

Vraagspecificatie Proces Eisen (VSP)

BIO bron duiding	eis type	eis nr	Concept contract eistekst voor generieke versie CSIR 3.4
5.1.1	VSP (proces)	VSP01	De Opdrachtnemer dient de Werkzaamheden met betrekking tot cybersecurity zodanig te verrichten dat het gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.
14.1.1.1	VSP (proces)	VSP04	De Opdrachtnemer dient als onderdeel van zijn Ontwerpwerkzaamheden ten aanzien van cybersecurity een risicoanalyse en risicoafweging conform NEN-ISO/IEC-27005 (Information security risk management) te maken en ter kennis te brengen van de Opdrachtgever.
6.1.1	VSP (proces)	VSP05	De Opdrachtnemer dient een sleutelfunctionaris aan te stellen die verantwoordelijk is voor de Werkzaamheden met betrekking tot cybersecurity.
16.1.3.1	VSP (proces)	VSP06	De opdrachtnemer dient een proces in te richten voor het ontvangen van meldingen van kwetsbaarheden van buitenaf conform de "Leidraad Coordinated Vulnerability Disclosure" van het Nationaal Cyber Security Centrum.
14.2.5	VSP (proces)	VSP07	Indien de Opdrachtnemer een test- en ontwikkelomgeving dient in te richten, dan dient hij daarbij de eisen ten aanzien van cybersecurity toe te passen.
5.1.1.1	VSP (proces)	VSP08	De Opdrachtnemer dient voor alle beheerobjecten die zijn voorzien van ICT en IA de van toepassing verklaarde cybersecuritymaatregelen uit "Cybersecurity Implementatierichtlijn Objecten" uit te voeren die behoren bij cybersecurity weerstandsniveau 1
5.1.1.1	VSP (proces)	VSP11	Indien de Opdrachtnemer tijdelijk niet aan cybersecurityeisen dreigt te voldoen, dan dient de Opdrachtnemer dit te behandelen als een afwijking in het kader van zijn kwaliteitsmanagementsysteem en dient de Opdrachtnemer deze afwijkingenrapportage ter kennis te brengen van de Opdrachtgever en op te nemen in het cybersecurity dossier.
5.1.1.1	VSP (proces)	VSP12	De Opdrachtnemer dient ten minste één keer per jaar een audit uit te voeren naar de opzet, het bestaan en de werking van de getroffen cybersecuritymaatregelen en dient de auditrapportage ter kennis te brengen van de Opdrachtgever.
16.1.6	VSP (proces)	VSP15	De Opdrachtnemer dient de opgetreden cybersecurity incidenten te analyseren en maatregelen te treffen om herhaling te voorkomen. De Opdrachtnemer dient jaarlijks alle cybersecurity incidenten te analyseren en deze rapportage op te nemen in het cybersecurity dossier.
16.1.7	VSP (proces)	VSP17	De Opdrachtnemer dient in voorkomende gevallen zijn medewerking te verlenen aan het verzamelen, bewaren en beschikbaar stellen van cybersecurity bewijsmateriaal.
18.1.4	VSP (proces)	VSP18	De Opdrachtnemer dient in het kader van de Algemene verordening gegevensbescherming (AVG) de persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, rechtmatig te behandelen.
15.1.1.3 18.1.4	VSP (proces)	VSP19	Indien de Opdrachtnemer persoonsgegevens en andere tot natuurlijke personen herleidbare gegevens, waaronder camerabeelden, opslaat en/of verwerkt, dan dient de Opdrachtnemer een verwerkersovereenkomst af te sluiten met de Opdrachtgever conform het <u>sjabloon "verwerkersovereenkomst"</u> dat de Opdrachtgever na opdrachtverlening op verzoek van de Opdrachtnemer beschikbaar stelt.

8.3.2.1 18.1.3	VSP (proces)	VSP22	De Opdrachtnemer dient het deel van zijn informatievoorziening, dat benodigd is voor de door de Opdrachtgever gevraagde Documenten en dat benodigd is bij de verwerking van de door de Opdrachtgever ter beschikking gestelde informatie, te beveiligen zodanig dat deze zijn beschermd tegen verlies, ongeautoriseerde kennisname en ongeautoriseerde wijziging.
8.3.2.2	VSP (proces)	VSP24	De Opdrachtnemer dient uiterlijk bij beëindiging van de Overeenkomst alle Documenten en door de Opdrachtgever ter beschikking gestelde informatie die kwetsbaarheden kunnen veroorzaken voor de Opdrachtgever en die niet eerder zijn overgedragen alsnog over te dragen aan de Opdrachtgever. Datgene wat is overgedragen en wat niet wordt of niet kan worden overgedragen, dient te worden gewist en/of vernietigd in de informatievoorziening van de Opdrachtnemer. Deze eis is ook van toepassing op een eventuele tussentijdse beëindiging van de Overeenkomst.
7.1.1	VSP (proces)	VSP27	De Opdrachtnemer dient de Werkzaamheden aan: 1. ontwerp- en constructietekeningen en constructieberekeningen en/of; 2. beveiligings- en veiligheidsdocumentatie en -instructies van: a. kunstwerken; b. bediengebouwen en -ruimten; c. ICT en IA; d. Kabels & Leidingen; dan wel de Werkzaamheden: 3. binnen bedien- en technische ruimten van de hiervoor genoemde objecten; 4. aan ICT en IA zelf; 5. aan kabels en leidingen door (zelfstandige) hulppersonen te laten verrichten die een geheimhoudingsverklaring hebben ondertekend en over een Verklaring Omtrent het Gedrag (VOG) beschikken die gerelateerd is aan de beoogde Werkzaamheden. In afwachting van het resultaat van de aanvraag van een VOG kan gedurende een periode van maximaal zes weken na start van de betreffende Werkzaamheden, welke termijn niet kan worden verlengd, worden volstaan met een eigen verklaring van de betreffende (zelfstandige) hulppersoon.
9.4.2.2	VSP (proces)	VSP30	Indien de Opdrachtnemer toegang tot ICT en IA op afstand (remote access) wenst, dan dient de Opdrachtnemer deze toegang via de centrale, beveiligde en gemonitorde voorzieningen van de Opdrachtgever te laten verlopen.
9.2.1	VSP (proces)	VSP32	De Opdrachtnemer dient te zorgen voor een procedure en actuele registratie van: 1. de door de Opdrachtnemer aan de (zelfstandige) hulppersonen verstrekte logische toegang tot ICT en IA door middel van accounts, autorisaties en bijbehorende middelen; 2. de fysieke toegang van de (zelfstandige) hulppersonen tot ICT en IA gerelateerde ruimten.
8.1.3	VSP (proces)	VSP37	De Opdrachtnemer dient alle door de Opdrachtgever beschikbaar gestelde toegangsmiddelen (waaronder tokens en pasjes tot beheerobjecten, data, ICT en IA) alleen te gebruiken voor het doel waarvoor en onder de voorwaarden waaronder deze zijn verstrekt, waarbij de beveiligingsmaatregelen niet mogen worden omzeild.
8.1.4	VSP (proces)	VSP38	De Opdrachtnemer dient alle door de Opdrachtgever ter beschikking gestelde bedrijfsmiddelen nadat ze niet meer van dienst zijn geworden doch uiterlijk bij beëindiging van de Overeenkomst terug te geven.
6.2.1.2	VSP (proces)	VSP43	De Opdrachtnemer dient maximale hardening toe te passen voor zijn (rand)apparatuur en (delen van) zijn eigen datanetwerkinfrastructuur die ten behoeve van de Werkzaamheden gekoppeld zijn aan de datanetwerkinfrastructuur van de Opdrachtgever.

5.1.1.1	VSP (proces)	VSP45	Indien er sprake is van een koppeling van (delen van) het datanetwerk van de Opdrachtnemer aan het datanetwerk van de Opdrachtgever, dan dient de Opdrachtnemer zijn medewerking te verlenen aan het risicogestuurd (laten) (pen)testen van (delen van) zijn datanetwerk.
5.1.1.1	VSP (proces)	VSP46	Indien er sprake is van een koppeling van (delen van) het datanetwerk van de Opdrachtnemer aan het datanetwerk van de Opdrachtgever, dan dient de Opdrachtnemer zijn medewerking te verlenen aan het risicogestuurd (laten) monitoren van (delen van) zijn datanetwerk.
14.2.1.1	VSP (proces)	VSP47	De Opdrachtnemer dient voor het ontwikkelen en/of het onderhouden van software de gangbare principes en de voorgeschreven maatregelen uit het document "Grip op Secure Software Development (SSD) Beveiligingseisen voor (web)applicaties" van het Centrum Informatiebeveiliging en Privacybescherming (CIP) te volgen.
14.2.7 18.2.3.1	VSP (proces)	VSP50	De Opdrachtnemer dient zijn medewerking te verlenen aan het (laten) pentesten en (laten) uitvoeren van (geautomatiseerde) kwetsbaarheidsscans van de ICT en IA door de Opdrachtgever.
12.6.1.1	VSP (proces)	VSP52	Indien de Opdrachtnemer meent geen gebruik te maken van de mogelijkheid om te patchen, dan dient hij een gemotiveerd voorstel ter kennis te brengen van de Opdrachtgever.
12.6.1.1	VSP (proces)	VSP53	Indien de Opdrachtgever melding maakt van een kritieke of niet kritieke patch dan dient de Opdrachtnemer daarvoor een implementatieadvies ter kennis te brengen van de Opdrachtgever. Daarbij gelden de volgende doorlooptijden: 1. voor een kritieke patch: maximaal 48 uur na melding door de Opdrachtgever, gerekend vanaf de eerstvolgende werkdag; 2. voor een niet kritieke patch: maximaal twee maanden na melding door de Opdrachtgever. De Opdrachtnemer dient de patch, na Acceptatie door de Opdrachtgever van het implementatieadvies, conform het advies te implementeren.
12.2.1	VSP (proces)	VSP54	Indien ICT en IA niet beschermd worden door antimalware oplossingen, dan dient de Opdrachtnemer ten minste jaarlijks, te scannen op malware en aangetroffen malware te verwijderen.
8.1.1	VSP (proces)	VSP56	De Opdrachtnemer dient alle configurations items (CI's) van de ICT en IA, te registreren in een door de Opdrachtgever beschikbaar gesteld Excel format en te leveren aan de Opdrachtgever.
12.3.1	VSP (proces)	VSP58	De Opdrachtnemer dient een protocol voor back-up en recovery, op te stellen en te leveren aan de Opdrachtgever.
7.2.1 18.2.2	VSP (proces)	VSP64	De Opdrachtnemer vereist dat zijn (zelfstandige) hulppersonen de cybersecurity eisen en maatregelen toepassen in overeenstemming met de vastgestelde beleidsregels en procedures.
18.2.1.1	VSP (proces)	VSP68	De Opdrachtnemer dient negatieve bevindingen en tekortkomingen die door de Opdrachtgever zijn geconstateerd en gemeld aan de Opdrachtnemer, af te handelen op gelijke wijze als afwijkingen die door de Opdrachtnemer zijn geconstateerd.
18.2.2	VSP (proces)	VSP69	De Opdrachtnemer dient de zelfstandige hulppersonen te managen, zodanig dat wordt gewaarborgd dat de door zelfstandige hulppersonen verrichte Werkzaamheden en de resultaten daarvan voldoen aan de eisen voortvloeiende uit de Overeenkomst.

Vraagspecificatie Systeemtechnische Eisen (VSE)

5.1.1	VSE (systeem)	VSE01	De ICT en IA van het beheerobject dient zodanig te zijn ingericht en onderhouden, dat gevaar of schade veroorzaakt door verstoring, uitval of misbruik van ICT en IA wordt voorkomen.
5.1.1.1	VSE (systeem)	VSE03	De ICT en IA van het beheerobject dient zodanig te zijn gerealiseerd dat de beveiliging van de ICT en IA volgens het principe van gelaagde beveiliging is ingericht.
6.2.1.2	VSE (systeem)	VSE04	Maximale hardening dient aangehouden te zijn voor de (rand)apparatuur en delen van de datanetwerkinfrastructuur van waaruit remote beheer en onderhoud wordt uitgevoerd aan de ICT en IA van het beheerobject.
10.1.1	VSE (systeem)	VSE08	Voor de ICT en IA van het beheerobject dient bij inzet van versleuteling alleen gekozen te worden voor de versleuteling, de onderliggende algoritmes en instellingen met uitsluitend de duiding "goed", zoals aangegeven in het NCSC document [Richtlijnen voor Transport Layer Security].
11.1.4	VSE (systeem)	VSE12	ICT en IA van het beheerobject dient tegen schade en storing beschermd te zijn.
11.1.4 11.2.6	VSE (systeem)	VSE13	De ICT en IA van het beheerobject dient, indien geplaatst buiten beveiligde gebouwen en ruimten, op basis van een risico analyse en afweging geplaatst te zijn in afsluitbare kasten of ruimten, die bij fysieke opening een alarmmelding genereren, die opgevolgd wordt, evenals bij ongeautoriseerde logische toegang tot het datanetwerk in de kast of ruimte.
11.2.1 11.2.3	VSE (systeem)	VSE14	Voedings- en telecommunicatiekabels van het beheerobject die voor dataverkeer of ondersteunende informatiediensten zijn toegepast dienen tegen interceptie, verstoring of schade beschermd te zijn.
12.1.4	VSE (systeem)	VSE15	De Ontwikkel-, Test-, Acceptatie-, Productie-, en Leeromgeving van het beheerobject dient gescheiden te zijn om het risico van onbevoegde toegang tot of veranderingen aan de productie omgeving te verlagen.
12.1.4	VSE (systeem)	VSE16	De ICT en IA van het beheerobject dient beschermd te zijn tegen malware.
12.2.1	VSE (systeem)	VSE17	De ICT en IA van het beheerobject dient gehardend te zijn.
12.2.1	VSE (systeem)	VSE18	De ICT en IA van het beheerobject dient gepatcht te zijn.
12.3.1	VSE (systeem)	VSE19	De integriteit en beschikbaarheid van de ICT en IA van het beheerobject dient geborgd te zijn doormiddel van back-ups.
12.4.1	VSE (systeem)	VSE20	De ICT en IA van het beheerobject dient de activiteiten van gebruikers, beheerders, uitzonderingen en informatiebeveiligingsgebeurtenissen vast te leggen in logbestanden.
12.4.1	VSE (systeem)	VSE21	Voor de ICT en IA van het beheerobject dient een (centrale) syslog server ingericht te zijn die syslog events verzamelt en toegankelijk maakt voor analysedoeleinden en automatische waarschuwingen door een Security Information & Event Management (SIEM) systeem en/of een Security Operations Centre (SOC).
12.4.1.3	VSE (systeem)	VSE23	Het objectdatanetwerk van het beheerobject dient uitgevoerd te zijn met analysepoorten door poorten in het lokale objectdatanetwerk tot analyse poort te configureren.
13.1.1	VSE (systeem)	VSE25	Alle datanetwerkverbindingen van het beheerobject dienen strikt en uitsluitend te verlopen via centrale beveiligde voorzieningen. Directe vaste of draadloze datanetwerkverbindingen met andere datanetwerken dan die van Opdrachtgever zijn strikt verboden.
13.1.1	VSE (systeem)	VSE26	Het aantal ICT en IA datanetwerkkoppelingen van het beheerobject met andere externe datanetwerken dient geminimaliseerd te zijn.
13.1.3	VSE (systeem)	VSE28	Voor de ICT en IA van het beheerobject dient gebruik te zijn gemaakt van een gecompartmenteerde datanetwerk dat van de kantoorautomatisering is gescheiden. De scheiding kan fysiek of logisch zijn.

13.1.3	VSE (systeem)	VSE29	Voor de ICT en IA van het beheerobject dient segmentering van dataverkeersstromen toegepast te zijn voor Ontwikkel-, Test-, Acceptatie-, Productie-, Leer- en Beheeromgeving.
14.1.1	VSE (systeem)	VSE31	ICT en IA van het beheerobject dient voorzien te zijn van invoer en uitvoer validatie controles om corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen traceerbaar te maken.
14.1.1	VSE (systeem)	VSE33	Bij inzet van (web)applicaties voor beheer of onderhoud van ICT en IA van het beheerobject dient de beveiliging van de in te zetten (web)applicaties ingericht te zijn conform de [ICT-Beveiligingsrichtlijnen Webapplicaties] van het Nationaal Cybersecurity Centrum.
14.2.1.1	VSE (systeem)	VSE36	De software van ICT en IA van het beheerobject dient ontwikkeld en beheerd te zijn volgens gangbare principes en de voorgeschreven maatregelen conform Secure Software Development (SSD) van het Centrum voor Informatiebeveiliging en Privacy (CIP).
14.2.7	VSE (systeem)	VSE38	De ICT en IA van het beheerobject dienen als integraal onderdeel van de FAT, SAT en SIT getest te zijn op technische naleving van beveiligingseisen en het aantoonbaar maken van de werking van de security functies en maatregelen.
16.1.5	VSE (systeem)	VSE39	De ICT en IA van het beheerobject dient naar een vooraf gedefinieerde veilige situatie gestuurd te worden in geval van een aanval, incident of calamiteit.