

Bijlage B – Informatiebeveiligingseisen ICO Wizard – Programma van Eisen	
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.
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 IV	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.
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-BBNz 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.

SPECIFIEKE EISEN

Thema	Discipline	Eis
Certificering, normen(kaders), rapportages	Informatie-veiligheid	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	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 gemeente.
Certificering, normen(kaders), rapportages	Informatie-veiligheid	Leverancier laat jaarlijks, voor zijn gedeelte van de DigiD normen, door een Register EDP-auditor (RE-auditor) een DigiD assessment uit voeren en stelt dit uiterlijk 1 november van het jaar ter beschikking aan opdrachtgever in de vorm van een Third Party Memorandum (TPM).
Certificering, normen(kaders), rapportages	Informatie-veiligheid	Wanneer de leverancier voor de aangeboden ICT Prestatie niet kan voldoen aan eis 2 en/of 3 dan dient de leverancier gelijkwaardigheid aan te tonen. De Gemeente 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.
Certificering, normen(kaders), rapportages	Informatie-veiligheid	Leverancier levert kosteloos een jaarlijkse Third Party Mededeling (TPM)-verklaring van een onafhankelijke RE-auditor aan de opdrachtgever ten behoeve van het jaarlijkse ICT- Beveiligingsassessment DigiD.

Authenticatie van gebruikers en systemen	Informatie-veiligheid	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	Indien authenticatie vanwege zwaarwegende 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	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.
Autorisaties van gebruikers en systemen	Informatie-veiligheid	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	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	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	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	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 blijvend moeten voldoen aan een 100% score op internet.nl , zowel voor de ICT Prestatie als voor de domeinnamen die het gebruikt.
Veilige verwerking	Informatie- veiligheid	Beveiligingseisen opgelegd aan de leverancier gelden onverminderd ook voor onderaannemers of partijen in de toeleveringsketen van de aanbestede dienst.
Data backup recovery	Informatie- veiligheid	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.
Beschikbaarheid garanderen	Informatie- veiligheid	Voor het uitvoeren van de ICT Prestatie heeft leverancier geautomatiseerde maatregelen getroffen waardoor de impact van een DDOS aanval wordt geminimaliseerd.
Segmentatie	Informatie- veiligheid	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	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-identificer ongeldig gemaakt.
Sessiemanagement	Informatie- veiligheid	De ICT-prestatie beschikt over een timeout van maximaal 15 minuten voor actieve sessies.
Sleutelbeheer	Informatie- veiligheid	Indien het cryptografische sleutelbeheer voor de ICT Prestatie niet bij de hoofdaannemer of opdrachtgever is belegd, dient u dit voorafgaand aan ingebruikname van de ICT Prestatie te melden bij opdrachtgever, waarbij inzage wordt gegeven welke derde partij het sleutelbeheer uitvoert.
Backup	Informatie- veiligheid	De ICT Prestatie heeft een backup en disaster recovery procedure gedocumenteerd en test deze periodiek op werking.

Monitoring, audit, logging	Informatie-veiligheid	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 Gemeente 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	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	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	In geval van een (vermoed) informatiebeveiligingsincident is de bewaartermijn van de gelogde incidentinformatie minimaal drie jaar.

Monitoring, audit, logging	Informatie-veiligheid	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	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	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	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	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. Zie Handreiking hardening beleid https://www.informatiebeveiligingsdienst.nl/product/hardening-beleid-voor-gemeenten/

Testen	Informatie- veiligheid	Het systeem wordt periodiek gescand op kwetsbaarheden en er wordt 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	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	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	De ICT-prestatie is voorzien van de laatste (beveiligings)patches en deze worden volgens een patchmanagement proces doorgevoerd.

ICO WIZARD EISEN

Nr. eis	Naam Eis	Referentie bron-document:	Referentie code norm:	BIO-O-maatregel:	Samenvatting eis:	Gebaseerd op: (ISO27002-paragraaf, of ander framework)
E1	Bedrijfs- en beveiligings-functies	Thema Software-pakketten	B.04		De noodzakelijke bedrijfs- en beveiligingsfuncties binnen het veranderingsgebied behoren te worden vastgesteld met organisatorische en technisch uitgangspunten.	CIP-netwerk
E2	Cryptografie	Thema Software-pakketten	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.
E3	O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaat-regelen	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

E4	O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaat-regelen	BIO 2019	10.1.1.2	Ja	Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd
E5	Beperkingen wijziging softwarepakket	Thema Software-pakketten	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.
E6	Bedrijfscontinuïteit	Thema Software-pakketten	U.03		De leverancier behoort processen, procedures en beheersmaatregelen te documenteren, te implementeren en te handhaven.	BIO 2019: 17.1.2.
E7	Input-/output-validatie	Thema Software-pakketten	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
E8	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
E9	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.

E10	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
E11	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
E12	Toegangsauto-risatie	Thema Software-pakketten	U.09		Het softwarepakket behoort een autorisatiemechanisme te bieden.	SSD 2020: SSD-8
E13	Autorisatiebe-heer	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
E14	Logging	Thema Software-pakketten	U.11		Het softwarepakket biedt signaleringsfuncties voor registratie en detectie die beveiligd zijn ingericht.	SSD 2020: SSD-30
E15	Application Programming Interface (API)	Thema Software-pakketten	U.12		Softwarepakketten behoren veilige API's te gebruiken voor import en export van gegevens.	OWASP ASVS 2020: V13
E16	Gegevensimport	Thema Software-pakketten	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

E17	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
E18	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
E19	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
E20	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

E21	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
E22	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
E23	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'
E24	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'

E25	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'
E26	Standaarden voor serverconfiguratie	Thema Server-platform	U.02		Het serverplatform is geconfigureerd volgens gedocumenteerde standaarden.	SoGP 2018: SY1.2
E27	Malwareprotectie	Thema Server-platform	U.03	Ja	Ter bescherming tegen malware behoren beheersmaatregelen voor preventie, detectie en herstel te worden geïmplementeerd, in combinatie met het stimuleren van een passend bewustzijn van gebruikers.	BIO 2019: 12.2.1.
E28	Beheer op afstand	Thema Server-platform	U.06		Richtlijnen en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.	BIO 2019: 6.2.2.

E29	Verwijderen of hergebruiken serverapparatuur	Thema Server-platform	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.
E30	Hardenen server	Thema Server-platform	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
E31	Serverconfiguratie	Thema Server-platform	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
E32	Virtualisatie serverplatform	Thema Server-platform	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
E33	Beperking van software- installatie	Thema Server--platform	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.

E34	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
E35	Kloksynchro-nisatie	Thema Server-platform	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.
E36	Logbestanden beheerders	Thema Server-platform	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.
E37	Logging	Thema Server-platform	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.

E38	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
E39	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
E40	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

E41	Dataminimalisatie door serverplatformen	Privacy-supplement Server-platform	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
E42	Scheiden door serverplatformen	Privacy-supplement Server-platform	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'
E43	Verbergen door serverplatformen	Privacy-supplement Server-platform	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'
E44	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 BIO2.0-opmaat: 8.5
E45	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

E46	Beveiliging van netwerkdiensten	Thema Communi- catievoor- zieningen	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 BIO2.0- opmaat: 8.21
E47	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
E48	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

E49	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
E50	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 BIO2.0-opmaat: 8.22
E51	O-maatregel. Scheiding in netwerken	BIO 2019	13.1.3.1	Ja	Alle gescheiden groepen hebben een gedefinieerd beveiligingsniveau.	Direct op BIO 2019 gebaseerd
E52	Elektronische berichten	Thema Communicatievoorzieningen	U.07	Ja	Informatie die is opgenomen in elektronische berichten behoort passend te zijn beschermd.	BIO 2019: 13.2.3 BIO2.0-opmaat: 5.14
E53	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
E54	O-maatregel. Elektronische berichten	BIO 2019	13.2.3.3	Ja	Maak gebruik van PKI-overheid-certificaten bij web- en mailverkeer van gevoelige gegevens. Gevoelige gegevens zijn onder andere digitale documenten binnen de overheid waar gebruikers rechten aan kunnen ontleen.	Direct op BIO 2019 gebaseerd

E55	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 gemaakt van de AdES Baseline Profile standaard.	Direct op BIO 2019 gebaseerd
E56	Toepassingen via openbare netwerken	Thema Communi- catievoor- zieningen	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 BIO2.0-opmaat: 8.26
E57	Gateways en firewalls	Thema Communi- catievoor- zieningen	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
E58	Virtual Private Networks	Thema Communi- catievoor- zieningen	U.10		Een VPN behoort een strikt gescheiden end-to-end-connectie te geven, waarbij de getransporteerde informatie, is voorbehouden aan tot de organisatie die de VPN gebruikt.	ISO 27033-5 2013: 6.1
E59	Cryptografische services	Thema Communi- catievoor- zieningen	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 BIO2.0-opmaat: 8.31

E60	Draadloze toegang	Thema Communi- catievoor- zieningen	U.12		Draadloos verkeer behoort te worden beveiligd met authenticatie van devices, autorisatie van gebruikers en versleuteling van de communicatie.	CIP- netwerk
E61	Netwerk- authenticatie	Thema Communi- catievoor- zieningen	U.14		Authenticatie van netwerkknooppunten behoort te worden toegepast om onbevoegd aansluiten van netwerkdevices (sniffing) te voorkomen.	CIP- netwerk
E62	Logging en monitoring	Thema Communi- catievoor- zieningen	U.16	Ja	Netwerken behoren te worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden getroffen om potentiële informatiebeveiligingsinci- denten te evalueren; logbestanden worden geregistreerd en bewaard.	BIO 2019: 12.4.1 BIO2.o- opmaat: 8.16
E63	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 gebaseer d

E64	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
E65	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
E66	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
E67	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'

E68	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'
E69	Logging binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.03		De logging en monitoring van het netwerk behoort op verwerkers/persoonsniveau te worden toegepast, 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
E70	Service Level Management	Thema Huisvesting-IV	B.06		Het management van huisvesting IV behoort diensten te leveren volgens een Diensten Niveauovereenkomst (DNO).	CIP-netwerk
E71	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 BIO2.0-opmaat: 7.5
E72	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 BIO2.0-opmaat: 7.1
E73	Beveiligingsfaciliteiten	Thema Huisvesting-IV	U.04	Ja	Voor het beveiligen van ruimten behoren faciliteiten te worden ontworpen en toegepast.	BIO 2019: 11.1.3 BIO2.0-opmaat: 7.3

E74	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 BIO2.0-opmaat: 7.11
E75	Apparatuur-positionering	Thema Huisvesting-IV	U.06	Ja	Apparatuur behoort effectief te worden geplaatst en beschermd.	BIO 2019: 11.2.1, 11.2.9 BIO2.0-opmaat: 7.8
E76	O-maatregel. 'Clear desk'- en 'clear screen'-beleid	BIO 2019	11.2.9.1	Ja	Een onbemende werkplek is altijd vergrendeld.	Direct op BIO 2019 gebaseerd
E77	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
E78	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
E79	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 sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.	Direct op BIO 2019 gebaseerd
E80	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

E81	Apparatuur- onderhoud	Thema Huisvesting-IV	U.07		Apparatuur behoort op een correcte wijze te worden onderhouden.	BIO 2019: 11.2.4 BIO2.0- opmaat: 7.13
E82	Apparatuur- verwijdering	Thema Huisvesting-IV	U.08	Ja	Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software vooraftgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	BIO 2019: 11.2.7 BIO2.0- opmaat: 7.14
E83	Verwijderen van media	BIO 2019	8.3.2.2	Ja	Verwijdering vindt plaats op een veilige manier, bijvoorbeeld door verbranding of versnippering. Verwijdering van alleen gegevens is ook mogelijk door het wissen van de gegevens voordat de media worden gebruikt voor een andere toepassing in de organisatie (ISO 27002 – implementatierichtlijn 8.3.2.a).	Direct op BIO 2019 gebaseer d
E84	Verwijderen van media	BIO 2019	8.3.2.3	Ja	Voor het wissen van alle data op het medium, wordt de data onherstelbaar verwijderd, bijvoorbeeld door minimaal twee keer te overschrijven met vaste data en één keer met random data. Er wordt gecontroleerd of alle data onherstelbaar verwijderd is.	Direct op BIO 2019 gebaseer d

E85	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 BIO2.0-opmaat: 7.10
E86	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 BIO2.0-opmaat: 7.2
E87	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 BIO2.0-opmaat: 7.12
E88	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
E89	Cryptografie	Thema Toegangs-beveiliging	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

Ego	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
Eg1	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
Eg2	Registratieprocedure	Thema Toegangsbeveiliging	U.01	Ja	Een formele registratie- en afmeldprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	BIO 2019: 9.2.1 BIO2.0-opmaat: 5.16
Eg3	Toegangsverleningsprocedure	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

Eg4	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 gebaseer d
Eg5	Inlogprocedure	Thema Toegangs- beveiliging	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
Eg6	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 gebaseer d
Eg7	Autorisatie-proces	Thema Toegangs- beveiliging	U.04		Een formeel autorisatieproces dient geïmplementeerd te zijn voor het beheersen van de toegangsrechten van de medewerkers en externe gebruikers tot informatie en informatieverwerkende faciliteiten.	SoGP 2018: SA1.2.1
Eg8	Wachtwoorden- beheer	Thema Toegangs- beveiliging	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

E99	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
E100	O-maatregel. Systeem voor wachtwoord-beheer	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
E101	O-maatregel. Systeem voor wachtwoord-beheer	BIO 2019	9.4.3.3	Ja	De eisen aan wachtwoorden moeten geautomatiseerd worden afgedwongen.	Direct op BIO 2019 gebaseerd
E102	O-maatregel. Systeem voor wachtwoord-beheer	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
E103	O-maatregel. Systeem voor wachtwoord-beheer	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
E104	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
E105	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

E106	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 gebaseer d
E107	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 gebaseer d
E108	Autorisatie	Thema Toegangs- beveiliging	U.09	Ja	Toegang (autorisatie) tot informatie en systeemfuncties van toepassingen behoren te worden beperkt in overeenstemming met het toegangsbeveiligingsbelei d.	BIO 2019: 9.4.1 BIO2.0- opmaat: 8.3
E109	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 gebaseer d
E110	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 gebaseer d
E111	Autorisatie- voorzieningen	Thema Toegangs- beveiliging	U.10		Voor autorisatiebeheer moeten binnen de daartoe in aanmerking komende applicaties technische autorisatievoorzieningen beschikbaar zijn, zoals: een personeelsregistratiesyste em, een autorisatiebeheersysteem en autorisatiefaciliteiten.	CIP- netwerk
E112	Fysieke toegangs- beveiliging	Thema Toegangs- beveiliging	U.11	Ja	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging.	BIO 2019: 11.1.2 BIO2.0- opmaat: 7.2

E113	Fysieke toegangs-beveiliging	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
E114	Het stelsel van toegangsbeheer	Privacy-supplement Toegangs-beveiliging	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 monitoring plaats.	AVG: art. 5, Wpg Art 6 lid 1 t/m 6 Art 6a
E115	Doelbinding op rolniveau	Privacy-supplement Toegangs-beveiliging	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
E116	Toegang op taakniveau	Privacy-supplement Toegangs-beveiliging	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

E117	Logging en monitoring uitgeven toegangsrechten	Privacy-supplement Toegangs-beveiliging	TBV P.04		De verwerking behoort op verwerkers/persoonsniveau te worden gelogd, 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
E118	Toegang tot fysieke omgevingen	Privacy-supplement Toegangs-beveiliging	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
E119	Transparantie	Thema Cloud-diensten	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
E120	IT-functionaliteit	Thema Cloud-diensten	B.07		IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.	SoGP 2018: BC1.3

E121	Privacy en bescherming persoons-gegevens	Thema Cloud-diensten	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/labels, eigenaarschap en locatie.	ITU-T FG Cloud TR Part 5 2012: 8.5
E122	Clouddienstenarchitectuur	Thema Cloud-diensten	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
E123	Bedrijfscontinuïteitsservices	Thema Cloud-diensten	U.03		Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.	BIO 2019: 17.2.1.
E124	Herstelfunctie voor data en clouddiensten	Thema Cloud-diensten	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
E125	Dataproductie	Thema Cloud-diensten	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

E126	Dataretentie en gegevens-vernietiging	Thema Cloud-diensten	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.
E127	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
E128	Datascheiding	Thema Cloud-diensten	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
E129	Scheiding dienstverlening	Thema Cloud-diensten	U.08		De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.	CIP-netwerk
E130	Malware-protectie	Thema Cloud-diensten	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.
E131	Toegang IT-diensten en data	Thema Cloud-diensten	U.10	Ja	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.	BIO 2019: 9.1.2.

E132	Cryptoservices	Thema Cloud-diensten	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.
E133	O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaat-regelen	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
E134	O-maatregel. Beleid inzake het gebruik van cryptografische beheersmaat-regelen	BIO 2019	10.1.1.2	Ja	Cryptografische toepassingen voldoen aan passende standaarden.	Direct op BIO 2019 gebaseerd
E135	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

E136	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
E137	Koppelvlakken	Thema Cloud-diensten	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.
E138	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
E139	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

E140	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
E141	Interoperabiliteit en portabiliteit	Thema Cloud-diensten	U.14		Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende IT-platforms 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
E142	Logging en monitoring	Thema Cloud-diensten	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.
E143	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

E144	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
E145	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
E146	Multi-tenant architectuur	Thema Cloud-diensten	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
E147	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

E148	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
E149	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
E150	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
E151	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

E152	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
E153	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'
E154	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'

E155	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'
E156	Dataminimalisatie Dataminimalisatie door serverplatformen	Privacy-supplement Server-platform	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
E157	Scheiden door serverplatformen	Privacy-supplement Server-platform	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'

E158	Verbergen door serverplatformen	Privacy-supplement Server-platform	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'
E159	Scheiden binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.01		De organisatie heeft een proces ingericht, zodat bij de configuratie van (onderdelen van) het netwerk de instellingen gebruiken, waarbij de scheiding van verwerkingen het uitgangspunt is.	NEN 7510 2017: A.12.3.1, ENISA strategie (January 12, 2015) 'scheiden'
E160	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'
E161	Logging binnen communicatievoorzieningen	Privacy-supplement Communicatievoorzieningen	CVZ P.03		De logging en monitoring van het netwerk behoort op werkers/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
E162	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 monitoring plaats.	AVG: art. 5, Wpg Art 6 lid 1 t/m 6 Art 6a

E163	Doelbinding op rolniveau	Privacy-supplement Toegangs-beveiliging	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
E164	Toegang op taakniveau	Privacy-supplement Toegangs-beveiliging	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
E165	Logging en monitoring uitgeven toegangsrechten	Privacy-supplement Toegangs-beveiliging	TBV P.04		De verwerking behoort op verwerkers/persoonsniveau te worden gelogd, 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
E166	Toegang tot fysieke omgevingen	Privacy-supplement Toegangs-beveiliging	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