Energie Diensten Centrum

Bijlage B informatiebeveiligingseisen – behorend bij Programma van Eisen

Informatiebeveiligingseisen ICO Wizard	
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).
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 standaardfunctionaliteit die door diverse organisaties gebruikt kan worden.
Toegangsbeveiliging	Bevat eisen die gesteld moeten worden aan het geheel van beheersprocessen en faciliteiten die noodzakelijk zijn voor het verschaffen van toegang tot digitale middelen van de organisatie.

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 producteisen voor. Eisen die te maken hebben met louter schaalgrootte zijn buiten beschouwing gelaten.

Naast de informatiebeveiligingseisen ICO geldende er op onderstaande thema's aanvullende specifieke eisen. Als een specifieke eis strijdig is met een ICO eis geldt de specifieke eis.

Energie Diensten Centrum

Specifieke eisen

Thema	Discipline	Eis
Certificering, normen(kaders), rapportages	Informatie-veiligheid	1: De leverancier beschikt over een geldige ISO27001 certificering, inclusief verklaring van toepasselijkheid met relevante scope van de ICT Prestatie.
Certificering, normen(kaders), rapportages	Informatie-veiligheid	2: De leverancier beschikt over een recente ISAE 3402 type 2 of SOC2 verklaring die maatregelen beschrijft van de ICT Prestatie op het gebied van beveiliging, beschikbaarheid, integriteit en vertrouwelijkheid. Hierbij dient voor de geleverde ICT Prestatie aangetoond te worden dat de ISO27002 beheersmaatregelen of een gelijkwaardige set aan beveiligingsmaatregelen in opzet, bestaan en werking ingeregeld zijn. Deze verklaring wordt kosteloos overhandigd aan de Provincie.
Certificering, normen(kaders), rapportages	Informatie-veiligheid	3: Wanneer de leverancier voor de aangeboden ICT Prestatie niet kan voldoen aan eis 2 dan dient de leverancier gelijkwaardigheid aan te tonen. De Provincie vraagt na voorlopige gunning om bewijs. Gelijkwaardigheid kan worden aangetoond, doordat de leverancier: a) Beschikt over een actueel en door de directie ondertekend informatiebeveiligingsbeleid. b) Een gelijkwaardige set aan beveiligingsnormen hanteert zoals de Baseline Informatiebeveiliging Overheid (BIO) en deze ter inzage geeft aan opdrachtgever. c) Soortgelijke rapportage heeft die maatregelen beschrijft van het informatiesysteem op het gebied van beveiliging, beschikbaarheid, integriteit en vertrouwelijkheid en deze ter inzage geeft aan de opdrachtgever. d) Kan aantonen aan de opdrachtgever dat maatregelen op het gebied van Informatiebeveiliging via een PDCA-cyclus actueel wordt gehouden.
Authenticatie van gebruikers en systemen	Informatie-veiligheid	4: Authenticatie verloopt via de Active Directory van de opdrachtgever. Na authenticatie via de Active Directory, hebben gebruikers door middel van Single Sign On (SSO) direct toegang tot alle onderdelen van de ICT-prestatie, uiteraard voor zover ze daartoe zijn geautoriseerd.

Authenticatie van gebruikers en systemen	Informatie-veiligheid	5: Indien authenticatie vanwege zwaar wegende redenen niet verloopt via de Active Directory van de opdrachtgever, dan moet authenticatie zowel met gebruikersnaam en wachtwoord en via een veilige tweede factor verlopen (Multi-Factor Authenticatie).
Autorisaties van gebruikers en systemen	Informatie-veiligheid	6: Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.
Autorisaties van gebruikers en systemen	Informatie-veiligheid	7: Om toegang tot persoonsgegevens te beperken tot die taken die gerechtvaardigd zijn (need-to-know/doelbinding) biedt de ICT-prestatie de mogelijkheid om, naast toegang op basis van (functie)rollen, tevens toegang op basis van taken (binnen een bepaalde rol) in te regelen. Daarnaast biedt de ICT-prestatie de mogelijkheid om (het toekennen) van toegangsrechten te loggen en te monitoren, zodat direct of periodiek kan worden beoordeeld welke persoonsgegevens deze medewerker heeft opgevraagd, ingezien en aangepast.
Autorisaties van gebruikers en systemen	Informatie-veiligheid	8: De ICT Prestatie voorziet in de mogelijkheid om autorisaties te baseren op Role Based Access Control (RBAC) en/of Attribute Based Access Control (ABAC) of soortgelijke.
Veilige verwerking	Informatie-veiligheid	9: De ICT-prestatie zet Transport Layer Security (TLS) Protocol in voor het beveiligen van verbindingen en de ICT-prestatie werkt voor data transport conform de meest actuele beveiligingsrichtlijnen van de NCSC.
Veilige verwerking	Informatie-veiligheid	10: Opgeslagen gegevens dienen te zijn versleuteld. Versleutelingstechniek voor de bescherming van de vertrouwelijkheid van de opgeslagen data vindt plaats conform de marktstandaarden van Forum voor standaardisatie.
Veilige verwerking	Informatie-veiligheid	11: Bij het sturen en ontvangen van e-mails wordt gebruik gemaakt van alle hiervoor relevante, voor overheden verplichte, beveiligingsstandaarden. Op dit moment betekent dat de correcte toepassing van SPF, DKIM, DMARC, DNSSEC, STARTTLS, DANE en IPv4 en IPv6, HTTPS en HSTS verkeer en kan hierop getoetst worden via www.internet.nl. Bij gunning zal gedurende de looptijd van het contract de applicatie streven naar een 100% score op internet.nl, zowel voor de ICT Prestatie als voor de domeinnamen die het gebruikt.

Veilige verwerking	Informatie-veiligheid	12: Beveiligingseisen opgelegd aan de leverancier gelden onverminderd ook voor onderaannemers of partijen in de toeleveringsketen van de aanbestede dienst.
Data backup recovery	Informatie-veiligheid	13: Voor het uitvoeren van de ICT Prestatie voorziet u in een recovery mechanisme dat voorziet in dataverlies van maximaal 28 uur, waarbij in geval van calamiteiten de back-up is gewaarborgd. De hersteltijd in geval van incidenten is maximaal 16 werkuren (twee dagen van 8 uur) in 85% van de gevallen.
Segmentatie	Informatie-veiligheid	14. Alle gegevens van opdrachtgever betreffende de ICT Prestatie worden verwerkt d.m.v. een logische scheiding tussen de afgenomen cloud-service, de interne informatievoorziening van de Cloud Service Provider en de data van andere organisaties, zowel tijdens transport, in bewerking als opslag.
Sessiemanage-ment	Informatie-veiligheid	15: Het aantal sessies dat één gebruiker gelijktijdig kan hebben. Bij het aanmelden van een nieuwe sessie wordt een eventueel al bestaande sessie van die gebruiker verbroken en de oude sessie-identifier ongeldig gemaakt.
Sessiemanagement	Informatie-veiligheid	16: De ICT-prestatie beschikt over een timeout van maximaal 15 minuten voor actieve sessies.
Backup	Informatie-veiligheid	17: De ICT Prestatie heeft een backup en disaster recovery procedure gedocumenteerd en test deze periodiek op werking.
Monitoring, audit, logging	Informatie-veiligheid	18: Activiteiten van gebruikers en beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen worden gemonitord en vastgelegd in audit-logbestanden, met inachtneming van relevante wetgeving, BIO, waarbij geldt: a. Dat deze audit-logbestanden minimaal drie maanden worden bewaard. b. Er is vastgelegd bij welke drempelwaarden meldingen en alarmoproepen gegenereerd worden. c. Van audit-logbestanden rapportages worden gemaakt die periodiek, zoals afgesproken met De Provincie worden gedeeld en beoordeeld. d. Handelingen van gebruikers moeten te allen tijde te herleiden zijn naar een natuurlijk persoon. e. Handelingen van systemen moeten te allen tijde te herleiden zijn naar een systeem. De volgende gebeurtenissen worden in ieder geval opgenomen in de logs:

		f. Gebruik van technische beheerfuncties, zoals een backup maken. g. Gebruik van functionele beheerfuncties, zoals het wijzigen van instellingen, updates van de applicaties. h. Handelingen van autorisatiebeheer, zoals het aanmaken van een gebruiker, wachtwoord reset. i. Inlogpogingen zowel succesvol als onsuccesvol worden vastgelegd. j. Handelingen van gebruikers, het uitvoeren van acties zoals het raadplegen van bestanden/informatie, uitvoeren van overige acties die binnen de applicatie kunnen worden uitgevoerd (bewerken, verwijderen, kopiëren etc) k. Foutmeldingen van applicaties. Een logregel bevat minimaal: l. de gebeurtenis. m. de benodigde informatie die nodig is om het incident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon. n. het gebruikte apparaat, o. het resultaat van de handeling. p. een datum en tijdstip van de gebeurtenis.
Monitoring, audit, logging	Informatie-veiligheid	19: Op verzoek van de opdrachtgever, bijv. n.a.v. een beveiligingsincident, dienen relevante logs en auditgegevens aan de opdrachtgever kosteloos aangeleverd te worden via een algemeen gehanteerd formaat.
Monitoring, audit, logging	Informatie-veiligheid	20: Gedurende de overeenkomst tussen opdrachtgever en leverancier kunnen informatiebeveiligingsincidenten optreden. Indien deze leiden of hebben geleid tot een vermoedelijk of mogelijk opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatie verwerkende systemen worden deze zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording gemeld bij opdrachtgever.
Monitoring, audit, logging	Informatie-veiligheid	21: In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.
Monitoring, audit, logging	Informatie-veiligheid	22: a. Het (automatisch) overschrijven of verwijderen van audit-logbestanden wordt gelogd in de nieuw aangelegde log. b. Het raadplegen van audit-logbestanden voorbehouden is aan geautoriseerde gebruikers. c. Audit-logbestanden en de instellingen van logmechanismen zodanig worden beschermd dat deze niet aangepast of gemanipuleerd kunnen worden.

		d. Indien de instellingen aangepast moeten worden, zal daarbij altijd het 4-ogen principe toegepast worden. e. Het goed functioneren van de logging wordt continue gemonitord. Logbestanden worden periodiek gecontroleerd.
Monitoring, audit, logging	Informatie-veiligheid	23: Leverancier neemt bij succesvolle pogingen tot ongeautoriseerde toegang tot de ICT Prestatie alle noodzakelijke maatregelen teneinde de eventuele schade tot een minimum te beperken en herhaling te voorkomen. De succesvolle ongeautoriseerde toegang alsmede alle getroffen maatregelen zullen tijdig en uiterlijk binnen 24 uur aan de opdrachtgever worden gerapporteerd.
Segmentatie	Informatie-veiligheid	24: Wanneer meerdere klanten van een leverancier dezelfde infrastructuur, database en applicatiecode delen, zijn er maatregelen getroffen om ervoor te zorgen dat de gegevens en configuraties van elke klant geïsoleerd en beschermd blijven. Dit omvat onder andere waarborgen voor multi-tenancy en segmentatie.
Security by design	Informatie-veiligheid	25: Onderliggende softwarecomponenten, zoals operatingsystemen, databasesoftware, middleware, browser versie, programmeer framework enz., waarop de software is gebouwd en draait dienen altijd door de oorspronkelijke leverancier/fabrikant van de betreffende software of framework ondersteund te zijn zodanig dat te allen tijde support is gewaarborgd. Let op: bovenstaande geldt ook voor hardware.
Security by design	Informatie-veiligheid	26: Voor het uitvoeren van de ICT Prestatie wordt gebruik gemaakt van systemen die zijn gehardened. Dit wil zeggen dat overbodige functies en/of software van het besturingssysteem zijn uitgezet of van het systeem zijn verwijderd.
Testen	Informatie-veiligheid	27: Het systeem wordt periodiek gescand op kwetsbaarheden. Tevens wordt er periodiek (minimaal jaarlijks) een security pentest uitgevoerd door een onafhankelijke derde partij in opdracht van de leverancier. De opdrachtgever ontvangt kosteloos een bewijs van uitvoering en indien er opvolging noodzakelijk is volgt dit binnen een afgesproken termijn door de opdrachtnemer. De pentest wordt uitgevoerd volgens de richtlijnen van bijv. de Open Source Security Testing Methodology Manual (OSSTMM), de NIST Special Publication 800-115, OWASP testing Guide of soortgelijke.

Security by design	Informatie-veiligheid	28: Leverancier maakt aantoonbaar dat passende maatregelen zijn genomen door bij het ontwerp de principes van gegevensbescherming te hanteren (privacy/security/archiving by design) en door het hanteren van standaardinstellingen (privacy/security/archiving by default) zoals de meest recente versies van de richtlijnen van Centrum Informatiebeveiliging en Privacybescherming (CIP) veilig ontwikkel beveiligingseisen voor (web)applicaties en de NCSC ICT beveiligingsrichtlijnen voor webapplicaties.
Monitoring, audit, logging	Informatie-veiligheid	29: Logbestanden worden op een andere plaats dan het bronsysteem (centraal) bewaard en zijn niet benaderbaar vanaf het ICT-systeem waarop ze gegenereerd zijn.
Veilige verwerking	Informatie-veiligheid	30. De ICT-prestatie is voorzien van de laatste (beveiligings)patches en deze worden volgens een patchmanagement proces doorgevoerd.

ICO Wizard eisen

Nr	**Naam Eis**	**Referentie brondocument:**	**Referentie code norm:**	**BIO-O-maatregel:**	**Samenvatting eis:**	**Gebaseerd op: (ISO27002-paragraaf, of ander framework)**
1	Bedrijfs- en beveiligingsfuncties	Thema Softwarepakketten	B.04		De noodzakelijke bedrijfs- en beveiligingsfuncties binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en	CIP-netwerk

					technisch uitgangspunten.	
2	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.
3	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
4	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

5	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.
6	Bedrijfscontinuïteit	Thema Softwarepakketten	U.03		De leverancier behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.	BIO 2019: 17.1.2.
7	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
8	Sessiebeheer	Thema Softwarepakketten	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
9	Gegevensopslag	Thema Softwarepakketten	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.

10	Communicatie	Thema Softwarepakketten	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
11	Authenticatie	Thema Softwarepakketten	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
12	Toegangsautorisatie	Thema Softwarepakketten	U.09		Het softwarepakket behoort een autorisatiemechanisme te bieden.	SSD 2020: SSD-8
13	Autorisatiebeheer	Thema Softwarepakketten	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
14	Logging	Thema Softwarepakketten	U.11		Het softwarepakket biedt signaleringsfuncties voor registratie en detectie die beveiligd zijn ingericht.	SSD 2020: SSD-30
15	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
16	Gegevensimport	Thema Softwarepakketten	U.13		Softwarepakketten behoren mechanismen te bieden om niet-	OWASP ASVS 2020: V12

					vertrouwde bestandsgegevens uit niet-vertrouwde omgevingen veilig te importeren en veilig op te slaan.	
17	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
18	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
19	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	CIP De Privacy Baseline 2020: U.05, AVG: art. 14, AVG: overwe

					persoonsgegevens) plaatsvindt en krijgt deze betrokkene een waarschuwing bij het verkrijgen van toegang tot bijzondere persoonsgegevens.	ging 60, Wpg: Art 24a lid 1 t/m 4, art 24b
20	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
21	Logging met applicaties	Privacy-supplement SSD	SSD P.05		De applicatie behoort op verwerkers/persoons niveau 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
22	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

23	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'
24	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'
25	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 middleware. Het implementatiemodel is getoetst.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'

26	Cryptografie	Thema Toegangsbeveiliging	B.04	Ja	Ter bescherming van authenticatie-informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	BIO 2019: 10.1.1 BIO2.0-opmaat: 8.24
27	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
28	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
29	Registratieprocedure	Thema Toegangsbeveiliging	U.01	Ja	Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd om toewijzing van	BIO 2019: 9.2.1 BIO2.0-opmaat: 5.16

					toegangsrechten mogelijk te maken.	
30	Toegangsverlenings procedure	Thema Toegangsbeveiliging	U.02	Ja	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle type gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	BIO 2019: 9.2.2 BIO2.0-opmaat: 5.18
31	O-maatregel. Gebruikers toegang verlenen	BIO 2019	9.2.2.3	Ja	Er is een actueel mandaatregister of er zijn functieprofielen waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten.	Direct op BIO 2019 gebaseerd
32	Inlogprocedure	Thema Toegangsbeveiliging	U.03	Ja	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	BIO 2019: 9.4.2 BIO2.0-opmaat: 8.5
33	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

34	Autorisatieproces	Thema Toegangsbeveiliging	U.04		Een formeel autorisatieproces dient geïmplementeerd te zijn voor het beheersen van de toegangsrechten van alle medewerkers en externe gebruikers tot informatie en informatieverwerken de faciliteiten.	SoGP 2018: SA1.2.1
35	Wachtwoordenbeheer	Thema Toegangsbeveiliging	U.05	Ja	De toewijzing en het beheer van authenticatie-informatie behoort te worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	BIO2.0-opmaat: 5.17 BIO 2019: 9.3.1, 9.4.3
36	O-maatregel. Geheime authenticatie-informatie gebruiken	BIO 2019	9.3.1.1	Ja	Medewerkers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkluis.	Direct op BIO 2019 gebaseerd
37	O-maatregel. Systeem voor wachtwoordbeheer	BIO 2019	9.4.3.2	Ja	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd (zie ook 9.4.2.1.).	Direct op BIO 2019 gebaseerd
38	O-maatregel. Systeem voor wachtwoordbeheer	BIO 2019	9.4.3.3	Ja	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Direct op BIO 2019 gebaseerd

39	O-maatregel. Systeem voor wachtwoordbeheer	BIO 2019	9.4.3.4	Ja	Initiële wachtwoorden en wachtwoorden die gereset zijn, hebben een maximale geldigheidsduur van een werkdag en moeten bij het eerste gebruik worden gewijzigd.	Direct op BIO 2019 gebaseerd
40	O-maatregel. Systeem voor wachtwoordbeheer	BIO 2019	9.4.3.5	Ja	Wachtwoorden die voldoen aan het wachtwoordbeleid hebben een maximale geldigheidsduur van een jaar. Daar waar het beleid niet toepasbaar is, geldt een maximale geldigheidsduur van 6 maanden.	Direct op BIO 2019 gebaseerd
41	Speciale toegangsrechtenbeheer	Thema Toegangsbeveiliging	U.06	Ja	Het toewijzen en het gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	BIO 2019: 9.2.3, 9.4.1 BIO2.0-opmaat: 8.2
42	O-maatregel. Beheren van speciale toegangsrechten	BIO 2019	9.2.3.1	Ja	De uitgegeven speciale bevoegdheden worden minimaal ieder kwartaal beoordeeld.	Direct op BIO 2019 gebaseerd
43	O-maatregel. Beperking toegang tot informatie	BIO 2019	9.4.1.1	Ja	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Direct op BIO 2019 gebaseerd
44	O-maatregel. Beperking toegang tot informatie	BIO 2019	9.4.1.2	Ja	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Direct op BIO 2019 gebaseerd

Energie Diensten Centrum

45	Autorisatie	Thema Toegangsbeveiliging	U.09	Ja	Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbeleid.	BIO 2019: 9.4.1 BIO2.0-opmaat: 8.3
46	O-maatregel. Beperking toegang tot informatie	BIO 2019	9.4.1.1	Ja	Er zijn maatregelen genomen die het fysiek en/of logisch isoleren van informatie met specifiek belang waarborgen.	Direct op BIO 2019 gebaseerd
47	O-maatregel. Beperking toegang tot informatie	BIO 2019	9.4.1.2	Ja	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.	Direct op BIO 2019 gebaseerd
48	Autorisatievoorzieningen	Thema Toegangsbeveiliging	U.10		Voor autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen beschikbaar zijn, zoals: een personeelsregistratiesysteem, een autorisatiebeheersysteem en autorisatiefaciliteiten.	CIP-netwerk
49	Fysieke toegangsbeveiliging	Thema Toegangsbeveiliging	U.11	Ja	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging.	BIO 2019: 11.1.2BIO2.0-opmaat: 7.2

Energie Diensten Centrum

50	Fysieke toegangsbeveiliging	BIO 2019	11.1.2.1	Ja	In geval van concrete beveiligingsrisico's worden waarschuwingen, conform onderlinge afspraken, verzonden aan de relevante collega's binnen het beveiligingsdomein van de overheid.	Direct op BIO 2019 gebaseerd
51	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
52	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
53	Toegang op taakniveau	Privacy-supplement Toegangsbeveiliging	TBV P.03		Het verlenen van toegang tot persoonsgegevens wordt beperkt op	CIP-netwerk, Wpg: Art 6 lid

					basis van duidelijke en afgebakende taken en het doel en de verstrekte toegang is toetsbaar.	1 t/m 6 Art 6a
54	Logging en monitoring uitgeven toegangsrechten	Privacy-supplement Toegangsbeveiliging	TBV P.04		De verwerking behoort op verwerkers/persoons niveau 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
55	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
56	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
57	IT-functionaliteit	Thema Clouddiensten	B.07		IT-functionaliteiten behoren te worden verleend vanuit een robuuste en	SoGP 2018: BC1.3

					beveiligde systeemketen van de CSP naar de CSC.	
58	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
59	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
60	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.
61	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	CIP-netwerk

Energie Diensten Centrum

					zijn en periodiek worden getest.	
6 2	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
6 3	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.
6 4	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
6 5	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
6 6	Scheiding dienstverlening	Thema Clouddiensten	U.08		De cloud-infrastructuur is zodanig ingericht dat de dienstverlening	CIP-netwerk

					aan gebruikers van informatiediensten zijn gescheiden.	
67	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.
68	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.
69	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.
70	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	Direct op BIO 2019 gebaseerd

					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.	
7 1	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
7 2	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
7 3	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
7 4	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.

75	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
76	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
77	O-maatregel. Beveiliging van netwerkdiensten	BIO 2019	13.1.2.3	Ja	Bij draadloze verbindingen zoals wifi en bij bedrade verbindingen buiten het gecontroleerd	Direct op BIO 2019 gebaseerd

					gebied wordt gebruik gemaakt van encryptiemiddelen waarvoor het NBV een positief inzetadvies heeft afgegeven.	
78	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
79	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.
80	O-maatregel. Gebeurtenissen registreren	BIO 2019	12.4.1.3	Ja	De informatieverwerken de 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	Direct op BIO 2019 gebaseerd

					gegevens en informatiesystemen, zodat aanvallen kunnen worden gedetecteerd.	
81	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
82	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
83	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

84	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
85	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
86	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	CIP De Privacy Baseline 2020: U.05, AVG: art. 14, AVG: overweging 60, Wpg: Art 24a lid 1 t/m 4, art 24b

					bijzondere persoonsgegevens.	
87	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
88	Logging met applicaties	Privacy-supplement SSD	SSD P.05		De applicatie behoort op verwerkers/persoons niveau 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
89	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
90	Generalisatie binnen applicaties	Privacy-supplement SSD	SSD P.07		De applicatie behoort, indien de functionele eisen aan	ENISA strategie

					de applicatie van de opdrachtgever dit toelaten, gegeneraliseerde gegevens te gebruiken.	(January 12, 2015) 'generaliseren'
91	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'
92	Verbergen binnen applicaties	Privacy-supplement SSD	SSD P.09		Een applicatie, en iedere Functie binnen deze applicatie, heeft een duidelijk omschreven verwerkingsdoel, zodat bij iedere doorgifte, verwerking door de applicatie en verwerking binnen een taak alleen de daarvoor noodzakelijke persoonsgegevens worden doorgegeven of zijn in te zien, waarbij de andere persoonsgegevens verborgen blijven door het toepassen van versleuteling van de opslagvoorzieningen, de transportpaden en de middleware. Het implementatiemodel is getoetst.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'

93	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
94	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'
95	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'
96	Scheiden binnen communicatievoorzieningen	Privacy-supplement Communicatie voorzieningen	CVZ P.01		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het	NEN 7510 2017: A.12.3.1,

					netwerk de instellingen gebruiken, waarbij de scheiding van verwerkingen het uitgangspunt is.	ENISA strategie (January 12, 2015) 'scheiden'
97	Verbergen binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.02		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij het verbergen van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'verbergen'
98	Logging binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.03		De logging en monitoring van het netwerk behoort op verwerkers/persoons niveau 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
99	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

100	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
101	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
102	Logging en monitoring uitgeven toegangsrechten	Privacy-supplement Toegangsbeveiliging	TBV P.04		De verwerking behoort op verwerkers/persoons niveau 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
103	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	ISO 27002 2017: 11.1, ABDO 2019 v1.1: 3.1.2, Wpg:

					medewerkers met noodzakelijk belang toegang hebben tot en zich bevinden in deze omgevingen; de toegang wordt geregistreerd.	Art 6 lid 1 t/m 6 Art 6a