PROVINCIE FLEVOLAND

Cybersecurity Overheid

Europese aanbesteding met betrekking tot Housing en hosting van ICT-middelen van de Provincie Flevoland.
PFL - 3225631

Datum : 20-9-2024

INHOUDSOPGAVE

1 Voorwoord

De steeds toenemende digitalisering en daarin meekomende risico's op diefstal en misbruik van gegevens maakt het noodzakelijk om voortdurend te blijven werken aan informatieveiligheid. De overheid hanteert daarbij als gezamenlijk kader de Baseline Informatiebeveiliging Overheid (BIO). Naast maatregelen die de organisaties zelf betreffen, moeten ook inkopen en uitbestedingen voldoen aan veiligheidseisen.

De overheid wil met haar inkoopbeleid de vraag naar digitaal veilige ICT-producten en diensten stimuleren. In de eerste plaats omdat zij zelf veilig moet zijn, maar ook kan zij als belangrijke gebruiker van ICT-diensten bredere impact creëren. Door cybersecuritycriteria op te nemen in aanbestedingen, inkopen en contracten wil de overheid nadrukkelijk sturen op de veiligheid van haar eigen uitbestedingen en daarnaast een proces stimuleren dat leidt tot een algemene verhoging van de veiligheid van ICT-middelen in de markt.

Dit rapport geeft de veiligheidseisen weer van een of meer opgegeven inkooponderdelen. Deze eisen zijn gericht op basisbeveiligingsniveaus (BBN) 1 en 2 van de BIO. Hogere beveiligingsniveaus zijn altijd maatwerk. Het gebruik van de ICO-hulpmiddelen is geen substituut voor eigen risicoafweging.

Op basis van risicoafwegingen van de behoeftesteller kunnen eisen worden geschrapt, verzacht of verzwaard. Dit blijkt uit de eventueel bij de eisen gemaakt opmerkingen.

2 Eisen voor Cybersecurity Overheid

De eisen in dit hoofdstuk zijn gebaseerd op de BIO en onderliggende uitwerkingen. Afhankelijk van de gemaakte selecties zijn ook eisen opgenomen die gebaseerd zijn op andere normenkaders, zoals CSIR, ABDO en Privacy-supplementen.

Bij de eisen is aangegeven uit welk brondocument deze afkomstig zijn en onder welke codes ze daarin voorkomen.

2.1 Cybersecurity Criteria

ID	Onderwerp	Criteria
1	Inkooponderdelen	Clouddiensten & Serverplatform
2	Proceseis	Ja
3	Producteis	Ja
4	Eis voor Opdrachtgever	Nee
5	Eis voor Opdrachtnemer	Ja
6	Schaalgrootte gerelateerde eisen specificeren.	Ja
7	Basispakket	Ja
8	Privacy gerelateerde eisen specificeren.	Nee
9	Toon BIO-O maatregelen BBN1	Nee
10	Toon BIO-O maatregelen BBN2	Nee
11	Toon ABDO-eisen TBB4	Nee
12	Toon ABDO-eisen TBB3	Nee
13	Toon ABDO-eisen TBB2	Nee
14	Toon ABDO-eisen TBB1	Nee
15	Aantal geselecteerde eisen	57

2.2 Geselecteerde Cybersecurity Eisen

Beleid voor beveiligde inrichting en onderhoud	
Referentie code norm:	B.01 (Beleid)
Referentie brondocument:	Thema Serverplatform
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	
Samenvatting eis:	Voor het beveiligd inrichten en onderhouden van het serverplatform behoren regels te worden vastgesteld en binnen de organisatie te worden toegepast.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.
Toelichting:	

Inrichtingsprincipes voor serverplatform	
Referentie code norm:	B.02 (Beleid)
Referentie brondocument:	Thema Serverplatform
BIO-BBN:	Ja
Samenvatting eis:	Principes voor het inrichten van beveiligde servers behoren te worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het inrichten van servers.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Serverplatform-architectuur	
Referentie code norm:	B.03 (Beleid)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	De functionele eisen, beveiligingseisen en architectuurvoorschriften van het serverplatform zijn in samenhang in een architectuurdocument vastgelegd.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Bedieningsprocedure	
Referentie code norm:	U.01 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.
Verificatie methode(n):	Overleg bewijsstukken.

Standaarden voor serverconfiguratie	
Referentie code norm:	U.02 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Het serverplatform is geconfigureerd volgens gedocumenteerde standaarden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Malwareprotectie	
Referentie code norm:	U.03 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
BIO-BBN:	Ja
Samenvatting eis:	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.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Technische kwetsbaarhedenbeheer	
Referentie code norm:	U.04 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	STIX en TAXII (uitwisseling van cyberdreigingsinformatie)
Samenvatting eis:	Informatie over technische serverkwetsbaarheden[1] behoort tijdig te worden verkregen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden dient te worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Patchmanagement	
Referentie code norm:	U.05 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Patchmanagement is procesmatig en procedureel opgezet en wordt ondersteund door richtlijnen zodat het zodanig kan worden uitgevoerd dat op de servers de laatste (beveiligings)patches tijdig zijn geïnstalleerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Beheer op afstand	
Referentie code norm:	U.06 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Richtlijnen en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van beheer op afstand van servers.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Server-onderhoud	
Referentie code norm:	U.07 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Servers behoren correct te worden onderhouden om de continue beschikbaarheid en integriteit te waarborgen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Verwijderen of hergebruiken serverapparatuur	
Referentie code norm:	U.08 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	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.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Hardenen server	
Referentie code norm:	U.09 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Voor het beveiligen van een server worden overbodige functies en ongeoorloofde toegang uitgeschakeld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Serverconfiguratie	
Referentie code norm:	U.10 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Serverplatforms behoren zo geconfigureerd te zijn, dat zij functioneren zoals het vereist is en zijn beschermd tegen ongeautoriseerd en incorrecte updates.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Virtualisatie serverplatform	
Referentie code norm:	U.11 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	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.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Beperking van software- installatie	
Referentie code norm:	U.12 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
BIO-BBN:	Ja
Samenvatting eis:	Voor het door gebruikers (beheerders) installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Kloksynchronisatie	
Referentie code norm:	U.13 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein behoren te worden gedocumenteerd en gesynchroniseerd met één referentietijdbron.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Ontwerpdocument	
Referentie code norm:	U.14 (Uitvoering)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Het ontwerp van een serverplatform behoort te zijn gedocumenteerd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Evaluatierichtlijn servers en serverplatforms	
Referentie code norm:	C.01 (Controle)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Richtlijnen behoren te worden vastgesteld om de implementatie en beveiliging van servers en besturingssystemen te controleren waarbij de bevindingen tijdig aan het management worden gerapporteerd.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Beoordeling technische serveromgeving	
Referentie code norm:	C.02 (Controle)
Referentie brondocument:	Thema Serverplatform
BIO-BBN:	Ja
Samenvatting eis:	Technische serveromgevingen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor servers en besturingssystemen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Logbestanden beheerders	
Referentie code norm:	C.03 (Controle)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Activiteiten van systeembeheerders en -operators behoren te worden vastgelegd en de logbestanden behoren te worden beschermd en regelmatig te worden beoordeeld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Logging	
Referentie code norm:	C.04 (Controle)
Referentie brondocument:	Thema Serverplatform
BIO-BBN:	Ja
Samenvatting eis:	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Monitoring	
Referentie code norm:	C.05 (Controle)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	De organisatie reviewt/analyseert regelmatig de logbestanden om onjuist gebruik en verdachte activiteiten op servers en besturingssystemen vast te stellen en bevindingen aan het management te rapporteren.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Beheerorganisatie servers en serverplatforms	
Referentie code norm:	C.06 (Controle)
Referentie brondocument:	Thema Serverplatform
Samenvatting eis:	Binnen de beheerorganisatie is een beveiligingsfunctionaris benoemd die de organisatie ondersteunt in de vorm van het bewaken van beveiligingsbeleid en die inzicht verschaft in de inrichting van de servers en het serverplatform.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Wet en Regelgeving	
Referentie code norm:	B.01 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	Alle relevante wettelijke, statutaire, regelgevende, contractuele eisen en de aanpak van de CSP om aan deze eisen te voldoen behoren voor elke clouddienst en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Cloudbeveiligingsstrategie	
Referentie code norm:	B.02 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP behoort een cloud-beveiligingsstrategie te hebben ontwikkeld die samenhangt met de strategische doelstelling van de CSP en die aantoonbaar de informatieveiligheid ondersteunt.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Exit-strategie	
Referentie code norm:	B.03 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	In de clouddienstenovereenkomst tussen de CSP en CSC behoort een exitstrategie te zijn opgenomen waarbij zowel een aantal bepalingen6 over exit zijn opgenomen, als een aantal condities6 die aanleiding kunnen geven tot een exit.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Clouddienstenbeleid	
Referentie code norm:	B.04 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP behoort haar informatiebeveiligingsbeleid uit te breiden met een cloud-beveiligingsbeleid om de voorzieningen en het gebruik van cloudservices te adresseren.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Transparantie	
Referentie code norm:	B.05 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	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.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Risicomanagement	
Referentie code norm:	B.06 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP behoort de organisatie en verantwoordelijkheden voor het risicomanagementproces voor de beveiliging van clouddiensten te hebben opgezet en onderhouden.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

IT-functionaliteit	
Referentie code norm:	B.07 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	IT-functionaliteiten behoren te worden verleend vanuit een robuuste en beveiligde systeemketen van de CSP naar de CSC.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Bedrijfscontinuïteitsmanagement	
Referentie code norm:	B.08 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP behoort haar BCM-proces adequaat te hebben georganiseerd, waarbij de volgende aspecten zijn geadresseerd: verantwoordelijkheid voor BCM, beleid en procedures, bedrijfscontinuïteitsplanning, verificatie en updaten en computercentra.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Privacy en bescherming persoonsgegevens	
Referentie code norm:	B.09 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	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.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Beveiligingsorganisatie	
Referentie code norm:	B.10 (Beleid)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Samenvatting eis:	De CSP behoort een beveiligingsfunctie te hebben benoemd en een beveiligingsorganisatie te hebben ingericht, waarin de organisatorische positie, de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen en de rapportagelijnen zijn vastgesteld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Clouddienstenarchitectuur	
Referentie code norm:	B.11 (Beleid)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP heeft een actuele architectuur vastgelegd die voorziet in een raamwerk voor de onderlinge samenhang en afhankelijkheden van de IT-functionaliteiten.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Standaarden voor clouddiensten	
Referentie code norm:	U.01 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP past aantoonbaar relevante, nationale standaarden en internationale standaarden toe voor de opzet en exploitatie van de diensten en de interactie met de CSC.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Risico-assessment	
Referentie code norm:	U.02 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP behoort een risico-assessment uit te voeren, bestaande uit een risico-analyse en risico-evaluatie met de criteria en de doelstelling voor clouddiensten van de CSP.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Bedrijfscontinuïteitsservices	
Referentie code norm:	U.03 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan continuïteitseisen te voldoen.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Herstelfunctie voor data en clouddiensten	
Referentie code norm:	U.04 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	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.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Dataprotectie	
Referentie code norm:	U.05 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding) * DNSSEC (ondertekende domeinnaam) * STARTTLS en DANE (beveiligde mailserver-verbindingen) * DMARC+DKIM+SPF (anti-mailphishing/-spoofing) * Digikoppeling (beveiligde gegevensuitwisseling tussen systemen)
Samenvatting eis:	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.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Dataretentie en gegevensvernietiging	
Referentie code norm:	U.06 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Samenvatting eis:	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.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Datascheiding	
Referentie code norm:	U.07 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	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.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Scheiding dienstverlening	
Referentie code norm:	U.08 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Malware-protectie	
Referentie code norm:	U.09 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Samenvatting eis:	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Toegang IT-diensten en data	
Referentie code norm:	U.10 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Samenvatting eis:	Gebruikers behoren alleen toegang te krijgen tot IT-diensten en data waarvoor zij specifiek bevoegd zijn.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Cryptoservices	
Referentie code norm:	U.11 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding)
Samenvatting eis:	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
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring. Daarnaast internet.nl.

Koppelvlakken	
Referentie code norm:	U.12 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Samenvatting eis:	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.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Service-orkestratie	
Referentie code norm:	U.13 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	Service-orkestratie biedt coördinatie, aggregatie en samenstelling van de servicecomponenten van de Cloud-service die aan de CSC wordt geleverd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Interoperabiliteit en portabiliteit	
Referentie code norm:	U.14 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Relevante standaard PToLU-lijst Forum Standaardisatie:	* TLS, HTTPS en HSTS (beveiligde verbinding)
Samenvatting eis:	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.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Logging en monitoring	
Referentie code norm:	U.15 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Samenvatting eis:	Logbestanden waarin gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Clouddienstenarchitectuur	
Referentie code norm:	U.16 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De clouddienstenarchitectuur specificeert de samenhang en beveiliging van de services en de interconnectie tussen de CSC en de CSP en biedt transparantie en overzicht van randvoorwaardelijke omgevingsparameters, voor zowel de opzet, de levering en de portabiliteit van CSC-data.
Verificatie methode(n):	Interne controle, Overleg bewijsstukken of Verklaring.

Multi-tenantarchitectuur	
Referentie code norm:	U.17 (Uitvoering)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	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
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Servicemanagementbeleid en evaluatierichtlijn	
Referentie code norm:	C.01 (Controle)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP heeft voor clouddiensten een servicemanagementbeleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Risico-control	
Referentie code norm:	C.02 (Controle)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	Risicomanagement en het risico-assessmentproces behoren continu te worden gemonitord en gereviewd en zo nodig te worden verbeterd.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Compliance en assurance	
Referentie code norm:	C.03 (Controle)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Samenvatting eis:	De CSP behoort regelmatig de naleving van de cloudbeveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een assurance-verklaring aan de CSC uit te brengen en te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Technische kwetsbaarhedenbeheer	
Referentie code norm:	C.04 (Controle)
Referentie brondocument:	Thema Clouddiensten
BIO-BBN:	Ja
Relevante standaard PToLU-lijst Forum Standaardisatie:	STIX en TAXII (Uitwisseling van cyberdreigingsinformatie)
Samenvatting eis:	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden dienen te worden geëvalueerd en passende maatregelen dienen te worden genomen om het risico dat ermee samenhangt aan te pakken.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring. Daarnaast Internet.nl.

Security-monitoringsrapportage	
Referentie code norm:	C.05 (Controle)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De performance van de informatiebeveiliging van de cloud-omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan verschillende stakeholders.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

Beheersorganisatie clouddiensten	
Referentie code norm:	C.06 (Controle)
Referentie brondocument:	Thema Clouddiensten
Samenvatting eis:	De CSP heeft een beheersorganisatie ingericht waarin de processtructuur en de taken, verantwoordelijkheden en bevoegdheden van de betrokken functionarissen zijn vastgesteld.
Verificatie methode(n):	Overleg bewijsstukken en/of Verklaring.

2.3 B-codes m.b.t. thema Clouddiensten

Binnen de NORM BIO (Baseline Informatiebeveiliging Overheid) zijn de B-codes met betrekking tot het thema Clouddiensten bedoeld om de veiligheid en integriteit van gegevens en systemen die in de Cloud worden beheerd te waarborgen. Deze codes behandelen verschillende aspecten van Cloud beveiliging, van toegangscontrole tot compliance en incidentbeheer. B-code staat voor Beleid maatregelen.

B01: Beveiliging van Clouddiensten
Deze code behandelt de algemene beveiliging van clouddiensten. Het richt zich op het waarborgen van de veiligheid van gegevens en systemen die worden opgeslagen en beheerd in de cloud. Dit omvat het toepassen van algemene beveiligingsmaatregelen zoals encryptie, toegangsbeheer, en configuratiebeheer om de vertrouwelijkheid, integriteit, en beschikbaarheid van gegevens te beschermen.

B02: Beheer van Toegang en Identiteit
Code B02 richt zich op het beheer van toegang en identiteit binnen clouddiensten. Het omvat maatregelen voor het beheren van gebruikersidentiteiten en toegangsrechten, zoals het implementeren van multi-factor authenticatie (MFA), role-based access control (RBAC), en het strikt beheren van wachtwoorden en andere authenticatiemiddelen om ongeautoriseerde toegang tot cloudresources te voorkomen.

B03: Compliance en Regelgeving
Deze code behandelt de naleving van wet- en regelgeving bij het gebruik van clouddiensten. Het richt zich op het waarborgen dat cloudoplossingen voldoen aan relevante juridische en regelgevende vereisten, zoals de Algemene Verordening Gegevensbescherming (AVG) en andere nationale en internationale wetgevingen. Dit omvat het evalueren van cloudproviders op naleving en het opstellen van contractuele afspraken om te voldoen aan wettelijke eisen.

B04: Beveiliging van Gegevens in de Cloud
Code B04 richt zich specifiek op de beveiliging van gegevens die in de cloud worden opgeslagen en verwerkt. Het omvat maatregelen zoals data-encryptie, zowel voor gegevens in rust als tijdens overdracht, alsook het beheer van back-ups en gegevensherstel om ervoor te zorgen dat gegevens beschermd zijn tegen verlies, schade, of ongeautoriseerde toegang.

B05: Incidentbeheer en Reactie
Deze code behandelt de procedures en maatregelen voor het beheren van beveiligingsincidenten in de cloud. Het richt zich op het ontwikkelen van incidentresponsplannen, het documenteren en rapporteren van incidenten, en het implementeren van processen voor het reageren op en herstellen van beveiligingsincidenten die cloudomgevingen kunnen beïnvloeden.

B06: Leveranciersbeheer en Contractbeheer
Code B06 richt zich op het beheer van cloudserviceproviders en de contractuele aspecten van het uitbesteden van diensten aan de cloud. Dit omvat het evalueren van de beveiligingsmaatregelen en compliance van cloudproviders, het opstellen en beheren van service level agreements (SLA's), en het vastleggen van verantwoordelijkheden en verplichtingen met betrekking tot beveiliging en gegevensbescherming.

B07: Continuïteit en Herstel
Code B07 behandelt de maatregelen die nodig zijn om de continuïteit van diensten in de cloud te waarborgen en om adequaat te kunnen herstellen in geval van een storing of calamiteit. Dit omvat het ontwikkelen van continuïteitsplannen en herstelstrategieën, het uitvoeren van tests en oefeningen, en het zorgen voor de beschikbaarheid van redundante systemen en back-ups.

B08: Monitoring en Rapportage
Deze code richt zich op het implementeren van monitoring- en rapportagemaatregelen voor clouddiensten. Het omvat het gebruik van monitoringtools om de prestaties en beveiliging van cloudresources te volgen, het bijhouden van logbestanden, en het rapporteren van bevindingen en incidenten aan relevante belanghebbenden om transparantie en proactieve beveiliging te bevorderen.

2.4 C-codes m.b.t. thema Clouddiensten

Binnen het thema Clouddiensten van de NORM BIO (Baseline Informatiebeveiliging Overheid) verwijzen de C-codes naar specifieke maatregelen en richtlijnen die betrekking hebben op de beveiliging en het beheer van clouddiensten. Deze codes helpen overheidsorganisaties bij het waarborgen van de veiligheid, privacy, en integriteit van gegevens die in de Cloud worden opgeslagen en beheerd. C-code staat voor Controlemaatregelen.

C01: Beveiligingsarchitectuur voor Clouddiensten

Deze code richt zich op het ontwerpen en implementeren van een beveiligingsarchitectuur voor clouddiensten. Het omvat het definiëren van de beveiligingsvereisten, het opzetten van een architectuur die deze vereisten adresseert, en het waarborgen van de integratie van beveiligingsmaatregelen in de cloudinfrastructuur. Belangrijke aspecten zijn de bescherming van data, netwerkbeveiliging, en het beveiligen van cloudapplicaties.

C02: Toegangscontrole en Identiteitsbeheer
Code C02 behandelt de maatregelen voor toegangscontrole en identiteitsbeheer binnen cloudomgevingen. Dit omvat het implementeren van beleid voor authenticatie en autorisatie, zoals multi-factor authenticatie (MFA), role-based access control (RBAC), en het beheren van gebruikersidentiteiten en -rechten om ervoor te zorgen dat alleen geautoriseerde gebruikers toegang hebben tot cloudresources en -gegevens.

C03: Gegevensbescherming en Encryptie
Deze code richt zich op de bescherming van gegevens die worden opgeslagen en verwerkt in de cloud. Het omvat het toepassen van encryptie om de vertrouwelijkheid en integriteit van gegevens te waarborgen, zowel voor gegevens in rust als tijdens overdracht. Het richt zich ook op het beheer van cryptografische sleutels en het implementeren van gegevensbeveiligingsmaatregelen die voldoen aan de geldende regelgeving en best practices.

C04: Compliance en Contractuele Afspraken
Code C04 behandelt de naleving van wet- en regelgeving bij het gebruik van clouddiensten en de contractuele afspraken die met cloudserviceproviders moeten worden gemaakt. Dit omvat het zorgen dat cloudoplossingen voldoen aan juridische en regelgevende vereisten zoals de AVG, en het opstellen van contracten en Service Level Agreements (SLA's) die de verantwoordelijkheden en verplichtingen van beide partijen vastleggen.

C05: Incidentbeheer en Respons
Deze code richt zich op het beheren en reageren op beveiligingsincidenten die zich kunnen voordoen binnen cloudomgevingen. Het omvat het ontwikkelen van incidentresponsplannen, het uitvoeren van forensisch onderzoek, en het implementeren van processen voor het documenteren, rapporteren en oplossen van incidenten. Het doel is om snel en effectief te reageren op incidenten om schade te minimaliseren en de continuïteit van diensten te waarborgen.

C06: Leveranciersbeheer en Beoordeling
Code C06 richt zich op het beheer en de beoordeling van cloudserviceproviders. Dit omvat het evalueren van de beveiligingsmaatregelen en compliance van cloudproviders, het monitoren van hun prestaties, en het beheren van de relatie met leveranciers. Het doel is om ervoor te zorgen dat de cloudserviceproviders voldoen aan de beveiligings- en compliance-eisen die zijn vastgesteld in contractuele afspraken en regelgeving.

C07: Beveiliging van Netwerken en Infrastructuur
Code C07 behandelt de beveiliging van de netwerken en infrastructuur die worden gebruikt voor clouddiensten. Dit omvat het beveiligen van netwerkinfrastructuur tegen ongeautoriseerde toegang, aanvallen en andere bedreigingen, en het implementeren van maatregelen zoals firewalls, intrusion detection systems (IDS), en netwerksegmentatie om de integriteit en beschikbaarheid van cloudomgevingen te beschermen.

C08: Beheer van Data en Back-ups
Deze code richt zich op het beheer van gegevens en back-ups in de cloud. Het omvat het implementeren van procedures voor het maken van regelmatige back-ups van gegevens, het testen van back-up- en herstelprocessen, en het zorgen voor de beveiliging van back-ups tegen verlies, schade, of ongeautoriseerde toegang. Het doel is om gegevensherstel te waarborgen in geval van een storing of incident.

2.5 U-codes m.b.t. thema Clouddiensten

Binnen het thema Clouddiensten van de NORM BIO (Baseline Informatiebeveiliging Overheid) zijn de U-codes bedoeld om de beveiliging en het beheer van cloudomgevingen te reguleren vanuit een gebruikersperspectief. Deze codes richten zich op de verantwoordelijkheden en acties die van gebruikers worden verwacht om de veiligheid van clouddiensten te waarborgen. U-code staat voor Uitvoering maatregelen.

U01: Gebruik van Clouddiensten
Deze code richt zich op de richtlijnen en verantwoordelijkheden voor het gebruik van clouddiensten door eindgebruikers. Het omvat het volgen van beveiligings- en gebruiksrichtlijnen zoals het niet opslaan van gevoelige informatie op ongecontroleerde cloudomgevingen, en het naleven van de toegangs- en beveiligingsregels die zijn ingesteld door de organisatie. Gebruikers moeten zich bewust zijn van de risico's van het gebruik van clouddiensten en handelen volgens de vastgestelde beleidslijnen en procedures.

U02: Beheer van Gebruikersaccounts
Code U02 behandelt het beheer van gebruikersaccounts binnen clouddiensten. Dit omvat het aanmaken, onderhouden en verwijderen van gebruikersaccounts volgens het beleid van de organisatie. Belangrijke aspecten zijn het naleven van sterke wachtwoordvereisten, het regelmatig bijwerken van toegangsrechten op basis van functie en behoefte, en het onmiddellijk intrekken van toegang bij vertrek of wijziging van rol van een medewerker.

U03: Bewustwording en Training
Deze code richt zich op de noodzaak van bewustwording en training voor gebruikers van clouddiensten. Het omvat het geven van trainingen en het verhogen van het bewustzijn over de beveiligingsrisico’s en best practices met betrekking tot clouddiensten. Gebruikers moeten regelmatig worden geïnformeerd over actuele dreigingen, beveiligingsprocedures en hun rol in het handhaven van de beveiliging van cloudomgevingen.

U04: Incidentmelding en Rapportage
Code U04 behandelt de procedures voor het melden en rapporteren van beveiligingsincidenten die gerelateerd zijn aan clouddiensten. Gebruikers moeten weten hoe en wanneer ze incidenten moeten melden, zoals ongeautoriseerde toegang, datalekken of andere beveiligingsproblemen. Het benadrukt het belang van snelle rapportage om te zorgen voor een tijdige reactie en mitigatie van mogelijke schade.

U05: Gebruik van Beveiligingsmiddelen
Deze code richt zich op het gebruik van beveiligingsmiddelen en tools door eindgebruikers van clouddiensten. Dit omvat het gebruik van door de organisatie goedgekeurde beveiligingssoftware, zoals antivirusprogramma’s en encryptietools, en het naleven van beveiligingsbeleid met betrekking tot het gebruik van clouddiensten. Gebruikers moeten de beschikbare beveiligingsmiddelen effectief gebruiken om hun gegevens en toegang te beschermen.

U06: Verantwoordelijkheden bij Dataoverdracht
Code U06 behandelt de verantwoordelijkheden van gebruikers bij het overdragen van gegevens naar en van clouddiensten. Dit omvat het volgen van richtlijnen voor veilige dataoverdracht, zoals het versleutelen van gegevens tijdens overdracht en het controleren van de integriteit van gegevens. Gebruikers moeten zich bewust zijn van de risico’s bij het overdragen van gegevens en zorgen voor veilige en conforme processen.