
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.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden'		Overleg bewijsstukken en/of verklaring	
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.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'		Overleg bewijsstukken en/of verklaring	
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.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a		Overleg bewijsstukken en/of verklaring	

- het Algemeen Rijksambtenarenreglement (Wnra)¹.

De Prestatie die Opdrachtnemer levert is integraal onderdeel van de informatievoorziening waar de rijksdienst gebruik van maakt. Dit betekent dat de Diensten van Opdrachtnemer niet strijdig mogen zijn met het beveiligingsbeleid van Opdrachtgever en/of Deelnemers.

De regels op het gebied van informatiebeveiliging die gelden voor de Rijksoverheid zijn gebaseerd op de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 normen. Opdrachtnemer dient haar beveiligingsbeleid gedurende de gehele looptijd van de opdracht steeds te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002 of opvolgers hiervan, of een gelijkwaardige normering.

In deze Bijlage zijn de beveiligingsaspecten die op de Overeenkomst van toepassing zijn opgenomen². Deze beveiligingsaspecten zijn onder te verdelen in:

- beveiligingseisen die gesteld worden aan Personeel dat door de Opdrachtnemer wordt ingezet voor het uitvoeren van alle voorkomende werkzaamheden zoals deze zijn onderkend;
- beveiligingseisen die gesteld worden aan de (levering van) de Diensten;
- beveiligingseisen rondom de uitvoering van de Diensten.

In het Dossier afspraken en procedures (DAP) tussen de Opdrachtnemer en de Deelnemer worden alle specifieke beveiligingsafspraken tussen de Opdrachtnemer en de Deelnemer vastgelegd.

Wet- en regelgeving is niet statisch. Opdrachtnemer zal zich steeds conformeren aan de actuele wet- en regelgeving. Uitgangspunt hierbij is dat de scope en reikwijdte van eventuele opvolgers van bestaande wet- en regelgeving niet wezenlijk wijzigen.

² Zie bijlage 2 'Specificatie van de Prestatie' Eisen 13.1

2 Eisen aan Personeel van Opdrachtnemer

2.1 Personeel

De Opdrachtnemer zet Personeel in voor het uitvoeren van alle voorkomende werkzaamheden zoals deze zijn onderkend. Onder Personeel van de Opdrachtnemer wordt verstaan medewerkers van de Opdrachtnemer die worden ingezet. Een niet uitputtende opsomming van werkzaamheden die te onderkennen zijn, is:

- werkzaamheden door personen die deel uitmaken van het accountteam;
- werkzaamheden door personen die betrokken zijn bij de Installatie;
- werkzaamheden door personen die betrokken zijn bij de uitvoering van de Diensten;
- werkzaamheden door personen die de incidentafhandeling uitvoeren.

Op verzoek van de Deelnemer dient Personeel van de Opdrachtnemer een VOG te overleggen die niet ouder is dan twaalf maanden. De kosten voor dit document zijn voor rekening van de Opdrachtnemer.

De Deelnemer kan eisen dat Personeel van of namens de Opdrachtnemer een geheimhoudingsverklaring ondertekent. De Deelnemer kan aanvullende screening eisen voor het Personeel dat door de Opdrachtnemer wordt ingezet. Indien de Deelnemer aanvullende screening of aanvullende geheimhouding eist, dienen bijbehorende voorwaarden en condities tussen de Deelnemer en de Opdrachtnemer vastgelegd te worden in de beveiligingsparagraaf van het Dossier afspraken en procedures (DAP). De kosten voor deze aanvullende screening komen voor rekening van de Deelnemer.

Personeel van Opdrachtnemer dat niet aan de gestelde beveiligingsvoorwaarden voldoet kan in beginsel niet door Opdrachtnemer worden ingezet. Hier kan alleen van worden afgeweken wanneer Opdrachtgever en/of Deelnemer hiervoor aan de Opdrachtnemer een tijdelijke ontheffing verleend.

Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het definiëren, vastleggen en uitvoeren van taken, bevoegdheden en verantwoordelijkheden met betrekking tot informatiebeveiliging voor de Prestatie en dient naar het Personeel van de Opdrachtnemer te communiceren dat:

1. deze ten uitvoer moeten worden gebracht;
2. deze van kracht blijven na beëindiging of wijziging van het dienstverband.

2.2 Toegang tot Locatie

Bij het betreden van een Locatie dient een medewerker van de Opdrachtnemer zich altijd te kunnen legitimeren met een wettelijk geldig legitimatiebewijs. Op de website van de Rijksoverheid is op de pagina identificatieplicht opgenomen welke

identiteitsbewijzen voldoen³. Personeel van de Opdrachtnemer zal handelen conform de op de Locatie geldende huisregels, wettelijke bepalingen en aanwijzingen van de Deelnemer.

2 ³ Zie hoofdstuk 5 Vertaalslag BIO en AVG naar concrete eisen conform ICO Wizzard

De onderstaande eisen zijn van toepassing en zijn een concretisering vanuit de BIO en AVG. Deze zijn opgesteld middels de ICO Wizzard: Communicatievoorzieningen en BIO t/m BBN2, op datum 2 juni 2023.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	BIO 2019: 13.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.	Onveilig versturen van gevoelige informatie.
Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1.		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.

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.	BSI 200-2 2017: 4.2		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Organisaties behoren hun netwerken te beveiligen met richtlijnen voor ontwerp, implementatie en beheer.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	BIO 2019: 9.4.2.	SAML (authenticatie)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van andermans identiteit.
Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onterecht hebben van rechten.
Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onterecht hebben van rechten.
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie, betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	BIO 2019: 13.2.4.		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van andermans identiteit.
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.	BIO 2019: 13.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.	Aanvallen via systemen die niet in eigen beheer zijn.

Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Aanvallen via systemen die niet in eigen beheer zijn.
Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Incidenten worden niet tijdig opgepakt.
Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Onveilig versturen van gevoelige informatie.
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.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Netwerkdiensten raken overbelast.
Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).	BIO 2019: 13.1.3.		Overleg bewijsstukken en/of Verklaring.	Misbruik van speciale bevoegdheden.
Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	BIO 2019: 13.2.3.	* STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-mailphishing/-spoofing)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onveilig versturen van gevoelige informatie.
Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen phishing en af luisteren op pas-toe-of-leg-uit lijst van het forum standaardisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de pas-toe-of-leg-uit lijst, gebruik gemaakt van de actuele versie van Digikoppeling.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Maak gebruik van PKI-overheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
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.	BIO 2019: 14.1.2.		Overleg bewijsstukken en/of Verklaring.	Onveilig versturen van gevoelige informatie.
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	ISO 27033-4 2014: 6		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

beveiligingsbeleid toegestaan netwerkverkeer wordt doorgelaten.				
Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie die over een VPN wordt getransporteerd, is ingeperkt tot de organisatie die de VPN gebruikt.	ISO 27033-5 2013: 6.1	TLS	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruiken van zwakheden in netwerkbeveiliging.
Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.	BIO 2019: 18.1.5, ISO 27033-1 2015: 7.2.2.2.	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekenen de domeinnaam) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de pas-toe-of-leg-uit lijst van het forum standaardisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.	CIP-netwerk	* WPA2 Enterprise (Beveiligde WiFi-netwerken)	Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Authenticatie van netwerk-nodes behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Logbestanden van informatiebeveiligingsgebeurtenissen in netwerken, behoren te worden gemaakt en bewaard en regelmatig te worden beoordeeld (op de ernst van de risico's).	BIO 2019: 12.4.1.		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
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.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatie-systemen, zodat aanvallen kunnen worden gedetecteerd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.

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.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Richtlijnen voor de naleving van het netwerkbeveiligingsbeleid behoren periodiek getoetst en geëvalueerd te worden.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De naleving van een, conform het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliance-toetsen).	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De robuustheid van de beveiligingsmaatregelen en de naleving van het netwerkbeveiligingsbeleid behoren periodiek getest en aangetoond te worden.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
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.	ISO 27033-1 2015: 8.5		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	BIO 2019: 6.1.1.		Overleg bewijsstukken en/of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.
De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.

De Deelnemers kunnen aanvullend eisen dat bij het betreden van de Locatie legitimatie plaatsvindt in combinatie met een kopie van de VOG van desbetreffende medewerkers van de Opdrachtnemer, alsmede een kopie van de door die persoon ondertekende geheimhoudingsverklaring. De Deelnemers zullen dit vooraf bekendmaken en vastleggen in het Dossier afspraken en procedures (DAP) tussen de Deelnemer en de Opdrachtnemer.

De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoorde lijkheid voor informatiebeveiliging niet.
Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoorde lijkheid voor informatiebeveiliging niet.
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.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden'		Overleg bewijsstukken en/of verklaring	
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.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'		Overleg bewijsstukken en/of verklaring	
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.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a		Overleg bewijsstukken en/of verklaring	

Indien de Deelnemer van mening is dat medewerkers die door de Opdrachtnemer ingezet worden op Locatie begeleid dienen te worden, zal de Deelnemer zorgdragen voor deze begeleiding.

3 Beveiliging bij Diensten

Beveiliging bij Diensten omvat de volgende aandachtsgebieden:

- beveiliging Diensten en Programmatuur algemeen;
- securitytesten zoals een penetratietest;
- toegang tot het centraal beheerplatform/online portaal;
- remote beheer;
- logging van gegevens;
- authenticatie;
- beveiligingsinstellingen Dienst;
- infrastructurele beveiligingseisen;
- onderhoud en innemen Diensten;
- beveiliging van transport.

In te zetten beveiligingsmaatregelen worden steeds in samenspraak met de Deelnemers vastgesteld.

3.1 Beveiliging Diensten algemeen

De Opdrachtnemer is verantwoordelijk voor de adequate beveiliging van de Diensten. Onder adequate beveiliging is onder andere inbegrepen: het kunnen aanmaken en verwijderen van accounts, een autorisatiemodel voor deze accounts, het gebruik van geëncrypte wachtwoorden en indien van toepassing maatregelen tegen malware, mogelijkheden voor back-ups en mogelijkheden voor logging, het toepassen van versleutelde protocollen en bescherming bij uitwisseling van elektronische berichten.

Wijzigingen welke de beveiliging kunnen aantasten worden voorafgaand met de Deelnemer besproken, waarbij de risico's worden benoemd en eventuele maatregelen worden geadviseerd. Alle beveiligingsrisico's worden door de Opdrachtnemer direct bij constatering kenbaar gemaakt bij de Deelnemer/System integrator, ook als het de instellingen of specifieke configuratie van een Deelnemer betreft. Tevens doet Opdrachtnemer voorstellen om de beveiliging te verbeteren.

Indien Opdrachtnemer voor het leveren van een Dienst gebruik maakt van een Onderaannemer, dan gelden voor de Onderaannemer dezelfde beveiligingseisen als voor hemzelf.

In alle gevallen blijft Opdrachtnemer verantwoordelijk voor borging bij de Onderaannemer van de met de Deelnemer gemaakte afspraken.

Indien Opdrachtnemer contractueel of wettelijk verplicht is tot de inzet van cryptografie ter bescherming van informatie betrokken bij de Prestatie, dient Opdrachtnemer voor het gebruik van deze cryptografische beheersmaatregelen over beleid en operationeel geborgde processen te beschikken, inclusief het gebruik, de bescherming en de levensduur van de daarbij behorende cryptografische sleutels, tijdens hun gehele levenscyclus.

3.2 Securitytesten

Het online portaal van de Opdrachtnemer wordt jaarlijks door Opdrachtnemer getest op kwetsbaarheden door middel van securitytesten (bijvoorbeeld whitebox penetratietesten) en de uitkomsten van deze securitytesten worden aan CCM ter beschikking gesteld.

Een Deelnemer kan ook voor eigen rekening een partij selecteren voor uitvoering van deze securitytesten. Deze testen kunnen onder andere bestaan uit:

- beoordeling van de opzet, bestaan en werking van informatiebeveiligingsmaatregelen;
- vormen van een oordeel over de betrouwbaarheid (beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid) door middel van een security assessment.

De Opdrachtnemer dient de hiervoor vereiste medewerking te verlenen en de bevindingen op te volgen indien deze zodanig zijn dat dit leidt tot onvoldoende beveiligde (delen van het) online portaal. Bevindingen die door Deelnemer gewenst worden, maar boven het overeengekomen beveiligingsniveau liggen komen voor rekening van de Deelnemer.

3.3 Afhandeling van Incidenten en Onderhoud op Locatie

Uit beveiligingsoverwegingen kan de Deelnemer eisen dat afhandeling van Incidenten en Onderhoud op hardware met een datadrager op de Locatie van een Deelnemer plaatsvindt. Indien de Deelnemer Onderhoud op Locatie eist, dient de Deelnemer de Opdrachtnemer hierin adequaat te faciliteren.

3.4 Penetratietest

Een Deelnemer kan voor eigen rekening een partij selecteren voor uitvoering van een penetratietest (PENtest) op het beheerplatform en online portaal van de Opdrachtnemer. Deze test bestaat onder andere uit:

- beoordeling van de opzet, bestaan en werking;
- vormen van een oordeel over de betrouwbaarheid (beschikbaarheid, vertrouwelijkheid, integriteit en controleerbaarheid) door middel van een security assessment.

De Opdrachtnemer dient de hiervoor vereiste medewerking te verlenen en de bevindingen op te volgen indien deze zodanig zijn dat dit leidt tot onvoldoende beveiligde (delen van de) Webshop en online portaal. Bevindingen die door Deelnemer gewenst worden maar boven het niveau van BBN2 liggen, zullen voor rekening van de Deelnemer komen.

3.5 Remote beheer

Onder remote beheer wordt verstaan het verrichten van handelingen ten behoeve van het (technisch) beheer dat plaatsvindt vanuit een locatie die gelegen is buiten de infrastructuur van de Deelnemer. Uitgangspunt is dat het remote beheer niet wordt toegestaan, tenzij de Deelnemer hiervoor schriftelijk toestemming heeft gegeven. Indien de Deelnemer remote beheer toestaat, gaat Opdrachtnemer akkoord met de hieronder genoemde en de eventueel aanvullende voorwaarden die door de Deelnemer kunnen worden gesteld.

Voor remote beheer geldt dat dit door de Deelnemer uitschakelbaar is. Remote beheer is uitsluitend toegestaan via een beveiligde verbinding, waarbij de wachtwoorden eveneens beveiligd zijn tijdens het transport. De toegang kan zowel webbased als via een speciale voorziening zijn. Hierbij geldt o.a.:

- encryptie: AES 256 of beter;
- hash algoritme: SHA2 (ISO/IEC 10118- 3:2016) of beter;
- beveiligingscertificaten: X.509 versie 3 of beter;
- beveiliging van webverkeer: HTTPS versie 1.2 of beter;
- beveiliging van verbindingen: TLS 1.2, 1.3 of de logische opvolger.

Tevens geldt dat het instelbaar sterk beheerderwachtwoord (voor zowel hard- als software) tenminste acht karakters moet zijn, bestaande uit letters, cijfer(s) en speciale teken(s).

Gezien het specifieke karakter van deze toepassing en de specifieke afspraken rondom de technische realisatie van remote support per Deelnemer kunnen gelden, dient de Deelnemer hier met de Opdrachtnemer aanvullende afspraken over te maken en deze vast te leggen in een Dossier Afspraken en Procedure (DAP).

3.6 Toegang tot het online portaal

Het online portaal is web-based, zodat met een standaard browser zonder specifieke aanpassingen op iedere willekeurige werkplek bij de Deelnemer het online portaal benaderd kan worden. De toegang tot het online portaal dient op professionele wijze door de Opdrachtnemer beveiligd te worden. Deze beveiliging voldoet aan de moderne en gangbare normen en standaarden. Het online portaal is uitsluitend toegankelijk voor geautoriseerde gebruikers.

3.7 Logging van gegevens

Voor het loggen van gegevens gelden de volgende uitgangspunten:

- de volgende gebeurtenissen worden in ieder geval opgenomen in de logging:
 - gebruik van technische beheerfuncties, zoals het wijzigen van configuratie of instelling; uitvoeren van een systeemcommando, starten en stoppen, uitvoering van een back-up of restore;
 - gebruik van functioneel beheerfuncties, zoals het wijzigen van configuratie en instellingen, release van nieuwe functionaliteit, ingrepen in gegevenssets (waaronder databases);
 - handelingen van beveiligingsbeheer, zoals het opvoeren en afvoeren gebruikers, toekennen en intrekken van rechten, wachtwoord reset, uitgifte en intrekken van cryptosleutels;
 - beveiligingsincidenten (zoals de aanwezigheid van malware, testen op zwakheden, foutieve inlogpogingen, overschrijding van autorisatiebevoegdheden, geweigerde pogingen om toegang te krijgen, het gebruik van niet operationele systeemservices, het starten en stoppen van security services);

- verstoringen in het productieproces (zoals het vollopen van queues, systeemfouten, afbreken tijdens executie van Programmatuur, het niet beschikbaar zijn van aangeroepen programmaonderdelen of systemen);
- handelingen van gebruikers en systeembeheerders, zoals systeemtoegang, gebruik van online transacties en toegang tot bestanden;
- iedere regel in de logging bevat ten minste de volgende informatie:
 - de gebeurtenis (handeling die leidde tot loggen ervan);
 - tot een natuurlijk persoon herleidbaar ID die de handeling heeft uitgevoerd;
 - indien mogelijk: ID van het werkstation/Locatie van waaruit handeling plaatsvond;
 - object waarop de handeling werd uitgevoerd;
 - het resultaat van de handeling;
 - de datum en het tijdstip van de gebeurtenis;
- in een logregel worden in geen geval gevoelige gegevens opgenomen. Dit betreft onder meer gegevens waarmee de beveiliging doorbroken kan worden (zoals wachtwoorden en inbelnummers);
- apparatuur die logging informatie verstuurt en ontvangt dient een gesynchroniseerde klok te hebben met een maximale afwijking van 500 milliseconde over een periode van twaalf maanden;
- logbestanden worden centraal opgeslagen op het beheerplatform. Op verzoek van Deelnemer kunnen de logging-gegevens naar een nader aangegeven (vanuit het beheerplatform gezien externe) Locatie worden weggeschreven;
- logbestanden kunnen voor een periode van minimaal drie maanden worden ingezien door uitsluitend geautoriseerd Personeel van de Opdrachtnemer. Gegevens van (vermoedelijke) informatiebeveiligingsincidenten dienen voor een periode tot vijf jaar beschikbaar te zijn;
- instellingen voor logging kunnen alleen door geautoriseerd Personeel van de Opdrachtnemer worden gewijzigd. Elke wijziging wordt gelogd;
- de instellingen van logmechanismen worden zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Indien de instellingen aangepast moeten worden zal daarbij altijd het vier ogen principe toegepast worden;
- het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in een nieuw aangelegd logbestand;
- logbestanden kunnen in principe niet worden gewijzigd. Indien noodzakelijk, dan alleen door Opdrachtgever geautoriseerd Personeel, onder strikte voorwaarden (onder andere vier ogen principe) en uitsluitend wanneer elke wijziging wordt gelogd in een nieuw logbestand;
- het vollopen van het opslagmedium voor de logbestanden boven een bepaalde grens wordt gelogd en leidt tot automatische alarmering van de beheerorganisatie bij Opdrachtnemer. Dit geldt ook als het bewaren van loggegevens niet (meer) mogelijk is (bijv. een logserver die niet bereikbaar is). Opdrachtnemer voorziet in voldoende capaciteit van het opslagmedium;
- Opdrachtnemer dient minimaal jaarlijks zowel de fysieke als logische toegangsrechten tot informatie verwerkende faciliteiten van het Personeel van de Opdrachtnemer te beoordelen en te actualiseren via een operationeel geborgd en formeel proces;
- Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor het controleren van het gebruik van systeemhulpmiddelen, die in staat

zijn om beheersmaatregelen te omzeilen voor informatiesystemen betrokken bij de Prestatie.

3.8 Beveiligingsinstellingen van Diensten

De mogelijke beveiligingsinstellingen van de Dienst dient vóór oplevering tussen Opdrachtnemer en Deelnemer te worden besproken en te worden vastgelegd. De afspraken over beveiligingsinstellingen van de Dienst betreffen onder andere:

- hardening: het uitschakelen en/ of blokkeren van niet gebruikte netwerkpoothen en protocollen;
- toegangsbeheer gebruik: de afspraken voor de wachtwoorden, gebruikersaccounts en de *Simple Network Management Protocol* (SNMP) community names;
- toegangsbeheer fysieke componenten: de afspraken rond het beveiligen van componenten van de gebruikte hardware, waaronder de datadrager en ongebruikte functionaliteiten. Voorkomen van ongeoorloofde toegang tot het component, waaronder het ongeoorloofd kunnen verwijderen of gebruiken;
- voorkomen van ongeoorloofde toegang tot het component, waaronder het ongeoorloofd kunnen verwijderen of gebruiken;
- toegangsbeheer interfaces: interfaces (zoals, maar niet uitsluitend, (draadloze) netwerkinterfaces en USB-interfaces) dienen geblokkeerd of verwijderd of uit te schakelen te zijn;
- wijzigingsbeheer: afspraken, waaronder autorisatie, betreffende het uitvoeren van software/firmware updates en upgrades op gebruikte hardware;
- het uitvoeren van firmware upgrades is alleen mogelijk na autorisatie.

3.9 Infrastructurele beveiligingseisen

Voor alle Diensten geldt dat de toegang tot de infrastructuur afgesloten moet zijn voor onbevoegden, tenzij dit niet mogelijk is en als zodanig is overeengekomen met de Deelnemer. Onder toegang wordt zowel fysieke als logische toegang verstaan. Ongeautoriseerde toegang dient gedetecteerd te worden, waarna passende maatregelen worden getroffen. De toegangsmethoden tot de Diensten en de te nemen maatregelen bij ongeautoriseerde toegang, dienen in de beveiligingsparagraaf van het Dossier Afspraken en Procedures vastgelegd te worden.

De Opdrachtnemer dient de integriteit⁴ en vertrouwelijkheid⁵ van het over zijn netwerk getransporteerde gesprek/verkeer van de Deelnemer te waarborgen.

⁴ Integriteit: De inhoud van een gesprek/verkeersstroom kan tijdens het transport niet worden gewijzigd.

⁵ Vertrouwelijkheid: Onbevoegden kunnen de inhoud van een gesprek/verkeersstroom niet afluisteren, aftappen, kopiëren, etc..

De Opdrachtnemer dient voor alle Diensten professionele maatregelen te nemen om de mogelijkheid van af luisteren van netwerkverbindingen en/of wijzigen van datastromen te verhinderen. Hiertoe worden binnen de branche gebruikelijke maatregelen toegepast. De Opdrachtnemer dient op aanvraag van de Deelnemer inzichtelijk te maken welke maatregelen geïmplementeerd zijn en hoe deze gecontroleerd worden.

De Opdrachtnemer dient de Aansluitingen, verbindingen, informatiesystemen, apparatuur en omgevingen betrokken bij de Prestatie zodanig in te richten, dat er geen voor de beveiliging nadelige beïnvloeding tussen Deelnemers en (onbekende) derden, Deelnemers onderling en tussen Deelnemers en overige klanten van de Opdrachtnemer mogelijk is.

Opdrachtnemer dient ontwikkel-, test-, productie- en, indien besteld, educatieve omgevingen aantoonbaar gescheiden (logisch, dan wel fysiek) te hebben voor alle informatiesystemen betrokken bij de Prestatie. Scheiding houdt in dat al het noodzakelijke geregeld moet worden om interferentie en ongewenste uitwisseling van informatie tussen de omgevingen te voorkomen en dat de betrouwbaarheid van de productiesystemen gewaarborgd is. De acceptatie- en educatieve omgevingen dienen representatief te zijn voor de productieomgeving, zodanig dat de test- dan wel oefenresultaten het gedrag van de functionaliteit in de productieomgeving weerspiegelen.

Opdrachtnemer dient een aantoonbaar operationeel geborgd proces te hebben voor versleutelen van gegevens op (mobiele) apparatuur betrokken bij de Prestatie waarbij rekening wordt gehouden met de classificatie van deze gegevens en actualiteit van de veiligheid van de gebruikte versleutelingsmethoden. Opdrachtnemer hanteert de standaard NEN-ISO/IEC 11770 voor het beheer van cryptografische sleutels. Indien (mobiele) apparatuur in gebruik door Personeel van de Opdrachtnemer gegevens bevat gerelateerd aan de Prestatie die door Deelnemer en/of Opdrachtgever als vertrouwelijk is geclassificeerd, dient Opdrachtnemer deze gegevens te versleutelen middels cryptografische toepassingen, waarbij uitsluitend algoritmes en instellingen worden gebruikt met de duiding goed uit de meest actuele versie van het NCSC document Richtlijnen voor Transport Layer Security (TLS)⁶. Gegevens of Programmatuur van Deelnemer

3 ⁶ Zie hoofdstuk 5 Vertaalslag BIO en AVG naar concrete eisen conform ICO Wizzard

De onderstaande eisen zijn van toepassing en zijn een concretisering vanuit de BIO en AVG. Deze zijn opgesteld middels de ICO Wizzard: Communicatievoorzieningen en BIO t/m BBN2, op datum 2 juni 2023.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	BIO 2019: 13.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.	Onveilig versturen van gevoelige informatie.
Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1.		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
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.	BSI 200-2 2017: 4.2		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Organisaties behoren hun netwerken te beveiligen met richtlijnen voor ontwerp, implementatie en beheer.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	BIO 2019: 9.4.2.	SAML (authenticatie)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van andermans identiteit.
Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onterecht hebben van rechten.
Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onterecht hebben van rechten.
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie, betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	BIO 2019: 13.2.4.		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van andermans identiteit.
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.	BIO 2019: 13.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.	Aanvallen via systemen die niet in eigen beheer zijn.
Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Aanvallen via systemen die niet in eigen beheer zijn.

Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Incidenten worden niet tijdig opgepakt.
Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Onveilig versturen van gevoelige informatie.
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.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Netwerkdiensten raken overbelast.
Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).	BIO 2019: 13.1.3.		Overleg bewijsstukken en/of Verklaring.	Misbruik van speciale bevoegdheden.
Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	BIO 2019: 13.2.3.	* STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onveilig versturen van gevoelige informatie.

		(anti-mailphishing/-spoofing)		
Voor de beveiliging van elektronische berichten gelden de vastgestelde standaarden tegen phishing en af luisteren op pas-toe-of-leg-uit lijst van het forum standaardisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de pastoe-of-leg-uit lijst, gebruik gemaakt van de actuele versie van Digikoppeling.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontleen.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
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.	BIO 2019: 14.1.2.		Overleg bewijsstukken en/of Verklaring.	Onveilig versturen van gevoelige informatie.
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.	ISO 27033-4 2014: 6		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie die over een VPN wordt getransporteerd, is ingeperkt tot de organisatie die de VPN gebruikt.	ISO 27033-5 2013: 6.1	TLS	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruiken van zwakheden in netwerkbeveiliging.
Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.	BIO 2019: 18.1.5, ISO 27033-1 2015: 7.2.2.2.	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (onderteken de domeinnaam) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de pas-toe-of-leg-uit lijst van het forum standaardisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.	CIP-netwerk	* WPA2 Enterprise (Beveiligde WiFi-netwerken)	Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Authenticatie van netwerk-nodes behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.		Overleg bewijsstukken	Misbruiken van zwakheden in

			en/of Verklaring.	netwerkbeveiliging.
Logbestanden van informatiebeveiligingsgebeurtenissen in netwerken, behoren te worden gemaakt en bewaard en regelmatig te worden beoordeeld (op de ernst van de risico's).	BIO 2019: 12.4.1.		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
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.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatie-systemen, zodat aanvallen kunnen worden gedetecteerd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De beveiligingsarchitectuur behoort de samenhang van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

principes en de geldende normen en standaarden.				
Richtlijnen voor de naleving van het netwerkbeveiligingsbeleid behoren periodiek getoetst en geëvalueerd te worden.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De naleving van een, conform het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliance-toetsen).	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De robuustheid van de beveiligingsmaatregelen en de naleving van het netwerkbeveiligingsbeleid behoren periodiek getest en aangetoond te worden.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
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.	ISO 27033-1 2015: 8.5		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	BIO 2019: 6.1.1.		Overleg bewijsstukken en/of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.
De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.

en/of Opdrachtgever, of door deze gegenereerde metadata, welke zich bevinden op informatiesystemen van Opdrachtnemer, is en blijft ten alle tijden eigendom van de Deelnemer en/of Opdrachtgever.

3.10 Toegangscontrole

Informatiesystemen betrokken bij de Prestatie moeten zijn ingericht volgens een Professioneel autorisatiemodel. Accounts op informatiesystemen betrokken bij de Prestatie beschikken uitsluitend over toegangsrechten gekoppeld aan rollen toegekend via het vigerende Professionele autorisatieproces. Opdrachtnemer dient

De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.
Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.
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.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden'		Overleg bewijsstukken en/of verklaring	
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.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'		Overleg bewijsstukken en/of verklaring	
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.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a		Overleg bewijsstukken en/of verklaring	

aantoonbaar operationeel geborgde Professionele beleidsregels, procedures en beheersmaatregelen te hebben ter bescherming van het informatietransport betrokken bij de Prestatie, dat via alle soorten communicatiefaciliteiten verloopt.

Opdrachtnemer dient beleid te hebben voor functiescheiding (mits redelijkerwijs mogelijk) bij het beleggen van uitvoerende, controlerende, en beheertaken betrokken bij de Prestatie, en dient dit aantoonbaar operationeel geborgd te hebben in processen. Opdrachtnemer dient te beschikken over een operationeel geborgd (project)beheerproces voor de Prestatie waarin informatiebeveiliging aantoonbaar geïntegreerd is.

3.11 Onderhoud en beëindigen Diensten

De Deelnemer kan eisen dat onderhoud van een Dienst, waarop zich gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer bevinden, op de Locatie van de Deelnemer plaatsvindt. De Deelnemer zal de Opdrachtnemer in dit geval adequaat faciliteren.

In het geval van beëindiging dient Opdrachtnemer (delen van) een Dienst, waarop zich gegevens en Programmatuur van de Deelnemer bevinden, nooit zonder voorafgaande toestemming van de Deelnemer en met inachtneming van de optioneel door de Deelnemer gestelde eisen buiten de Locatie te brengen. De Deelnemer kan hierbij aanvullende eisen stellen. De Opdrachtnemer dient een proces-verbaal op te maken.

4 Uitvoeringsaspecten

4.1 Beveiligingsincidenten

Een beveiligingsincident is een gebeurtenis die mogelijk een nadelige invloed heeft op de vertrouwelijkheid, integriteit en/of beschikbaarheid van (bedrijfs-)informatie of (bedrijfs-)informatie verwerkende systemen en derhalve een bedreiging vormt voor de bedrijfsvoering. Iedere activiteit dat het beveiligingsbeleid schendt, wordt beschouwd als een beveiligingsincident.

Opdrachtnemer dient over een operationeel geborgd proces te beschikken voor de registratie, rapportage en afhandeling van beveiligingsincidenten die aansluit op het incidentmanagementproces van Opdrachtgever en/of de Deelnemers. Periodiek dient over deze beveiligingsincidenten gerapporteerd te worden richting Opdrachtgever. Beveiligingsincidenten dienen onverwijld aan de betreffende functionaris(sen) van de Deelnemer(s) te worden gemeld.

4.2 Wijziging in beveiliging

Wijzigingen welke de beveiliging kunnen aantasten worden voorafgaand met de Deelnemer besproken, waarbij de risico's worden benoemd en eventuele maatregelen worden geadviseerd.

4.3 Controle en audits

In Bijlage 09 – Kwaliteitsborging en auditing zijn instrumenten opgenomen waarmee de Opdrachtgever en de Deelnemers nader inzicht kunnen krijgen in de kwaliteit van de Prestatie van de Opdrachtnemer. Middels deze instrumenten uit Bijlage 09 – Kwaliteitsborging en auditing hebben de Opdrachtgever en de Deelnemers de mogelijkheid nader inzicht te verkrijgen in de beveiligingsmaatregelen die de Opdrachtnemer heeft geïmplementeerd.

Aanvullend op de instrumenten uit Bijlage 09 – Kwaliteitsborging en auditing dient de Opdrachtnemer op verzoek van de Deelnemers periodiek een assurance rapportage betreffende opzet, bestaan en werking van de kwaliteit van de geleverde Diensten op te leveren. Beveiliging is een vast onderwerp in deze rapportage. Deze rapportage is op aanvraag beschikbaar voor alle Deelnemers.

4.4 Organiseren van informatiebeveiliging

Opdrachtnemer dient haar beveiligingsbeleid te baseren op de meest actuele versies van de NEN-ISO/IEC 27001 en de NEN-ISO/IEC 27002. De in de Overeenkomst opgenomen proces- en systeemvereisten van Opdrachtgever maken middels een toepasselijkheidsverklaring aantoonbaar onderdeel uit van de scope van deze certificering. De Opdrachtnemer dient op aanvraag van de Deelnemer inzichtelijk te maken welke beveiligingsmaatregelen zijn geïmplementeerd en hoe deze gecontroleerd worden.

Opdrachtnemer dient voor informatiebeveiliging minimaal jaarlijks een risicoanalyse en risicoafweging conform NEN-ISO/IEC 27005 te maken en passende maatregelen te treffen. Opdrachtnemer dient aantoonbaar te beschikken

over een continuïteitsplan voor het handhaven van de Prestatie in ongunstige situaties, waarin ook de continuïteit van de informatiebeveiliging is gewaarborgd.

Opdrachtnemer dient te beschikken over een aantoonbaar operationeel geborgd proces voor het geautoriseerd vernietigen van gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer en/of Opdrachtgever, welke zich bevinden op (delen van) informatiesystemen betrokken bij de Prestatie die tijdens de looptijd van de Overeenkomst afgevoerd of vervangen worden.

Opdrachtnemer dient te beschikken over een formeel en operationeel geborgd Professioneel proces voor back-up en recovery voor van alle informatiesystemen betrokken bij de Prestatie. Het betreft alle aanwezige gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer en/of Opdrachtgever. Opdrachtnemer dient minimaal hiervan dagelijks back-ups te maken. Opdrachtnemer past bij de back-ups dezelfde beveiligingsmaatregelen toe die ook gelden voor de informatiesystemen betrokken bij de Prestatie.

Opdrachtnemer dient op verzoek van de Deelnemer een actuele registratie te kunnen overleggen van back-upactiviteiten en de fysieke en logische verblijfplaats van de media. De fysieke en logische toegang tot back-ups is zodanig geregeld dat alleen geautoriseerde personen toegang hebben.

Opdrachtnemer dient het recovery proces dat deel uitmaakt van het back-upproces van alle informatie en Programmatuur in gebruik voor de Prestatie, minimaal jaarlijks te testen en naar Opdrachtgever te communiceren over de uitkomst hiervan.

Gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer en/of Opdrachtgever wordt door Personeel van Opdrachtnemer op geen enkele wijze buiten de bij de Prestatie betrokken informatiesystemen en apparatuur gebracht, tenzij dit nodig is voor het leveren van de Prestatie en aantoonbaar is overeengekomen met de Deelnemer en/of Opdrachtgever.

Opdrachtnemer dient, in het geval dat het contract tussen beide Partijen wordt beëindigd en gegevens, Programmatuur en eventueel hierdoor gegenereerde metadata van de Deelnemer en/of Opdrachtgever zich bevinden op informatiesystemen betrokken bij de Prestatie, te assisteren bij de overdracht van deze gegevens naar een (eventuele) nieuwe Opdrachtnemer en na de overeengekomen periode te verwijderen.

5 Vertaalslag BIO en AVG naar concrete eisen conform ICO Wizzard

De onderstaande eisen zijn van toepassing en zijn een concretisering vanuit de BIO en AVG. Deze zijn opgesteld middels de [ICO Wizzard](#): Communicatievoorzieningen en BIO t/m BBN2, op datum 2 juni 2023.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	BIO 2019: 13.2.1.		Interne controle, Overleg bewijsstukken of Verklaring.	Onveilig versturen van gevoelige informatie.
Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1.		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
In het cryptografiebeleid zijn minimaal de volgende onderwerpen uitgewerkt: (a) Wanneer cryptografie ingezet wordt. (b) Wie verantwoordelijk is voor de implementatie. (c) Wie verantwoordelijk is voor het sleutelbeheer. (d) Welke normen als basis dienen voor cryptografie en de wijze waarop de normen van het Forum worden toegepast. (e) De wijze waarop het beschermingsniveau vastgesteld wordt. (f) Bij communicatie tussen organisaties wordt het beleid onderling vastgesteld.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
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.	BSI 200-2 2017: 4.2		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
Organisaties behoren hun netwerken te beveiligen met richtlijnen voor ontwerp, implementatie en beheer.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	BIO 2019: 9.4.2.	SAML (authenticatie)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van andermans identiteit.
Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onterecht hebben van rechten.
Voor het verlenen van toegang tot het netwerk aan externe leveranciers wordt vooraf een risicoafweging gemaakt. De risicoafweging bepaalt onder welke voorwaarden de leveranciers toegang krijgen. Uit een registratie blijkt hoe de rechten zijn toegekend.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onterecht hebben van rechten.
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Eisen voor vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie, betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	BIO 2019: 13.2.4.		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruik van andermans identiteit.
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.	BIO 2019: 13.1.2.		Interne controle, Overleg bewijsstukken of Verklaring.	Aanvallen via systemen die niet in eigen beheer zijn.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
Het dataverkeer dat de organisatie binnenkomt of uitgaat wordt bewaakt / geanalyseerd op kwaadaardige elementen middels detectievoorzieningen (zoals beschreven in de richtlijn voor implementatie van detectieoplossingen), zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties) of GDI, die worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Aanvallen via systemen die niet in eigen beheer zijn.
Bij ontdekte nieuwe dreigingen vanuit 13.1.2.1 worden deze, rekening houdend met de geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of de sectorale CERT, bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing).	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Incidenten worden niet tijdig opgepakt.
Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Onveilig versturen van gevoelige informatie.
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.	Direct op BIO 2019 gebaseerd		Interne controle, Overleg bewijsstukken of Verklaring.	Netwerkdiensten raken overbelast.
Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).	BIO 2019: 13.1.3.		Overleg bewijsstukken en/of Verklaring.	Misbruik van speciale bevoegdheden.
Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	BIO 2019: 13.2.3.	* STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-mailphishing/-spoofing)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Onveilig versturen van gevoelige informatie.
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.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Voor veilige berichtenuitwisseling met basisregistraties, wordt conform de pastoe-of-leg-uit lijst, gebruik gemaakt van de actuele versie van Digikoppeling.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenu.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik gemaakt van de AdES Baseline Profile standaard.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Informatie buiten de beschermde omgeving.
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.	BIO 2019: 14.1.2.		Overleg bewijsstukken en/of Verklaring.	Onveilig versturen van gevoelige informatie.
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	ISO 27033-4 2014: 6		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
beveiligingsbeleid toegestaan netwerkverkeer wordt doorgelaten.				
Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie die over een VPN wordt getransporteerd, is ingeperkt tot de organisatie die de VPN gebruikt.	ISO 27033-5 2013: 6.1	TLS	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruiken van zwakheden in netwerkbeveiliging.
Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.	BIO 2019: 18.1.5, ISO 27033-1 2015: 7.2.2.2.	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (onderteken de domeinnaam) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Cryptografische beheersmaatregelen moeten expliciet aansluiten bij de standaarden op de pas-toe-of-leg-uit lijst van het forum standaardisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.	Misbruik van cryptografische sleutels en/of gebruik van zwakke algoritmen.
Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.	CIP-netwerk	* WPA2 Enterprise (Beveiligde WiFi-netwerken)	Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Authenticatie van netwerk-nodes behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.		Overleg bewijsstukken en/of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Logbestanden van informatiebeveiligingsgebeurtenissen in netwerken, behoren te worden gemaakt en bewaard en regelmatig te worden beoordeeld (op de ernst van de risico's).	BIO 2019: 12.4.1.		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
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.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Een logregel bevat in geen geval gegevens die tot het doorbreken van de beveiliging kunnen leiden.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De informatieverwerkende omgeving wordt gemonitord door een SIEM en/of SOC middels detectie-voorzieningen, zoals het Nationaal Detectie Netwerk (alleen voor rijksoverheidsorganisaties). Deze worden ingezet op basis van een risico-inschatting, mede aan de hand van de aard van de te beschermen gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Bij ontdekte nieuwe dreigingen (aanvallen) via 12.4.1.3 worden deze binnen geldende juridische kaders verplicht gedeeld binnen de overheid, waaronder met het NCSC (alleen voor rijksoverheidsorganisaties) of via de sectorale CERT (voor andere overheidsorganisaties), middels (bij voorkeur geautomatiseerde) threat intelligence sharing mechanismen.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
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.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Misbruiken van zwakheden in netwerkbeveiliging.
Richtlijnen voor de naleving van het netwerkbeveiligingsbeleid behoren periodiek getoetst en geëvalueerd te worden.	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De naleving van een, conform het beveiligingsbeleid, veilige inrichting van netwerk(diensten), behoort periodiek gecontroleerd te worden en de resultaten behoren gerapporteerd te worden aan het verantwoordelijke management (compliance-toetsen).	CIP-netwerk		Interne controle, Overleg bewijsstukken of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De robuustheid van de beveiligingsmaatregelen en de naleving van het netwerkbeveiligingsbeleid behoren periodiek getest en aangetoond te worden.	CIP-netwerk		Overleg bewijsstukken en/of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
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.	ISO 27033-1 2015: 8.5		Overleg bewijsstukken en/of Verklaring.	Incidenten worden niet tijdig opgepakt.
Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	BIO 2019: 6.1.1.		Overleg bewijsstukken en/of Verklaring.	Gebrek aan sturing op informatiebeveiliging vanuit de directie.
De leiding van de organisatie heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.
De verantwoordelijkheden en rollen ten aanzien van informatiebeveiliging zijn gebaseerd op relevante voorschriften en wetten.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoordelijkheid voor informatiebeveiliging niet.

Eis:	Gebaseerd op:	Relevante Open standaard:	Verificatie methode(n):	Mitigeert risico:
De rol en verantwoordelijkheden van de Chief Information Security Officer (CISO) zijn in een CISO-functieprofiel vastgelegd.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoorde lijkheid voor informatiebeveiliging niet.
Er is een CISO aangesteld conform een vastgesteld CISO-functieprofiel.	Direct op BIO 2019 gebaseerd		Overleg bewijsstukken en/of Verklaring.	Lijnmanagers nemen hun verantwoorde lijkheid voor informatiebeveiliging niet.
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.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden'		Overleg bewijsstukken en/of verklaring	
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.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'		Overleg bewijsstukken en/of verklaring	
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.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a		Overleg bewijsstukken en/of verklaring	

6 Bronvermeldingen

Onderstaand zijn de links opgenomen van de documenten en onderwerpen die in deze Bijlage zijn genoemd. De opgegeven links zijn de geldige links op het moment van publiceren van de Aanbesteding.

Voor de meest actuele versie van deze documenten tijdens de uitvoering van de Overeenkomst dient contact opgenomen te worden met het Centraal Contractmanagement (CCM).

Document	Locatie
Besluit BVA-stelsel Rijksdienst 2021	<u>wetten.nl - Regeling - Besluit BVA-stelsel Rijksdienst 2021 - BWBR0044617 (overheid.nl)</u>
Baseline Informatiebeveiliging Overheid (BIO)	<u>https://www.bio-overheid.nl/category/producten/producten/</u>
Voorschrift Informatiebeveiliging Rijksdienst (VIR 2007)	<u>http://www.earonline.nl/index.php/Voorschrift Informatiebeveiliging Rijksdienst (VIR)</u>
Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI 2013)	<u>http://www.earonline.nl/index.php/Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie (VIRBI)</u>
Algemene Verordening Gegevensbescherming (AVG)	<u>https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving</u>
Wet normalisering rechtspositie ambtenaren (Wnra)	<u>https://wetten.overheid.nl/BWBR0039393/2017-05-10</u>
Identificatieplicht	<u>https://www.Rijksoverheid.nl/onderwerpen/identificatieplicht/vraag-en-antwoord/met-welke-identiteitsbewijzen-kan-ik-mij-identificeren</u>
Wet veiligheidsonderzoeken	<u>http://wetten.overheid.nl/BWBR0008277/2015-09-01</u>
Door het NBV goedgekeurde producten	<u>https://www.aivd.nl/onderwerpen/informatiebeveiliging/inhoud/beveiligingsproducten/goedgekeurde-producten</u>
Forum Standaardisatie: Pas Toe of Leg Uit	<u>'Pas toe leg uit' standaarden (verplicht) Forum Standaardisatie</u>
NCSC: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0	<u>https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls</u>