Bijlage L – Informatiebeveiligingseisen ICO Wizard **Behorend bij Aanbesteding 220016REG Basisdienstverlening Platform Duurzaam Drechtsteden**	
Inkooponderdeel	**Omschrijving**
Clouddiensten	Bevat generieke informatieveiligheidseisen voor de verschillende vormen van clouddiensten. (zoals IAAS, PAAS, en SAAS, zowel in de vorm van Public- als Private Cloud).
Digi-D applicaties	Bevat de eisen die verplicht zijn gesteld voor dienstverlening waarbij authenticatie plaatsvindt m.b.v. DigiD
Softwarepakketten	Bevat generieke IB&P eisen die gehanteerd kunnen worden bij het verwerven van standaardpakketten. Dit zijn softwarepakketten die op de markt beschikbaar zijn en beschikken over standaardfuctionaliteit die door diverse organisaties gebruikt kan worden.
Communicatievoorzieningen	Bevat eisen die te maken hebben met diensten zoals instant-messaging, sociale media, elektronische berichten (ook de inhoud), informatietransport via e-mail, telefoon, video (ook de inhoud) etc. en netwerkdiensten (zoals infrastructuur, fysiek en logisch)
Huisvesting	Bevat de eisen die gesteld moeten worden aan de fysieke bescherming van rekencentra, terreinen en gebouwen, alsmede de middelen en apparatuur t.b.v. verwerking, transport en opslag van data.
Serverplatform	Bevat de generieke eisen aan serverplatforms en het beheer daarvan. Het serverplatform omvat componenten als serverhardware, virtualisatietechnologie en besturingssystemen.

Supplement aan bovenstaande inkooponderdelen is het basispakket aan eisen, privacy toevoegingen, en Overheidsmaatregelen BIO-BBN2 meegenomen

Al deze eisen zijn toegespitst op de opdrachtnemer en schrijven zowel proces- als producteisen. Eisen die te maken hebben met louter schaalgrootte laten we voor nu buiten beschouwing.

Naam Eis	Referentie brondocument:	Referentie code norm:	BIO-O-matrix egel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)	Relevante standaard PToLU-lijst Forum Standaardisatie:
Informatiebeveiligingsbeleid	Beveiligingsrichtlijnen WEB-applicaties	B.01		De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.	Beveiligingsrichtlijnen WEB-applicaties: B.01	
Contractmanagement	Beveiligingsrichtlijnen WEB-applicaties	B.05		In een contract met een derde partij voor de uitbestede levering of beheer van een web-applicatie (als dienst) zijn de beveiligingseisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.	Beveiligingsrichtlijnen WEB-applicaties: B.05	
Toegangsvoorzieningsmiddelen	Beveiligingsrichtlijnen WEB-applicaties	U/TV.01		Het toegangsvoorzieningsbeleid formuleert, op basis van eisen en wensen van de organisatie, richtlijnen voor de organisatorische en technische inrichting (ontwerp) van de processen en middelen, waarmee de toegang en het gebruik van ICT-diensten wordt gereguleerd.	Beveiligingsrichtlijnen WEB-applicaties: U/TV.01	
Webapplicatiebeheer	Beveiligingsrichtlijnen WEB-applicaties	U/WA.02		Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.	Beveiligingsrichtlijnen WEB-applicaties: U/WA.02	

Webapplicatie-invoer	Beveiligingsrichtlijnen WEB-applicaties	U/WA.03		De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.	Beveiligingsrichtlijnen WEB-applicaties: U/WA.03	
Webapplicatie-uitvoer	Beveiligingsrichtlijnen WEB-applicaties	U/WA.04		De webapplicatie beperkt de uitvoer tot waarden die (veilig) kunnen worden verwerkt door deze te normaliseren.	Beveiligingsrichtlijnen WEB-applicaties: U/WA.04	
Betrouwbaarheid van gegevens	Beveiligingsrichtlijnen WEB-applicaties	U/WA.05		De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.	Beveiligingsrichtlijnen WEB-applicaties: U/WA.05	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam)
Webprotocollen	Beveiligingsrichtlijnen WEB-applicaties	U/PW.02		De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.	Beveiligingsrichtlijnen WEB-applicaties: U/PW.02	
Webserver	Beveiligingsrichtlijnen WEB-applicaties	U/PW.03		De webserver is ingericht volgens een configuratie-baseline.	Beveiligingsrichtlijnen WEB-applicaties: U/PW.03	
Toegang tot beheermechanismen	Beveiligingsrichtlijnen WEB-applicaties	U/PW.05		Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.	Beveiligingsrichtlijnen WEB-applicaties: U/PW.05	
Hardening van platformen	Beveiligingsrichtlijnen WEB-	U/PW.07		Voor het configureren van platformen is een hardeningrichtlijn beschikbaar.	Beveiligingsrichtlijnen WEB-applicatie	

	applicaties				s: U/PW.07	
Netwerkzonering	Beveiligingsrichtlijnen WEB-applicaties	U/NW.03		Het netwerk is gescheiden in logische en fysieke domeinen (zones), in het bijzonder is er een Demilitarized Zone (DMZ) die tussen het interne netwerk en het internet is gepositioneerd.	Beveiligingsrichtlijnen WEB-applicaties: U/NW.03	
Protectie- en detectiefunctie	Beveiligingsrichtlijnen WEB-applicaties	U/NW.04		De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.	Beveiligingsrichtlijnen WEB-applicaties: U/NW.04	
Beheer- en productieomgeving	Beveiligingsrichtlijnen WEB-applicaties	U/NW.05		Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.	Beveiligingsrichtlijnen WEB-applicaties: U/NW.05	
Hardening van netwerken	Beveiligingsrichtlijnen WEB-applicaties	U/NW.06		Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.	Beveiligingsrichtlijnen WEB-applicaties: U/NW.06	
Vulnerability-assessments	Beveiligingsrichtlijnen WEB-applicaties	C.03		Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).	Beveiligingsrichtlijnen WEB-applicaties: C.03	
Penetratietestproces	Beveiligingsrichtlijnen WEB-applicaties	C.04		Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).	Beveiligingsrichtlijnen WEB-applicaties: C.04	
Logging	Beveiligingsrichtlijnen	C.06		In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief	Beveiligingsrichtlijnen WEB-	

	WEB-applicaties			en efficiënt, effectief en beveiligd ingericht.	applicaties: C.06	
Monitoring	Beveiligingsrichtlijnen WEB-applicaties	C.07		De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.	Beveiligingsrichtlijnen WEB-applicaties: C.07	
Wijzigingenbeheer	Beveiligingsrichtlijnen WEB-applicaties	C.08		Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.	Beveiligingsrichtlijnen WEB-applicaties: C.08	
Patchmanagement	Beveiligingsrichtlijnen WEB-applicaties	C.09		Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings) patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.	Beveiligingsrichtlijnen WEB-applicaties: C.09	
Informatiebeveiligingsbeleid voor leveranciersrelaties	Thema Softwarepakketten	B.02	Ja	Met de leverancier behoren de informatiebeveiligingseisen en een periodieke actualisering daarvan te worden overeengekomen.	BIO 2019: 15.1.1.	
O-maatregel. Informatiebeveiligingsbeleid voor leveranciersrelaties	BIO 2019	15.1.1.2	Ja	Op basis van een expliciete risicoafweging worden de beheersmaatregelen met betrekking tot leverancierstoegang tot bedrijfsinformatie vastgesteld.	Direct op BIO 2019 gebaseerd	
O-maatregel. Informatiebeveiligingsbeleid voor leveranciersrelaties	BIO 2019	15.1.1.3	Ja	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk	Direct op BIO 2019 gebaseerd	

				vereiste afspraken zijn vastgesteld.		
Exit-strategie	Thema Softwarepakketten	B.03		In de overeenkomst tussen de klant en leverancier behoort een exit-strategie te zijn opgenomen, waarbij zowel een aantal bepalingen over exit zijn opgenomen, als een aantal condities die aanleiding kunnen geven tot een exit.	CIP-netwerk	
Bedrijfs- en beveiligingsfuncties	Thema Softwarepakketten	B.04		De noodzakelijke bedrijfs- en beveiligingsfuncties binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en technisch uitgangspunten.	CIP-netwerk	
Cryptografie	Thema Softwarepakketten	B.05	Ja	Ter bescherming van de communicatie en opslag van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1.	
O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen	BIO 2019	10.1.1.1	Ja	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	Direct op BIO 2019 gebaseerd	

				organisaties wordt het beleid onderling vastgesteld.		
O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen	BIO 2019	10.1.1.2	Ja	Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd	
Levenscyclusmanagement softwarepakket	Thema Softwarepakketten	U.01		De leverancier behoort de klant te adviseren met marktontwikkelingen en kennis van (de leeftijd van) applicaties en technische softwarestack over strategische ontwikkeling en innovatieve keuzes voor het ontwikkelen en onderhouden van informatiesystemen in het applicatielandschap.	CIP-netwerk	
Beperkingen wijziging softwarepakket	Thema Softwarepakketten	U.02	Ja	Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en alle veranderingen behoren strikt te worden gecontroleerd.	ISO 27002 2017: 14.2.4, BIO 2019: 14.1.1.	
Bedrijfscontinuïteit	Thema Softwarepakketten	U.03		De leverancier behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.	BIO 2019: 17.1.2.	
Input-/output-validatie	Thema Softwarepakketten	U.04		Het softwarepakket behoort mechanismen te bevatten voor normalisatie en validatie van invoer en voor schoning van de uitvoer.	SSD 2020: SSD-19; SSD 2020: SSD-20	

Sessiebeheer	Thema Software pakketten	U.05		Sessies behoren authentiek te zijn voor elke gebruiker en behoren ongeldig gemaakt te worden na een time-out of perioden van inactiviteit.	SSD 2020: SSD-12; SSD 2020: SSD-14	SAML (authenticatie)
Gegevensopslag	Thema Software pakketten	U.06		Te beschermen gegevens worden veilig opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Opslag vindt alleen plaats als noodzakelijk.	SSD 2020: SSD-2 met O-maatregel BIO 2019: 10.1.1.2.	
Communicatie	Thema Software pakketten	U.07		Het softwarepakket past versleuteling toe op de communicatie van gegevens die passend bij het classificatieniveau is van de gegevens en controleert hierop.	SSD 2020: SSD-4	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam)
Authenticatie	Thema Software pakketten	U.08		Softwarepakketten behoren de identiteiten van gebruikers vast te stellen met een mechanisme voor identificatie en authenticatie.	SSD 2020: SSD-5 SIG 2019: 3.2.3	
Toegangsautorisatie	Thema Software pakketten	U.09		Het softwarepakket behoort een autorisatiemechanisme te bieden.	SSD 2020: SSD-8	
Autorisatiebeheer	Thema Software pakketten	U.10		De rechten die gebruikers hebben binnen een softwarepakket (inclusief beheerders) zijn zo ingericht dat autorisaties kunnen worden toegewezen aan organisatorische functies en scheiding van niet verenigbare autorisaties mogelijk is.	SSD 2020: SSD-7	

Logging	Thema Softwarepakketten	U.11		Het softwarepakket biedt signaleringsfuncties voor registratie en detectie die beveiligd zijn ingericht.	SSD 2020: SSD-30	
Application Programming Interface (API)	Thema Softwarepakketten	U.12		Softwarepakketten behoren veilige API's te gebruiken voor import en export van gegevens.	OWASP ASVS 2020: V13	
Gegevensimport	Thema Softwarepakketten	U.13		Softwarepakketten behoren mechanismen te bieden om niet-vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.	OWASP ASVS 2020: V12	
Versiebeheer	Thema Softwarepakketten	C.02	Ja	Wijzigingen aan het softwarepakket binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	BIO 2019: 12.1.2, 14.2.2.	
Patchmanagement	Thema Softwarepakketten	C.03	Ja	Patchmanagement behoort procesmatig en procedureel uitgevoerd te worden, dat tijdig vanuit externe bibliotheken informatie wordt ingewonnen over technische kwetsbaarheden van de gebruikte code, zodat zo snel mogelijk de laatste (beveiligings-)patches kunnen worden geïnstalleerd.	BIO 2019: 12.6.1, NCSC 2015: C.09.	
Privacy by Default binnen applicaties	Privacy-supplement SSD	SSD P.01		De applicatie vraagt bij elke verzameling van persoonsgegevens vrijelijk en ondubbelzinnig toestemming aan betrokkene, waarvan de persoonsgegevens worden verwerkt, om de gegevens te mogen verwerken, waarbij standaard zo min mogelijk	CIP De Privacy Baseline 2020: U.05, AVG: art. 25, Wpg Art 4b lid 1a en lid 1b	

				persoonsgegevens worden verwerkt		
Correcte en gewenste verwerking met applicaties	Privacy-supplement SSD	SSD P.02		De applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.	AVG: art. 7, 11, 12, 16, 17, 18, 19, 20, 21, 22 en 23, Wpg: Art 27 Art 28	
Informatieverstrekking aan betrokkene met applicaties	Privacy-supplement SSD	SSD P.03		Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, geïnformeerd betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens.	CIP De Privacy Baseline 2020: U.05, AVG: art. 14, AVG: overweging 60, Wpg: Art 24a lid 1 t/m 4, art 24b	
Toegang op taakniveau met applicaties	Privacy-supplement SSD	SSD P.04		Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	CIP-netwerk, Wpg: Art 6 lid 1 t/m 6 Art 6a	
Logging met applicaties	Privacy-supplement SSD	SSD P.05		De applicatie behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a	

Dataminimalisatie binnen applicaties	Privacy-supplement SSD	SSD P.06		De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.	AVG: art. 6 lid 1, Wpg art 3 lid 2 en 5, Art 4 lid 2, Art 8 lid 1, 2, 6, Art 9 lid 4, Art 14	
Generalisatie binnen applicaties	Privacy-supplement SSD	SSD P.07		De applicatie behoort, indien de functionele eisen aan de applicatie van de opdrachtgever dit toelaten, gegeneraliseerde gegevens te gebruiken.	ENISA strategie (January 12, 2015) 'generaliseren'	
Scheiden binnen applicaties	Privacy-supplement SSD	SSD P.08		Iedere applicatie kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst.	AVG: art. 6 lid 1, NISA strategie (January 12, 2015) 'scheiden'	
Verbergen binnen applicaties	Privacy-supplement SSD	SSD P.09		Een applicatie, en iedere Functie binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de applicatie en verwerking binnen een functie alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'	

				middleware. Het implementatiemodel is getoetst.		
Beleid voor beveiligde inrichting en onderhoud	Thema Serverplatform	B.01	Ja	Voor het beveiligd inrichten en onderhouden van het serverplatform behoren regels te worden vastgesteld en binnen de organisatie te worden toegepast.	BIO 2019: 14.2.1.	
Inrichtingsprincipes voor serverplatform	Thema Serverplatform	B.02	Ja	Principes voor het inrichten van beveiligde servers behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het inrichten van servers.	BIO 2019: 14.2.1, 14.2.5.	
Serverplatform-architectuur	Thema Serverplatform	B.03		De functionele eisen, beveiligingseisen en architectuurvoorschriften van het serverplatform zijn in samenhang in een architectuurdocument vastgelegd.	NIST SP 800-53 Rev. 5 2020: PL-8	
Bedieningsprocedure	Thema Serverplatform	U.01		Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	BIO 2019: 12.1.1.	
Standaarden voor serverconfiguratie	Thema Serverplatform	U.02		Het serverplatform is geconfigureerd volgens gedocumenteerde standaarden.	SoGP 2018: SY1.2	
Malwareprotectie	Thema Serverplatform	U.03	Ja	Ter bescherming tegen malware behoren beheersmaatregelen voor preventie, detectie en herstel te worden geïmplementeerd, in	BIO 2019: 12.2.1.	

				combinatie met het stimuleren van een passend bewustzijn van gebruikers.		
Technische kwetsbaarhedenbeheer	Thema Serverplatform	U.04	Ja	Informatie over technische serverkwetsbaarheden[1] behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden dient te worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.	BIO 2019: 12.6.1.	STIX en TAXII (uitwisseling van cyberdreigingsinformatie)
Patchmanagement	Thema Serverplatform	U.05		Patchmanagement is procesmatig en procedureel opgezet en wordt ondersteund door richtlijnen zodat het zodanig kan worden uitgevoerd dat op de servers de laatste (beveiligings)patches tijdig zijn geïnstalleerd.	NCSC 2015: C.09	
Beheer op afstand	Thema Serverplatform	U.06		Richtlijnen en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.	BIO 2019: 6.2.2.	
Server-onderhoud	Thema Serverplatform	U.07		Servers behoren correct te worden onderhouden om de continue beschikbaarheid en integriteit te waarborgen.	BIO 2019: 11.2.4.	
Verwijderen of hergebruiken serverapparatuur	Thema Serverplatform	U.08		Alle onderdelen van servers die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	BIO 2019: 11.2.7.	

Hardenen server	Thema Serverplatform	U.09		Voor het beveiligen van een server worden overbodige functies en ongeoorloofde toegang uitgeschakeld.	SoGP 2018: SY1.2.5 SoGP 2018: SY1.2.8	
Serverconfiguratie	Thema Serverplatform	U.10		Serverplatforms behoren zo geconfigureerd te zijn, dat zij functioneren zoals het vereist is en zijn beschermd tegen ongeautoriseerd en incorrecte updates.	SoGP 2018: SY1.2	
Virtualisatie serverplatform	Thema Serverplatform	U.11		Virtuele servers behoren goedgekeurd te zijn en toegepast te worden op robuuste en veilige fysieke servers (bestaande uit hypervisors en virtuele servers) en behoren zodanig te zijn geconfigureerd dat gevoelige informatie in voldoende mate is beveiligd.	SoGP 2018: SY1.3	
Beperking van software- installatie	Thema Serverplatform	U.12	Ja	Voor het door gebruikers (beheerders) installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	BIO 2019: 12.6.2.	
O-maatregel. Beperkingen voor het installeren van software	BIO 2019	12.6.2.1	Ja	Gebruikers kunnen op hun werkomgeving niets zelf installeren, anders dan wat via de ICT-leverancier wordt aangeboden of wordt toegestaan (whitelist).	Direct op BIO 2019 gebaseerd	
Kloksynchronisatie	Thema Serverplatform	U.13		De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gedocumenteerd en gesynchroniseerd met één referentietijdbron.	BIO 2019: 12.4.4.	

Ontwerpdocument	Thema Serverplatform	U.14		Het ontwerp van een serverplatform behoort te zijn gedocumenteerd.	SoGP 2018: SY1.1.1	
Evaluatierichtlijn servers en serverplatforms	Thema Serverplatform	C.01		Richtlijnen behoren te worden vastgesteld om de implementatie en beveiliging van servers en besturingssystemen te controleren waarbij de bevindingen tijdig aan het management worden gerapporteerd.	ISO 27002 2017: 10.10.2	
Beoordeling technische serveromgeving	Thema Serverplatform	C.02	Ja	Technische serveromgevingen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor servers en besturingssystemen.	BIO 2019: 18.2.3.	
O-maatregel. Beoordeling van technische naleving	BIO 2019	18.2.3.1	Ja	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde) kwetsbaarheidsanalyses of penetratietesten.	Direct op BIO 2019 gebaseerd	
Logbestanden beheerders	Thema Serverplatform	C.03		Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.	BIO 2019: 12.4.3.	
Logging	Thema Serverplatform	C.04	Ja	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	BIO 2019: 12.4.1.	

O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.3	Ja	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	
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.4	Ja	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	
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.5	Ja	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Direct op BIO 2019 gebaseerd	
Monitoring	Thema Serverplatform	C.05		De organisatie reviewt/analyseert regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten op servers en besturingssystemen vast te stellen en bevindingen aan het management te rapporteren.	NCSC 2015: C.07	

Beheerorganisatie servers en serverplatforms	Thema Serverplatform	C.06		Binnen de beheerorganisatie is een beveiligingsfunctionaris benoemd die de organisatie ondersteunt in de vorm van het bewaken van beveiligingsbeleid en die inzicht verschaft in de inrichting van de servers en het serverplatform.	CIP-netwerk	
DataminimalisatieDataminimalisatie door serverplatformen	Privacy-supplement Serverplatform	SVP P.01		De organisatie behoort een proces te hebben ingericht en afspraken te hanteren, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en verwijdering van persoonsgegevens mogelijk is.	AVG: art. 6 lid 1, Wpg art 3 lid 2	
Scheiden door serverplatformen	Privacy-supplement Serverplatform	SVP P.02		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden'	
Verbergen door serverplatformen	Privacy-supplement Serverplatform	SVP P.03		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'	

Beleid en procedures voor informatietransport	Thema Communicatievoorzieningen	B.01		Ter bescherming van het informatietransport, dat via allerlei soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	BIO 2019: 13.2.1.	
Cryptografiebeleid voor communicatie	Thema Communicatievoorzieningen	B.03	Ja	Ter bescherming van informatie behoort een cryptografiebeleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1.	
O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen	BIO 2019	10.1.1.1	Ja	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	
O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen	BIO 2019	10.1.1.2	Ja	Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd	
Organisatiestructuur netwerkbeheer	Thema Communicatievoorzieningen	B.04		In het beleid behoort te zijn vastgesteld dat een centrale organisatiestructuur gebruikt wordt voor het beheren van netwerken (onder andere Local Area Network (LAN) en Virtual	BSI 200-2 2017: 4.2	

				Local Area Network (VLAN)) en zo veel mogelijk van de hardware en softwarecomponenten daarvan.		
Richtlijnen voor netwerkbeveiliging	Thema Communicatievoorzieningen	U.01		Organisaties behoren hun netwerken te beveiligen met richtlijnen voor ontwerp, implementatie en beheer.	CIP-netwerk	
Beveiligde inlogprocedure	Thema Communicatievoorzieningen	U.02	Ja	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot (communicatie)systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	BIO 2019: 9.4.2.	SAML (authenticatie)
O-maatregel. Beveiligde inlogprocedures	BIO 2019	9.4.2.2	Ja	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	
Netwerkbeveiligingsbeheer	Thema Communicatievoorzieningen	U.03		Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.	
Vertrouwelijkheids- en of geheimhoudingsovereenkomst	Thema Communicatievoorzieningen	U.04		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.	

Beveiliging van netwerkdiensten	Thema Communicatievoorzieningen	U.05	Ja	Beveiligingsmechanismen, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	BIO 2019: 13.1.2.	
O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.1	Ja	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	
O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.2	Ja	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	
O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.3	Ja	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd gebied wordt gebruik gemaakt van	Direct op BIO 2019 gebaseerd	

				encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.		
Zonering en filtering	Thema Communicatievoorzieningen	U.06	Ja	Groepen van informatiediensten, -gebruikers en -systemen behoren in netwerken te worden gescheiden (in domeinen).	BIO 2019: 13.1.3.	
O-maatregel. Scheiding in netwerken	BIO 2019	13.1.3.1	Ja	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Direct op BIO 2019 gebaseerd	
Elektronische berichten	Thema Communicatievoorzieningen	U.07	Ja	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)
O-maatregel. Elektronische berichten	BIO 2019	13.2.3.2	Ja	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	
O-maatregel. Elektronische berichten	BIO 2019	13.2.3.3	Ja	Maak gebruik van PKIoverheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontlenen.	Direct op BIO 2019 gebaseerd	
O-maatregel. Elektronische berichten	BIO 2019	13.2.3.4	Ja	Om zekerheid te bieden over de integriteit van het elektronische bericht, wordt voor elektronische handtekeningen gebruik	Direct op BIO 2019 gebaseerd	

				gemaakt van de AdES Baseline Profile standaard.		
Toepassingen via openbare netwerken	Thema Communicatievoorzieningen	U.08		Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten, geschillen over contracten en onbevoegde openbaarmaking en wijziging.	BIO 2019: 14.1.2.	
Gateways en firewalls	Thema Communicatievoorzieningen	U.09		De filterfuncties van gateways en firewalls behoren zo te zijn geconfigureerd, dat inkomend en uitgaand netwerkverkeer wordt gecontroleerd en dat daarbij in alle richtingen uitsluitend het vanuit beveiligingsbeleid toegestaan netwerkverkeer wordt doorgelaten.	ISO 27033-4 2014: 6	
Virtual Private Networks	Thema Communicatievoorzieningen	U.10		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
Cryptografische services	Thema Communicatievoorzieningen	U.11	Ja	Ter bescherming van de vertrouwelijkheid en integriteit van de getransporteerde informatie behoren passende cryptografische beheersmaatregelen te worden ontwikkeld, geïmplementeerd en ingezet.	BIO 2019: 18.1.5, ISO 27033-1 2015: 7.2.2.2.	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)
Draadloze toegang	Thema Commun	U.12		Draadloos verkeer behoort te worden beveiligd met	CIP-netwerk	* WPA2 Enterprise

	icatievoorzieningen			authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.		(Beveiligde WiFi-netwerken)
Netwerkconnecties	Thema Communicatievoorzieningen	U.13		Alle gebruikte routeringen, segmenten, verbindingen en aansluitpunten van een bedrijfsnetwerk behoren bekend te zijn en te worden bewaakt.	CIP-netwerk	
Netwerkauthenticatie	Thema Communicatievoorzieningen	U.14		Authenticatie van netwerk-nodes behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.	CIP-netwerk	
Netwerkbeheeractiviteiten	Thema Communicatievoorzieningen	U.15		Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	BIO 2019: 13.1.1.	
Logging en monitoring	Thema Communicatievoorzieningen	U.16	Ja	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.	
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.3	Ja	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	

O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.4	Ja	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	
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.5	Ja	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Direct op BIO 2019 gebaseerd	
Netwerk beveiligingsarchitectuur	Thema Communicatievoorzieningen	U.17		De beveiligingsarchitectuur behoort de samenhang van het netwerk te beschrijven en structuur te bieden in de beveiligingsmaatregelen, gebaseerd op het vigerende bedrijfsbeleid, de leidende principes en de geldende normen en standaarden.	CIP-netwerk	
Naleving richtlijn netwerkbeheer en evaluaties	Thema Communicatievoorzieningen	C.01		Richtlijnen voor de naleving van het netwerkbeveiligingsbeleid behoren periodiek getoetst en geëvalueerd te worden.	CIP-netwerk	
Compliance-toets netwerkbeveiliging	Thema Communicatievoorzieningen	C.02		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	CIP-netwerk	

				management (compliancy-toetsen).		
Evalueren robuustheid netwerkbeveiliging	Thema Communicatievoorzieningen	C.03		De robuustheid van de beveiligingsmaatregelen en de naleving van het netwerkbeveiligingsbeleid behoren periodiek getest en aangetoond te worden.	CIP-netwerk	
Evalueren netwerkgebeurtenissen (monitoring)	Thema Communicatievoorzieningen	C.04		Toereikende logging en monitoring behoren te zijn ingericht, om detectie, vastlegging en onderzoek van gebeurtenissen mogelijk te maken van gebeurtenissen, die mogelijk van invloed op of relevant kunnen zijn voor de informatiebeveiliging.	ISO 27033-1 2015: 8.5	
Beheersorganisatie netwerkbeveiliging	Thema Communicatievoorzieningen	C.05	Ja	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	BIO 2019: 6.1.1.	
Scheiden binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.01		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden'	
Verbergen binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.02		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruikt wordt, waarbij het verbergen van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'	

Logging binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.03		De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a	
Huisvesting IV-Beleid	Thema Huisvesting-IV	B.01	Ja	Ten behoeve van het huisvesting IV-beleid behoort een reeks beleidsregels te worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	BIO 2019: 5.1.1.	
Wet- en regelgeving	Thema Huisvesting-IV	B.02		Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de huisvesting IV-organisatie om aan deze eisen te voldoen behoren voor elke huisvestingsdienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	BIO 2019: 18.1.1.	
Eigenaarschap	Thema Huisvesting-IV	B.03		Huisvesting IV-bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben.	BIO 2019: 8.1.2.	
Certificering	Thema Huisvesting-IV	B.04		Huisvesting IV van de leverancier behoort gecertificeerd te zijn conform de gangbare standaarden.	CIP-netwerk	
Service Level Management	Thema Huisvesting-IV	B.06		Het management van huisvesting IV behoort diensten te leveren conform een	CIP-netwerk	

				dienstenniveau-overeenkomst (Service Level Agreement).		
In- en externe bedreigingen	Thema Huisvesting-IV	B.07	Ja	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	BIO 2019: 11.1.4.	
Training en bewustwording	Thema Huisvesting-IV	B.08	Ja	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	BIO 2019: 7.2.2.	
Organisatiestructuur huisvesting IV	Thema Huisvesting-IV	B.09		De huisvesting IV-organisatie behoort voor de te realiseren huisvesting IV een adequate organisatiestructuur in te richten en de aan functionarissen toe te wijzen taken, verantwoordelijkheden en bevoegdheden vast te stellen.	CIP-netwerk	
Richtlijn gebieden en ruimten	Thema Huisvesting-IV	U.01		Voor het werken in beveiligde gebieden behoren richtlijnen te worden ontwikkeld en toegepast.	BIO 2019: 11.1.5.	
Bedrijfsmiddelen-inventaris	Thema Huisvesting-IV	U.02		Bedrijfsmiddelen die samenhangen met informatie en informatie-verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze bedrijfsmiddelen behoort een inventaris te worden opgesteld en onderhouden	BIO 2019: 8.1.1.	

Fysieke zonering	Thema Huisvesting-IV	U.03	Ja	Fysieke beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	BIO 2019: 11.1.1.	
Beveiligingsfaciliteiten	Thema Huisvesting-IV	U.04	Ja	Voor het beveiligen van ruimten behoren faciliteiten te worden ontworpen en toegepast.	BIO 2019: 11.1.3.	
Nutsvoorziening	Thema Huisvesting-IV	U.05		Apparatuur behoort te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	BIO 2019: 11.2.2.	
Apparatuur-positionering	Thema Huisvesting-IV	U.06	Ja	Apparatuur behoort zo te worden geplaatst en beschermd, dat risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	BIO 2019: 11.2.1, 11.2.9.	
O-maatregel. 'Clear desk'- en 'clear screen'-beleid	BIO 2019	11.2.9.1	Ja	Een onbemensde werkplek is altijd vergrendeld.	Direct op BIO 2019 gebaseerd	
O-maatregel. 'Clear desk'- en 'clear screen'-beleid	BIO 2019	11.2.9.2	Ja	Informatie wordt automatisch ontoegankelijk gemaakt met bijvoorbeeld een screensaver na een inactiviteit van maximaal 15 minuten.	Direct op BIO 2019 gebaseerd	
O-maatregel. 'Clear desk'- en 'clear screen'-beleid	BIO 2019	11.2.9.3	Ja	Sessies op remote desktops worden op het remote platform vergrendeld na een vastgestelde periode.	Direct op BIO 2019 gebaseerd	
O-maatregel. 'Clear desk'- en 'clear screen'-beleid	BIO 2019	11.2.9.4	Ja	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de	Direct op BIO 2019 gebaseerd	

				sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.		
O-maatregel. 'Clear desk'- en 'clear screen'-beleid	BIO 2019	11.2.9.5	Ja	Bij het gebruik van een chipcardtoken voor toegang tot systemen wordt bij het verwijderen van het token de toegangsbeveiligingslock automatisch geactiveerd.	Direct op BIO 2019 gebaseerd	
Apparatuur-onderhoud	Thema Huisvesting-IV	U.07		Apparatuur behoort op een correcte wijze te worden onderhouden.	BIO 2019: 11.2.4.	
Apparatuur-verwijdering	Thema Huisvesting-IV	U.08		Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	BIO 2019: 11.2.7.	
Bedrijfsmiddelenverwijdering	Thema Huisvesting-IV	U.09		Informatieverwerkende bedrijfsmiddelen, uitgezonderd daarvoor bestemde mobiele apparatuur, behoren niet van de locatie te worden verwijderd zonder voorafgaande goedkeuring.	BIO 2019: 11.2.5.	
Laad- en loslocatie	Thema Huisvesting-IV	U.10		Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden, behoren te worden beheerst, en zo mogelijk te worden afgeschermd van IT-voorzieningen	BIO 2019: 11.1.6.	
Bekabeling	Thema Huisvesting-IV	U.11		Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen	BIO 2019: 11.2.3.	

Huisvesting IV-architectuur	Thema Huisvesting-IV	U.12		Voor het implementeren en onderhouden van huisvestingsvoorzieningen behoren architectuurvoorschriften en benodigde documentatie beschikbaar te zijn.	CIP-netwerk	
Controle-richtlijn huisvesting IV	Thema Huisvesting-IV	C.01		Bedrijfsmiddelen behoren periodiek te worden gecontroleerd met formeel vastgestelde richtlijnen en geconstateerde bevindingen dienen tijdig aan het management te worden gerapporteerd.	CIP-netwerk	
Onderhoudsplan	Thema Huisvesting-IV	C.02		Voor iedere locatie van huisvesting IV behoort een onderhoudsplan te zijn opgesteld met een risicoafweging en onderhoudsbepalingen.	CIP-netwerk	
Continuïteitbeheer	Thema Huisvesting-IV	C.03		Continuïteitbeheer behoort procesmatig voor de gehele organisatie te zijn ingericht, zodat na het plaatsvinden van een calamiteit de hosting services zo snel mogelijk worden hersteld en voortgezet.	NCSC 2015: C10	
Uitvallen van een dienst	Privacy-supplement Huisvesting-IV	HVI P.01		De organisatie heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.	AVG: art. 24, 32, 35, 36	

Wet en Regelgeving	Thema Clouddiensten	B.01		Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de CSP om aan deze eisen te voldoen behoren voor elke clouddienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	BIO 2019: 18.1.1.	
Cloudbeveiligingsstrategie	Thema Clouddiensten	B.02		De CSP behoort een cloud-beveiligingsstrategie te hebben ontwikkeld die samenhangt met de strategische doelstelling van de CSP en die aantoonbaar de informatieveiligheid ondersteunt.	SoGP 2018: SG2.1	
Exit-strategie	Thema Clouddiensten	B.03		In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exitstrategie te zijn opgenomen waarbij zowel een aantal bepalingen6 over exit zijn opgenomen, als een aantal condities6 die aanleiding kunnen geven tot een exit.	CIP-netwerk	
Clouddienstenbeleid	Thema Clouddiensten	B.04		De CSP behoort haar informatiebeveiligingsbeleid uit te breiden met een cloud-beveiligingsbeleid om de voorzieningen en het gebruik van cloudservices te adresseren.	ISO 27017 2015: 5.1.1	
Transparantie	Thema Clouddiensten	B.05		De CSP voorziet de CSC in een systeembeschrijving waarin de clouddiensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.	BSI C5 2020: BC-01 BSI C5 2020: BC-05 BSI C5 2020: BC-06	

Risicomanagement	Thema Clouddiensten	B.06		De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.	ISO 27005 2018: 7.4	
IT-functionaliteit	Thema Clouddiensten	B.07		IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.	SoGP 2018: BC1.3	
Bedrijfscontinuïteitsmanagement	Thema Clouddiensten	B.08		De CSP behoort haar BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.	CIP-netwerk	
Privacy en bescherming persoonsgegevens	Thema Clouddiensten	B.09		De CSP behoort, ter bescherming van bedrijfs- en persoonlijke data, beveiligingsmaatregelen te hebben getroffen vanuit verschillende dimensies: beveiligingsaspecten en stadia, toegang en privacy, classificatie/labelen, eigenaarschap en locatie.	ITU-T FG Cloud TR Part 5 2012: 8.5	
Beveiligingsorganisatie	Thema Clouddiensten	B.10	Ja	De CSP behoort een beveiligingsfunctie te hebben benoemd en een beveiligingsorganisatie te hebben ingericht, waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.	CIP-netwerk, BIO 2019: 6.1.1.	

Clouddienstenarchitectuur	Thema Clouddiensten	B.11		De CSP heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.	CIP-netwerk	
Standaarden voor clouddiensten	Thema Clouddiensten	U.01		De CSP past aantoonbaar relevante, nationale standaarden en internationale standaarden toe voor de opzet en exploitatie van de diensten en de interactie met de CSC.	CIP-netwerk	
Risico-assessment	Thema Clouddiensten	U.02		De CSP behoort een risico-assessment uit te voeren, bestaande uit een risico-analyse en risico-evaluatie met de criteria en de doelstelling voor clouddiensten van de CSP.	ISO 27005 2018: 8.1	
Bedrijfscontinuïteitsservices	Thema Clouddiensten	U.03		Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.	BIO 2019: 17.2.1.	
Herstelfunctie voor data en clouddiensten	Thema Clouddiensten	U.04		De herstelfunctie van de data en clouddiensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest.	CIP-netwerk	
Dataprotectie	Thema Clouddiensten	U.05		Data ('op transport', 'in verwerking' en 'in rust') met de classificatie BBN2 of hoger behoort te worden beschermd met cryptografische maatregelen en te voldoen aan Nederlandse wetgeving.	ISO 27040 2016: 6.3.2.1	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam) * STARTTLS en DANE (beveiligde mailserver-verbindingen)

						* DMARC+DKIM+SPF (anti-mailphishing/-spoofing) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)
Dataretentie en gegevensvernietiging	Thema Clouddiensten	U.06	Ja	Gearchiveerde data behoort gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van de CSC/data-eigenaar te kunnen worden vernietigd.	CIP-netwerk, BIO 2019: 18.1.3.	
O-maatregel. Beschermen van registraties	BIO 2019	18.1.3.1	Ja	De proceseigenaar heeft per soort informatie inzichtelijk gemaakt wat de bewaartermijn is.	Direct op BIO 2019 gebaseerd	
Datascheiding	Thema Clouddiensten	U.07		CSC-gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van en andere dienstverlening aan andere CSC's, die de CSP in beheer heeft.	ISO 27040 2016: 7.7.4	
Scheiding dienstverlening	Thema Clouddiensten	U.08		De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.	CIP-netwerk	
Malware-protectie	Thema Clouddiensten	U.09	Ja	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.	BIO 2019: 12.2.1.	

Toegang IT-diensten en data	Thema Clouddiensten	U.10	Ja	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.	BIO 2019: 9.1.2.	
Cryptoservices	Thema Clouddiensten	U.11	Ja	Gevoelige data van CSC's behoort conform het overeengekomen beleid inzake cryptografische maatregelen tijdens transport via netwerken en bij opslag bij CSP te zijn versleuteld	CIP-netwerk, BIO 2019: 10.1.1, 10.1.2.	* TLS, HTTPS en HSTS (beveiligde verbinding)
O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen	BIO 2019	10.1.1.1	Ja	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	
O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaatregelen	BIO 2019	10.1.1.2	Ja	Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd	
O-maatregel. Sleutelbeheer	BIO 2019	10.1.2.1	Ja	Ingeval van PKIoverheid-certificaten: hanteer de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties: hanteer de standaard ISO 11770 voor het beheer van cryptografische sleutels.	Direct op BIO 2019 gebaseerd	

O-maatregel. Sleutelbeheer	BIO 2019	10.1.2.2	Ja	Er zijn (contractuele) afspraken over reservecertificaten van een alternatieve leverancier als uit risicoafweging blijkt dat deze noodzakelijk zijn.	Direct op BIO 2019 gebaseerd	
Koppelvlakken	Thema Clouddiensten	U.12	Ja	De onderlinge netwerkconnecties (koppelvlakken) in de keten van de CSC naar de CSP behoren te worden bewaakt en beheerst om de risico's van datalekken te beperken.	CIP-netwerk, BIO 2019: 13.1.2.	
O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.1	Ja	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	
O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.2	Ja	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	

O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.3	Ja	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	
Service-orkestratie	Thema Clouddiensten	U.13		Service-orkestratie biedt coördinatie, aggregatie en samenstelling van de servicecomponenten van de cloud-service die aan de CSC wordt geleverd.	ISO 17789 2014: 9.2.3.4	
Interoperabiliteit en portabiliteit	Thema Clouddiensten	U.14		Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende ITplatforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit) naar andere CSP's.	ISO 19941 2017: 7.1.7 BSI C5 2020: COS-02	* TLS, HTTPS en HSTS (beveiligde verbinding)
Logging en monitoring	Thema Clouddiensten	U.15	Ja	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	BIO 2019: 12.4.1.	
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.3	Ja	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	Direct op BIO 2019 gebaseerd	

				informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.		
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.4	Ja	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	
O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.5	Ja	De SIEM en/of SOC hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management.	Direct op BIO 2019 gebaseerd	
Clouddienstenarchitectuur	Thema Clouddiensten	U.16		De clouddienstenarchitectuur specificeert de samenhang en beveiliging van de services en de interconnectie tussen de CSC en de CSP en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.	CIP-netwerk	
Multi-tenantarchitectuur	Thema Clouddiensten	U.17		Bij multi-tenancy wordt de CSC-data binnen clouddiensten, die door meerdere CSC's worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines	CIP-netwerk	

Servicemanagementbeleid en evaluatierichtlijn	Thema Clouddiensten	C.01		De CSP heeft voor clouddiensten een servicemanagementbeleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.	CIP-netwerk	
Risico-control	Thema Clouddiensten	C.02		Risicomanagement en het risico-assessmentproces behoren continu te worden gemonitord en gereviewd en zo nodig te worden verbeterd.	ISO 27005 2018: 12.1 ISO 27005 2018: 12.2	
Compliance en assurance	Thema Clouddiensten	C.03	Ja	De CSP behoort regelmatig de naleving van de cloudbeveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een assurance-verklaring aan de CSC uit te brengen en te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.	BIO 2019: 5.1.2, 18.2.1, 18.2.2, 18.2.3.	
O-maatregel. Onafhankelijke beoordeling van informatiebeveiliging	BIO 2019	18.2.1.1	Ja	Er is een information security management system (ISMS) waarmee aantoonbaar de gehele Plan-Do-Check-Act cyclus op gestructureerde wijze wordt afgedekt.	Direct op BIO 2019 gebaseerd	
O-maatregel. Onafhankelijke beoordeling van informatiebeveiliging	BIO 2019	18.2.1.2	Ja	Er is een vastgesteld auditplan waarin jaarlijks keuzes worden gemaakt voor welke systemen welk soort beveiligingsaudits worden uitgevoerd.	Direct op BIO 2019 gebaseerd	
O-maatregel. Beoordeling van technische naleving	BIO 2019	18.2.3.1	Ja	Informatiesystemen worden jaarlijks gecontroleerd op technische naleving van beveiligingsnormen en risico's ten aanzien van de feitelijke veiligheid. Dit kan bijvoorbeeld door (geautomatiseerde)	Direct op BIO 2019 gebaseerd	

				kwetsbaarheidsanalyses of penetratietesten.		
Technische kwetsbaarhedenbeheer	Thema Clouddiensten	C.04	Ja	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.	BIO 2019: 12.6.1.	STIX en TAXII (Uitwisseling van cyberdreigingsinformatie)
Security-monitoringsrapportage	Thema Clouddiensten	C.05		De performance van de informatiebeveiliging van de cloud-omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan verschillende stakeholders.	ISO 27002 2017:12.4 SoGP 2018: SI2.1	
Beheersorganisatie clouddiensten	Thema Clouddiensten	C.06		De CSP heeft een beheersorganisatie ingericht waarin de processtructuur en de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.	CIP-netwerk	
Testdata	Privacy-supplement Applicatieontwikkeling Algemeen	APO P.01		Waar mogelijk wordt als testdata gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data, wanneer op basis van de resultaten van een risico-analyse gebruik gemaakt wordt van persoonsgegevens, worden passende maatregelen ter bescherming van de persoonsgegevens genomen.	ISO 27701 2019: 6.11.3.1, NEN 7510 2017: 14.3.1 AVG: art. 4.2, 6, 15, 25.1 en 32	

Privacy by Default binnen applicaties	Privacy-supplement SSD	SSD P.01		De applicatie vraagt bij elke verzameling van persoonsgegevens vrijelijk en ondubbelzinnig toestemming aan betrokkene, waarvan de persoonsgegevens worden verwerkt, om de gegevens te mogen verwerken, waarbij standaard zo min mogelijk persoonsgegevens worden verwerkt	CIP De Privacy Baseline 2020: U.05, AVG: art. 25, Wpg Art 4b lid 1a en lid 1b	
Correcte en gewenste verwerking met applicaties	Privacy-supplement SSD	SSD P.02		De applicatie biedt de mogelijkheid om op aangeven van betrokkene, waarvan de persoonsgegevens worden verwerkt, controle te houden over de gegevens en de verwerking ervan, zodat de juistheid en nauwkeurigheid van de gegevens kan worden gewaarborgd en de verwerking ervan kan worden gecorrigeerd, gestaakt of overgedragen.	AVG: art. 7, 11, 12, 16, 17, 18, 19, 20, 21, 22 en 23, Wpg: Art 27 Art 28	
Informatieverstrekking aan betrokkene met applicaties	Privacy-supplement SSD	SSD P.03		Om de gegevens te mogen verwerken wordt de betrokkene, waarvan de persoonsgegevens worden verwerkt, geïnformeerd betreffende welke verwerking (van de persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens.	CIP De Privacy Baseline 2020: U.05, AVG: art. 14, AVG: overweging 60, Wpg: Art 24a lid 1 t/m 4, art 24b	
Toegang op taakniveau met applicaties	Privacy-supplement SSD	SSD P.04		Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	CIP-netwerk, Wpg: Art 6 lid 1 t/m 6 Art 6a	

Logging met applicaties	Privacy-supplement SSD	SSD P.05		De applicatie behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a	
Dataminimalisatie binnen applicaties	Privacy-supplement SSD	SSD P.06		De organisatie behoort een proces te hebben ingericht, waarbinnen een analyse wordt gemaakt en aantoonbaar is dat het verzamelen van de persoonsgegevens rechtmatig en noodzakelijk is en het ontwerp getoetst wordt aan het uitgangspunt dataminimalisatie, de juiste wijze van opslag en het hanteren van de bewaartermijn.	AVG: art. 6 lid 1, Wpg art 3 lid 2 en 5, Art 4 lid 2, Art 8 lid 1, 2, 6, Art 9 lid 4, Art 14	
Generalisatie binnen applicaties	Privacy-supplement SSD	SSD P.07		De applicatie behoort, indien de functionele eisen aan de applicatie van de opdrachtgever dit toelaten, gegeneraliseerde gegevens te gebruiken.	ENISA strategie (January 12, 2015) ‘generaliseren’	
Scheiden binnen applicaties	Privacy-supplement SSD	SSD P.08		Iedere applicatie kent een duidelijk verwerkingsdoel, waarbij de scheiding van de verwerking gerealiseerd is op het niveau van de applicatie, de transportpaden, de middleware, de opslagvoorzieningen en is hierop getoetst.	AVG: art. 6 lid 1, NISA strategie (January 12, 2015) ‘scheiden’	
Verbergen binnen applicaties	Privacy-supplement SSD	SSD P.09		Een applicatie, en iedere Functie binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de applicatie en verwerking binnen een taak alleen de daarvoor noodzakelijke	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015)	

				persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de middleware. Het implementatiemodel is getoetst.	'verbergen'	
DataminimalisatieDataminimalisatie door serverplatformen	Privacy-supplement Serverplatform	SVP P.01		De organisatie behoort een proces te hebben ingericht en afspraken te hanteren, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruiken, waarbij enkel de minimaal benodigde hoeveelheid persoonsgegevens wordt verwerkt en verwijdering van persoonsgegevens mogelijk is.	AVG: art. 6 lid 1, Wpg art 3 lid 2	
Scheiden door serverplatformen	Privacy-supplement Serverplatform	SVP P.02		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden'	
Verbergen door serverplatformen	Privacy-supplement Serverplatform	SVP P.03		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) serverplatforms de instellingen gebruikt worden, waarbij de scheiding van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'	
Scheiden binnen communicatievoorzieningen	Privacy-supplement Communicatievoo	CVZ P.01		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij	NEN 7510 2017: A.12.3.1, ENISA strategie	

	rzieninge n			de scheiding van verwerkingen het uitgangspunt is.	(January 12, 2015) ‘scheiden’	
Verbergen binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieninge n	CVZ P.02		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij het verbergen van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) ‘verbergen’	
Logging binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieninge n	CVZ P.03		De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.	AVG: art. 5 lid 2 en art. 33 lid 5, Wpg Art. 32a	
Uitvallen van een dienst	Privacy-supplement Huisvesting-IV	HVI P.01		De organisatie heeft maatregelen getroffen die voorkomen dat de uitval van een dienst, of dit nu een eigen dienst is of van een derde is, leidt tot een datalek of andere gevolgen voor betrokkenen, waarvan de persoonsgegevens worden verwerkt, en heeft een procedure om de werking van de maatregel te evalueren.	AVG: art. 24, 32, 35, 36	
Het stelsel van toegangsbeheer	Privacy-supplement Toegangsbeveiliging	TBV P.01		Het doel van de verwerking van persoonsgegevens en van de toegang zijn welbepaald, gerechtvaardigd en uitdrukkelijk omschreven, waarbij de toegang naar keuze rol gebaseerd en waar nodig taak gebaseerd wordt verstrekt. Aanvullend vindt logging en monitoringplaats.	AVG: art. 5, Wpg Art 6 lid 1 t/m 6 Art 6a	

Doelbinding op rolniveau	Privacy-supplement Toegangsbeveiliging	TBV P.02		De organisatie behoort verwerkers gescheiden en beperkt toegang te verlenen tot persoonsgegevens, op basis van uit te voeren activiteiten die binnen een specifieke rol worden uitgevoerd en in te trekken, indien de activiteiten, noodzaak of vastgestelde doelbinding niet meer geldt voor deze persoon of rol; de verstrekte toegang is toetsbaar.	NEN 7510 2017: A.9.2.6, Wpg Art 6 lid 1 t/m 6 Art 6a	
Toegang op taakniveau	Privacy-supplement Toegangsbeveiliging	TBV P.03		Het verlenen van toegang tot persoonsgegevens wordt beperkt op basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	CIP-netwerk, Wpg: Art 6 lid 1 t/m 6 Art 6a	
Logging en monitoring uitgeven toegangsrechten	Privacy-supplement Toegangsbeveiliging	TBV P.04		De verwerking behoort op verwerkers/persoonsniveau te loggen, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens de medewerker heeft opgevraagd, ingezien en aangepast.	AVG: art. 33 lid 5 en 5 lid 2, Wpg Art. 32a	
Toegang tot fysieke omgevingen	Privacy-supplement Toegangsbeveiliging	TBV P.05		De organisatie behoort fysieke beveiliging van omgevingen waar persoonsgegevens worden verwerkt, op passende wijze ingericht te hebben, zodat enkel medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd.	ISO 27002 2017: 11.1, ABDO 2019 v1.1: 3.1.2, Wpg: Art 6 lid 1 t/m 6 Art 6a	
Toegang buiten beveiligde omgevingen	Privacy-supplement Toegangsbeveiliging	TBV P.06		Er is een procedure ingericht voor het transporteren van persoonsgegevens buiten een beschermde omgeving, waarbij door versleuteling de kans op een datalek is verkleind en door	AVG: art.32, Wpg: Art 6 lid 1 t/m 6 Art 6a	

				minimalisatie de omvang van een datalek wordt beperkt.		
Toegang in het buitenland	Privacy-supplement Toegangsbeveiliging	TBV P.07		De organisatie hanteert regels voor medewerkers en andere verwerkers, die buiten Nederland persoonsgegevens of authenticatiemiddelen (voor de toegang tot persoonsgegevens vanuit het buitenland) met zich meedragen of in hun bezit hebben, ongeacht of deze informatie versleuteld is.	AVG: art. 32, Wpg: Art 6 lid 1 t/m 6 Art 6a	
Beëindiging (verwerkers)overeenkomst	Privacy-supplement Toegangsbeveiliging	TBV P.08		De verwerkingsverantwoordelijke legt in de (verwerkers) overeenkomst afspraken vast, met de persoon of partij die persoonsgegevens verwerkt, over het verwijderen of overdragen van persoonsgegevens bij beëindiging van de relatie; eventuele derden worden over de beëindiging geïnformeerd.	AVG: art.32, AP Werkende verwerkersovereenkomsten september 2019 : 4.3.6	