HOOGHEEMRAADSCHAP
DE STICHTSE
RIJNLANDEN

# Bijlage 10 Programma van Eisen SaaS diensten

| Eis | Standaarden voor clouddiensten |
|---|---|
| U.01 | De inschrijver past aantoonbaar relevante, nationale standaarden en internationale standaarden (conform Forum standaardisatie) toe voor de opzet en exploitatie van de diensten en de interactie met HDSR - Sluit aan bij architectuurprincipe AL001 (221020_Enterprise_Architectuur_HDSR_Architectuurprincipes V0.9) |
| U.01.1 | De inschrijver maakt haar dienstverlening transparant, zodanig dat HDSR daarmee aantoonbaar aan de voor haar verplichte BIO en 'pas toe of leg uit'-standaarden kan voldoen. |

| Eis | Continuïteitsservices |
|---|---|
| U.02 | Informatie verwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan HDSR continuïteitseisen te voldoen. |
| U.02.1 | De technische beschikbaarheid, (d.w.z. server, storage, netwerk en koppelpunt datacenter, besturingssoftware, virtualisatie, database en middleware) van de SaaS-dienst dient, binnen de gestelde reactietijden (max. 1 seconde) en gebruikersaantallen (tussen 500 en 600 en concurrent 200), een jaarlijkse beschikbaarheid te hebben van minimaal 99,6%. |
| U.02.2 | De SaaS-dienst dient optimale performance te bieden (maximale reactietijd van 1 seconde). |
| U.02.3 | De inschrijver dient gepland onderhoud minimaal 1 maand van te voren aan te kondigen bij HDSR, inclusief welke wijzigingen doorgevoerd gaan worden. Het gepland onderhoud vindt plaats tussen 99:00 uur tot 99:00 uur (SaaS dienst specifiek invulling aangeven) van maandag tot en met vrijdag. Inschrijver bepaalt in overleg met HDSR wanneer de werkzaamheden worden doorgevoerd. EIS is dat het aangekondigd moet worden |
| U.02.4 | De inschrijver rubriceert storingen in de SaaS-dienst als volgt:<br>Kritiek: Wanneer HDSR meer dan 1 uur geen gebruik kan maken van de dienstverlening.<br>Overig: Alle storingen die niet vallen onder de rubriek Kritiek of daartoe bijdragen.<br>Voor de storingen en servicelevels geldt e.e.a. voor zover dit in de invloedsfeer zit van de Inschrijver. Voor storingen buiten de invloedsfeer van de Inschrijver geldt een coördinatieverplichting om storingen zo snel mogelijk met HDSR of derden op te lossen. |
| U.02.4a | Voor storingen met rubricering Kritiek geldt voor de technische werking (d.w.z. server, storage, netwerk en koppelpunt datacenter, besturingssoftware, virtualisatie, database en middleware) de reactietijd op het incident, statusrapportage en hersteltijd zoals hieronder vermeld:<br>- Reactietijd (de tijd tussen de melding bij de tweedelijnsupport van de Inschrijver, interne bewakingsdienst of geautomatiseerde detectie en het tijdstip waarop Inschrijver respons geeft met indicatie van corrigerende maatregelen) is maximaal 15 minuten na melding;<br>- Hersteltijd (de tijd tussen de melding bij de tweedelijnsupport van de Inschrijver, interne bewakingsdienst of geautoriseerde detectie en het tijdstip waarop de storing is opgelost) is maximaal 60 minuten na melding. |
| U.02.4b | Voor storingen met rubricering Overig geldt voor de technische werking de reactietijd op het incident, statusrapportage en hersteltijd zoals hieronder vermeld:<br>• Reactietijd (de tijd tussen de melding bij de tweedelijnsupport van de Inschrijver, interne bewakingsdienst of geautomatiseerde detectie en het tijdstip waarop Inschrijver respons geeft met indicatie van corrigerende maatregelen) is maximaal 240 minuten;<br>• Statusrapportage wordt meegenomen in de periodieke rapportage en bij elke verandering van de situatie;<br>• Hersteltijd (de tijd tussen de melding bij de tweedelijnsupport van de Inschrijver, interne bewakingsdienst of geautoriseerde detectie en het tijdstip waarop de storing is opgelost) is maximaal 2 werkdagen in 85% van de gevallen, tenzij anders overeengekomen met HDSR. |
| U.02.4c | De inschrijver dient met HDSR de regels voor prioritering van incidenten op te stellen en te onderhouden zodat alle incidenten meteen een prioriteit krijgen. |

| Eis | Continuïteitsservices |
|---|---|
| U.02.5 | De inschrijver garandeert dat in geval van een calamiteit dat SaaS-dienst binnen 24 uur na het ontstaan van de calamiteit weer beschikbaar is. |

| Eis | Herstelfunctie voor data en clouddiensten |
|---|---|
| U.03 | De herstelfunctie van de data en SaaS-diensten, gericht op ondersteuning van bedrijfsprocessen, behoort te worden gefaciliteerd met infrastructuur en IT-diensten, die robuust zijn en periodiek worden getest. |
| U.03.1 | In geval van een calamiteit dienen alle gegevens in de SaaS dienst tot maximaal 8 uur voor het tijdstip van de calamiteit, beschikbaar te zijn voor herstel. |
| U.03.2 | Het continue proces van herstelbaar beveiligen van data wordt gemonitord en met HDSR gedeeld danwel gerapporteerd. |
| U.03.3 | Het toereikend functioneren van de herstelfuncties wordt periodiek (min. jaarlijks) of na een grote wijziging getest door gekwalificeerd personeel en de resultaten daarvan worden gedeeld met danwel gerapporteerd aan HDSR. |

| Eis | Dataprotectie |
|---|---|
| U.04 | 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. |
| U.04.1 | Gegevenstransport wordt naar de laatste stand der techniek beveiligd met cryptografie (conform Forum Standaardisatie), waarbij het sleutelbeheer zo mogelijk door HDSR zelf wordt uitgevoerd. |
| U.04.2 | De binnen de SaaS-dienst opgeslagen gegevens worden naar de laatste stand der techniek beveiligd met encryptie en met een tenminste voor het doel toereikende sleutellengte, waarbij het sleutelbeheer zo mogelijk niet als SaaS-dienst wordt afgenomen en door HDSR zelf wordt uitgevoerd. |
| U.04.3 | Gegevens dienen gegarandeerd binnen de Europees Economische Ruimte te worden opgeslagen. |

| Eis | Dataretentie en gegevensvernietiging |
|---|---|
| U.05 | Gearchiveerde data behoren gedurende de overeengekomen bewaartermijn, technologie-onafhankelijk, raadpleegbaar, onveranderbaar en integer te worden opgeslagen en op aanwijzing van HDSR/data-eigenaar te kunnen worden vernietigd. |
| U.05.1 | De gegarandeerde en met de inschrijver overeengekomen opslagduur is gelijk aan de duur van de overeenkomst. En bepalingen in de exit strategie. |
| U.05.2 | Gegevens zijn, onafhankelijk van de door de inschrijver toegepaste technologie, raadpleegbaar tijdens de gehele bewaartermijn. |
| U.05.3 | Gegevens worden gearchiveerd met Write Once Read Many (WORM)-technologie, waarmee de integriteit van de data wordt gegarandeerd. |
| U.05.4 | Voorafgaand aan het voor onderhoudsdoeleinden wijzigen van opslagmedia, worden de data van HDSR, inclusief de back-up van gegevens en metadata veilig gesteld. |
| U.05.5 | Bij het beëindigen van de overeenkomst worden de data van HDSR, inclusief de back-up van gegevens en de metadata na overdracht aan HDSR veilig gewist, om te voorkomen dat HDSR-gegevens naderhand door de inschrijver kunnen worden hersteld, bijvoorbeeld met forensische hulpmiddelen. |

| Eis | Datascheiding |
|---|---|
| U.06 | HDSR-gegevens behoren tijdens transport, bewerking en opslag duurzaam geïsoleerd te zijn van beheerfuncties en data van andere dienstafnemers, die de inschrijver in beheer heeft. |

| Eis | Datascheiding |
|---|---|
| U.06.1 | De bevoegdheden voor het inzien of wijzigen van HDSR-data en/of van encryptiesleutels door beheerfuncties en beheerders worden gecontroleerd verleend en het gebruik van deze rechten wordt gelogd. |

| Eis | Scheiding dienstverlening |
|---|---|
| U.07 | De cloud-infrastructuur is zodanig ingericht dat de dienstverlening aan gebruikers van informatiediensten zijn gescheiden. |
| U.07.1 | De inschrijver realiseert de volgende scheiding van SaaS-diensten:<br>* onderlinge scheiding van dienstafnemers in een multi-tenant-omgeving;<br>* scheiding tussen de afgenomen cloud-service en de interne informatievoorziening van de inschrijver;<br>* de inschrijver maakt het mogelijk om de beoogde scheiding van SaaS-diensten te verifiëren. |

| Eis | Malware-protectie |
|---|---|
| U.08 | Ter bescherming tegen malware behoren door de inschrijver beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers. |
| U.08.1 | De inschrijver specificeert, als onderdeel van de overeenkomst, welke maatregelen (voor onder andere malware-protectie) op welke positie in de informatieketen van HDSR en de inschrijver moeten worden genomen. |
| U.08.2 | De inschrijver heeft de voor ontwikkeling en exploitatie van SaaS-diensten gebruikte IT-systemen en netwerkperimeters, waarvoor zij verantwoordelijk is, uitgerust met tools ter bescherming en verwijdering van malware. |
| U.08.3 | De malware-bescherming wordt op verschillende omgevingen uitgevoerd, zoals op mailservers, (desktop)computers en bij de toegang tot het netwerk van de organisatie. De scan op malware omvat onder andere:<br>* alle bestanden die via netwerken of via elke vorm van opslagmedium zijn ontvangen, nog voor het gebruik;<br>* alle bijlagen en downloads nog voor het gebruik;<br>* virtuele machines;<br>* netwerkverkeer. |

| Eis | Toegang IT-diensten en data |
|---|---|
| U.09 | Gebruikers behoren alleen toegang te krijgen tot de IT-diensten en data waarvoor zij specifiek bevoegd zijn. |
| U.09.1 | De inschrijver biedt HDSR uitsluitend toegang tot services, IT-diensten en data waarvoor zij specifiek bevoegd is, waarbij:<br>* Technische maatregelen voorkomen dat gebruikers en beheerders toegang hebben tot services, IT-diensten en data buiten datgene wat formeel is toegestaan.<br>* Gebruikers met nood-toegangsrechten (in geval van calamiteiten, wanneer acties niet door bevoegde beheerders kunnen worden uitgevoerd), zijn gedocumenteerd, door het management geaccordeerd en wordt uitgevoerd met functiescheiding. Noodtoegang is geactiveerd zolang als nodig is voor de corresponderende taak/taken. |
| U.09.2 | Onder verantwoordelijkheid van de inschrijver wordt aan beheerders:<br>* toegang verleend tot data met het least privilege-principe;<br>* toegang verleend tot data met het need-to-know principe;<br>* toegang verleend met multi-factorauthenticatie;<br>* toegang verleend tot data en applicatieve functies via autorisatie maatregelen. |
| U.09.3 | Alleen gebruikers met geauthenticeerde apparatuur kunnen toegang krijgen tot IT-diensten en data. |
| U.09.4 | Onder de verantwoordelijkheid van de inschrijver worden bevoegdheden (systeemautorisaties) voor gebruikers toegekend via formele procedures. |

| Eis | Toegang IT-diensten en data |
|---|---|
| U.09.5 | Toegang tot IT-diensten en data is beperkt door technische maatregelen en is geïmplementeerd, met gebruik van het rollen- en rechtenconcept. Gebruik van rollen en rechten zoals vastgelegd in Active Directory; Single sign on is hierbij een eis. |
| U.09.6 | Het benaderen van de een SaaS-dienst dient via het (webbased) https protocol (de toepassingslaag volgens het TCP/IP model) te geschieden. Andere protocollen voor het benaderen van een SaaS dienst zijn niet toegestaan. |
| U.09.10 | De SaaS dienst dient benaderbaar te zijn via een “fully qualified domain name”.<br>Een Fully Qualified Domain Name (FQDN) is een in het Internet Domain Name System (DNS) geregistreerde volledige naam waarmee een server op het Internet uniek is te identificeren en te adresseren. |

| Eis | Cryptoservices |
|---|---|
| U.10 | Gevoelige data van HDSR behoren middels cryptografische maatregelen tijdens transport via netwerken en bij opslag bij inschrijver te zijn versleuteld. |
| U.10.1 | In geval van PKIoverheid-certificaten: de inschrijver hanteert de PKIoverheid-eisen ten aanzien van het sleutelbeheer. In overige situaties: de inschrijver hanteert de standaard ISO 11770 voor het beheer van cryptografische sleutels. |

| Eis | Koppelvlakken |
|---|---|
| U.11 | De onderlinge netwerkconnecties (koppelvlakken) in de keten van HDSR naar de inschrijver behoren door de inschrijver te worden bewaakt en beheerst om de risico’s van datalekken te beperken. |
| U.11.1 | In koppelpunten met externe of onvertrouwde zones heeft de inschrijver zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijvoorbeeld Distributed Denial of Service attacks (DDos)-aanvallen) te signaleren en hierop te reageren. |
| U.11.2 | Fysieke en gevirtualiseerde netwerkcomponenten zijn door de inschrijver zodanig ontworpen en geconfigureerd dat netwerkconnecties tussen vertrouwde en onvertrouwde netwerken worden beperkt en gemonitord (bewaakt). |
| U.11.3 | Beheeractiviteiten van de inschrijver zijn strikt gescheiden van de data van HDSR. |
| U.11.4 | Dataverkeer voor dienstafnemers bij de inschrijver zijn in gezamenlijk gebruikte netwerkomgevingen gescheiden volgens een gedocumenteerd concept voor de op netwerkniveau (logische) segmentatie van dienstafnemers, om zo de integriteit en vertrouwelijkheid van de verzonden gegevens te garanderen. |
| U.11.5 | Het dataverkeer dat bij de inschrijver binnenkomt of uitgaat wordt, in relatie tot de aard van de te beschermen gegevens/informatiesystemen, bewaakt en geanalyseerd op kwaadaardige elementen middels detectievoorzieningen. |
| U.11.6 | De inschrijver heeft Intrusion Detection Prevention (IDP) en Intrusion Detection System (IDS) geïntegreerd in een allesomvattend Security Information and Event Management (SIEM), zodat beveiligingsgebeurtenissen en onbekende apparatuur vanuit de benodigde technische maatregelen worden opgemerkt en correctieve maatregelen kunnen worden genomen. |
| U.11.7 | Bij ontdekte nieuwe dreigingen worden deze, rekening houdend met geldende juridische kaders, verplicht gedeeld binnen de overheid, waaronder met het NCSC of het sectorale Computer Emergency Response Team (CERT), bij voorkeur door geautomatiseerde mechanismen (threat intelligence sharing). |
| U.11.8 | Er wordt door de inschrijver geen gebruik gemaakt van plug-in componenten (zoals o.a. Microsoft Active X, Microsoft Silverlight, Microsoft ClickOnce, Adobe Flash en Java plug-in. Onder plug-in componenten worden tevens de volgende software verstaan VMware Horizon client, Citrix Receiver en Microsoft remote client.<br>Bedoeld wordt Java-software voor een client-device, ook Java Runtime Environment, Java Runtime, JRE, Java Virtual Machine, Java VM, JVM, Java-uitbreiding of Java-download genoemd. |

| Eis | Interoperabiliteit en portabiliteit |
|---|---|
| U.12 | Cloud-services zijn bruikbaar (interoperabiliteit) op verschillende IT-platforms en kunnen met standaarden verschillende IT-platforms met elkaar verbinden en data overdragen (portabiliteit). |
| U.12.1 | Om de interoperabiliteit van cloud-services te garanderen, zijn gegevens beschikbaar conform erkende industrie-standaarden en gedocumenteerde invoer- en uitvoerinterfaces. |
| U.12.2 | Om de portabiliteit van de data te garanderen, maakt de inschrijver gebruik van beveiligde netwerkprotocollen voor de import en export van data waarmee de integriteit en vertrouwelijkheid worden gegarandeerd. |

| Eis | Logging en monitoring |
|---|---|
| U.13 | Logbestanden waarin gebruikersactiviteiten, en informatiebeveiliging gebeurtenissen worden geregistreerd, behoren te worden bewaard en regelmatig te worden beoordeeld. |
| U.13.1 | Beoordelingen en eventueel hieruit volgende maatregelen dienen door de inschrijver en daar waar van toepassing door HDSR te worden vastgelegd. |
| U.13.2 | De SIEM en/of Security Operation Centre (SOC) hebben heldere regels over wanneer een incident moet worden gerapporteerd aan het verantwoordelijk management. |
| U.13.3 | De inschrijver hanteert een lijst van alle assets die kritisch zijn in termen van logging en monitoring en beoordeelt deze lijst regelmatig (min. 1x per half jaar) op correctheid. |
| U.13.4 | Aan logboeken en bewaking worden strenge eisen gesteld. Voor de kritieke componenten zijn geavanceerde beveiligingen voor logboeken en bewaking door de inschrijver gedefinieerd. |
| U.13.5 | De toegang tot en het beheer van de loggings- en monitoringsfunctionaliteit is beperkt tot geselecteerde en geautoriseerde medewerkers van de inschrijver. |
| U.13.6 | Wijzigingen in logging en monitoring worden gecontroleerd door onafhankelijke en geautoriseerde medewerkers. (Logregels mogen nooit worden gewijzigd; deze zijn immers bedoeld om als bewijslast te kunnen gebruiken). |

| Eis | Multi-tenantarchitectuur |
|---|---|
| U.14 | Bij multi-tenancy worden HDSR-data binnen SaaS-diensten, die door meerdere klanten worden afgenomen, in rust versleuteld en gescheiden verwerkt op gehardende (virtuele) machines. |
| U.14.1 | HDSR-data op transport en in rust zijn versleuteld. |
| U.14.2 | Virtuele machine platforms voor dienstafnemers van de inschrijver met speciale/verhoogde beveiligingsvereisten zijn gescheiden ingericht. |
| U.14.3 | Virtuele machine platforms zijn gehardend. |

| Eis | Tweedelijnsupport |
|---|---|
| U.H. | HDSR heeft een eigen helpdesk organisatie voor eerste lijn support, een productowner, functioneelbeheerders en keyusers. |
| U.H.1 | De Inschrijver zal minimaal 2 vaste contactpersonen toewijzen voor tweede lijnsupport voor de HDSR productowner en functioneelbeheerders. |
| U.H.2 | Alle contactpersonen van de inschrijver voor de tweedelijnsupport zijn na de projectfase bij voorkeur Nederlandstalig en anders tenminste Engelstalig. |
| U.H.3 | De contactpersonen van de inschrijver zijn bereikbaar op, werkdagen tussen 8:00 en 17:00 uur, via diverse media zoals telefoon, mail en chat. |
| U.H.4 | De inschrijver geeft maandelijks aan HDSR input op basis van loggegevens om de frequently asked questions en antwoorden daarop te verbeteren. |

| Eis | SaaS dienst |
|---|---|
| S.D. | Specifieke eisen met betrekking tot een SaaS dienst het device waarop gewerkt wordt. (Denk aan laptop, mobiele telefoon of tablet) |
| S.D.1 | Een SaaS dienst dient responsivie te zijn. De SaaS dienst dient zich te kunnen aanpassen aan het device waarop gewerkt wordt. (Denk aan laptop, mobiele telefoon of tablet) |
| S.D.2 | Alle gebruikersinterfaces (GUI's) zijn volledig 'webbased' en conformeren zich aan de W3C standaard zonder enige beperking voor wat betreft weergave en functionaliteit (interfaces t.b.v. functioneel beheer vallen hier ook onder). |
| S.D.3 | Voor de presentatie van een SaaS dienst aan eindgebruikers (inclusief functioneel beheerders) is het niet toegestaan gebruik te maken van zogenaamde remote desktop, virtual desktop infrastructuur (VDI) en/of server based computing (SBC) technologieën (voorbeelden hiervan zijn o.a. VMware Horizon, Citrix Xenapp en Microsoft remote desktop services). Deze technologieën worden niet als "volledig webbased" beschouwd (zie voorgaande eis). |
| S.D.4 | HDSR streeft naar browseronafhankelijkheid van een SaaS dienst, daarom dient een SaaS dienst (voor wat betreft de volledig aangeboden functionaliteit) MINIMAAL geschikt te zijn voor het gebruik in de volgende webbrowsers: Mozlla Firefox; Google Chrome; Safari; Microsoft Edge. |
| S.D.5 | Voor het functioneren van een SaaS dienst op het client device en/of in de webbrowser zijn geen verdere instellingen, dan wel installaties (op het client device en/of in de browser) benodigd. |
| S.D.6 | De inschrijver accepteert dat goedkeuring tot het gebruik van de SaaS dienst alleen afgegeven wordt na een technische acceptatietest waarbij nagegaan wordt of de SaaS disnet, voor wat betreft de volledige functionaliteit, ook daadwerkelijk aan de gestelde eisen in dit document voldoet. |