# Bijlage 3 - Programma van Eisen

**Amsterdam UMC**

**inzake**

Sleutelkasten

TenderNed-kenmerk: TN 602783

# 1 Instructie:

In dit Programma van Eisen zijn de eisen opgenomen waaraan de aangeboden oplossing en de dienstverlening van Opdrachtnemer gedurende de looptijd van de Overeenkomst dienen te voldoen.

Door het indienen van een Inschrijving verklaart Ondernemer onvoorwaardelijk te voldoen aan alle in dit Programma van Eisen opgenomen eisen.

Dit Programma van Eisen is opgebouwd uit twee delen:

- **Deel 1: Algemene eisen**
  In dit deel zijn de functionele, operationele, technische, contractuele en overige eisen opgenomen. De eisen zijn gegroepeerd per onderwerp.
- **Deel 2: ICT-eisen**
  In dit deel zijn de eisen opgenomen met betrekking tot de softwarevoorziening, informatiebeveiliging, privacy, koppelingen, beheer, continuïteit en overige ICT-gerelateerde aspecten. Ook deze eisen zijn gegroepeerd per onderwerp.

Bijlagen bij dit document:

- Bijlage 3.1: Huisregels
- Bijlage 3.2: Mediaprotocol
- Bijlage 3.3: Procedure beheren van gegevens
- Bijlage 3.4: Ultimo Upload Lijst - Dienst HV&T
- Bijlage 3.5: ICT: Richtlijn soevereiniteit UMC
- Bijlage 3.6: ICT: Clouddiensten beleidskader ICT

## 2 Deel 1 – Eisen aan de aanbesteding

| 1. | Algemene eisen |
|---|---|
| 1.1 | De communicatie tussen Opdrachtnemer en Opdrachtgever (Amsterdam UMC) vindt plaats in de Nederlandse taal, zowel mondeling als schriftelijk. |
| 1.2 | Leverancier overlegt periodiek, ten minste twee (2) keer per jaar een account- en onderhoudsoverzicht aan UMC met daarin de relevante prestatiegegevens, incidenten, onderhoudswerkzaamheden, openstaande acties en verbetervoorstellen. |
| 1.3 | Opdrachtnemer dient te handelen in overeenstemming met de geldende wet- en regelgeving, waaronder relevante normen voor kwaliteit, veiligheid en privacy binnen de zorgsector. |
| 1.4 | Opdrachtnemer waarborgt de continuïteit en betrouwbaarheid van de geleverde oplossing. |
| 1.5 | Opdrachtnemer is verantwoordelijk voor het naleven van geldende ARBO- en veiligheidsvoorschriften bij levering en installatie op locatie. |
| 1.6 | Opdrachtnemer heeft een in Nederland vertegenwoordigde, Nederlands sprekende serviceorganisatie voor ondersteuning bij technische en/of softwaregerelateerdevraagstukken. Deze serviceorganisatie is tijdens reguliere kantooruren bereikbaar en daarbuiten via een noodnummer voor calamiteiten. |
| 1.7 | Binnen één (1) maand na de ingangsdatum van de Overeenkomst levert Opdrachtnemer documentatie aan waaruit blijkt dat de dienstverlening, hardware en software aantoonbaar worden voorbereid op en in lijn worden gebracht met nieuwe en aankomende wet- en regelgeving, waaronder ten minste:<br>• de NIS2 (network and information security 2);<br>• de CER (Critical Entity Resilience), Wwke = Wet weerbaarheid kritieke entiteiten);<br>• CRA (Cyber Resilience Act).<br>Opdrachtnemer licht toe op welke wijze aan deze wet- en regelgeving wordt voldaan of zal worden voldaan en verstrekt hiervoor relevante bewijsstukken, zoals certificeringen, auditrapportages, implementatieplannen, beleidsdocumenten of een roadmap waarin deze ontwikkelingen en maatregelen expliciet zijn opgenomen. |
| 1.8 | Het aangeboden systeem is een SaaS-oplossing. Voor verdere eisen zie deel 2 van dit PVE m.b.t. ICT eisen. |
| 1.9 | Opdrachtnemer werkt conform onderstaande regelementen:<br>• Bijlage 3.1: Huisregels<br>• Bijlage 3.2: Mediaprotocol<br>• Bijlage 3.3: Procedure beheren van gegevens |

| 2. | Producteisen |
|---|---|
| 2.1 | De aangeboden apparatuur beschikt op het moment van inschrijven over een geldig CE-certificaat en wordt op verzoek van Opdrachtgever aangeleverd. Zie ook 1.7 in relatie tot het CE-certificaat conform de CRA. |
| 2.2 | De aangeboden apparatuur betreft een apparaat met stekker als arbeidsmiddel conform NEN3140. |
| 2.3 | Als onderdeel van de oplevering voert Opdrachtnemer na installatie van de aangeboden apparatuur een functionele controle uit zodat de apparatuur gebruiktsklaar wordt opgeleverd. |
| 2.4 | De aangeboden apparatuur beschikt over een minimale inbraakwerendheid die vergelijkbaar is met EN 14450 klasse S1. Een hogere classificatie, zoals EN 14450 klasse S2, heeft de voorkeur en wordt positief gewaardeerd bij de beoordeling, maar is geen minimumeis. Ook oplossingen zonder formele EN 14450-certificering worden geaccepteerd, mits objectief kan worden aangetoond dat zij een gelijkwaardig of hoger beveiligingsniveau bieden dan EN 14450 klasse S1. |
| 2.5 | Het slot waarmee de kast elektronisch en handmatig ontgrendeld wordt dient voorzien te zijn van een passende certificering, zoals SKG*** |

| 3. | Systeem Algemeen |
|---|---|
| 3.1 | Het systeem bestaat uit het fysieke aantal en de locaties van de sleutelkasten conform bijlage 4 en 4.1 |

| | |
|---|---|
| 3.2 | Het systeem wordt uitgevoerd in één nader te bepalen RAL-kleur en voorzien van een dichte of transparante deur, zoals per sleutelkast aangegeven, zie bijlage 4 en 4.1. |
| 3.3 | De sleutelkasten moeten gemaakt zijn van robuuste onderdelen en ontworpen zijn om minimaal 500 keer per dag geopend en gesloten te worden. Dit geldt ook voor de elektronische onderdelen zoals de display en/of touchscreens. |
| 3.4 | De sleutelkasten bieden toegang aan minimaal 2.500 gebruikers.<br>Een uitgenomen sleutel kan uitsluitend worden teruggeplaatst in de kast en op de sleutelpositie waarvan deze is uitgenomen. |
| 3.5 | De verwachte technische levensduur bij normaal onderhoud en gebruik is ten minste 15 jaar. |
| 3.6 | Het systeem dient modulair te zijn: bijvoorbeeld een toegangspaneel dat uitgewisseld kan worden. Hetzelfde geldt voor badgelezers. |

| **4.** | **Noodsituatie** |
|---|---|
| 4.1 | Bij stroomuitval moeten de sleutelkasten gesloten blijven. |
| 4.2 | Om de sleutelkasten operationeel te houden bij stroomuitval dient er een noodstroomaccu aanwezig te zijn met een autonomietijd van 12 uur of 1000 handelingen. |
| 4.3 | De sleutelkasten moeten ook functioneren wanneer de netwerkverbinding uitvalt. |
| 4.4 | Vrijgave op afstand moet mogelijk zijn in verband met calamiteiten vanuit de twee meldkamers. |

| **5.** | **Autorisatie en passysteem** |
|---|---|
| 5.1 | De sleutelkasten zijn in normale operatie vergrendeld en door normale gebruikers niet te openen zonder autorisatie. |
| 5.2 | Op een personeelspas moet het versleutelde deel van een MIFARE DESFire v1/v2/v3 kunnen worden uitgelezen. Voor locatie AMC en locatie VUmc betreft dit twee verschillende applicatiefiles met verschillende sleutels. Het systeem leest op locatie AMC de AMC-applicatiefile op de MIFARE DESFire EV1-pas uit en op locatie VUmc de VUmc applicatiefile op de DESFire EV- pas.<br>Vanaf medio 2027 tot begin 2028 wordt een pas geïntroduceerd waarop alle applicatiefiles van locatie AMC en locatie VUmc zijn gecombineerd (bestaande settings). |
| 5.3 | Het moet mogelijk zijn om gebruikers bij de sleutelkast te authenticeren door middel van een personeelspas en pincode (4 tot6 cijfers). De pincode moet zowel door de applicatiebeheerders kunnen worden ingesteld enbeheerd alsook door de pashouder (gebruiker van het systeem) middels een selfservice (bijvoorbeeld op de terminal van de kast). |
| 5.4 | Opdrachtnemer toont binnen één (1) maand na de ingangsdatum van de Overeenkomst aan dat het aangeboden systeem en de applicatie worden voorbereid op toekomstige ontwikkelingen, waaronder de implementatie van de DUOX-pastechnologie. Opdrachtnemer verstrekt hiervoor een roadmap en aanvullende bewijsstukken, zoals testresultaten, ontwikkelplannen of andere relevante documentatie, waaruit blijkt dat deze ontwikkeling actief wordt gerealiseerd. |
| 5.5 | Informatie over welke personeelspas bij welke gebruiker hoort, wordt verkregen via de koppeling met One Identity Manager (OIM) van Amsterdam UMC. Opdrachtnemer dient hierbij te voldoen aan bijlage 2: NFU Algemene Inkoopvoorwaarden zoals bijgevoegd bij eis 5.6. |
| 5.6 | Intrekkingen en toevoegingen van personeelspassen van gebruikers in het CMS worden automatisch doorgegeven via OIM en verwerkt in de beheerapplicatie van de sleutelkasten. Opdrachtnemer dient hierbij te voldoen aan de bijlage 2: NFU Algemene Inkoopvoorwaarden zoals bijgevoegd bij eis 5.5. |
| 5.7 | De maximale uitgiftetijd bedraagt 15 seconden. Dit geldt voor het gehele systeem. Iedere sleutelbos wordt derhalve binnen 15 seconden vrijgegeven, ongeacht de locatie en kast (totaal 11 kasten binnen het systeem, plus twee mogelijke). |
| 5.8 | Sleutels hebben een vaste positie teneinde de uitgifte te versnellen. |
| 5.9 | Voor gebruikers die slechts één sleutel kunnen uitnemen, geeft de kast de desbetreffende positie direct vrij. |

| | |
|---|---|
| 5.10 | Indien pashouders meerdere sleutelbossen kunnen ophalen, maakt de sleutelhouder een keuze welke sleutelbos wordt uitgenomen. Deze keuze kan mechanisch worden gemaakt (via een knop in de kast bij de sleutelpositie) of softwarematig via het (touch)screen. |
| 5.11 | De applicatie van de sleutelkasten kan notificaties versturen wanneer sleutels niet op tijd worden ingeleverd. Deze notificaties worden verzonden via SMS en/of e- mail. |

| **6.** | **Toegang en bewaking** |
|---|---|
| 6.1 | De sleutelkasten beschikken over de mogelijkheid om de deur handmatig en mechanisch te ontgrendelen. Deze mogelijkheid is uitsluitend beschikbaar voor gebruikers met een specifieke autorisatie. |
| 6.2 | De sleutelkasten bevatten een mogelijkheid om handmatig, mechanisch een sleutelpositie te kunnen ontgrendelen in de kast. Deze mogelijkheid is alleen te gebruiken door gebruikers met een speciale autorisatie. |
| 6.3 | Het is mogelijk om gebruikers beheerder te maken van alleen een deel van de sleutelposities in één of meerdere sleutelkast(en). |
| 6.4 | Gebruikers die zich bij de sleutelkast hebben geauthentiseerd, worden automatisch uitgelogd 15 seconden na het uitnemen van hun sleutel(s). |
| 6.5 | Sleutelkasten zijn voorzien van een signalering wanneer de deur onbevoegd wordt geopend. Deze signalering wordt in de vorm van een alarm doorgestuurd naar de meldkamers van Amsterdam UMC. De alarmen van de kasten op locatie VUmc komen binnen in de meldkamer VUmc en de alarmen van de kasten locatie AMC in de meldkamer van AMC. De applicatie voorziet in een actieve pop-up en bijbehorend akoestisch signaal bij alarmmeldingen. |
| 6.6 | Sleutelkasten dienen verankerd te worden aan vloer en/of muur om diefstal te voorkomen. |

| **7.** | **Koppelingen met andere systemen** |
|---|---|
| 7.1 | Indien gewenst kan Opdrachtnemer gebruik maken van de paslezers van de aanwezige toegangssystemen. Op locatie AMC betreft dit ATS van EAL en op locatie VUmc is dit AEOS van NEDAP. De keuze voor wat betreft paslezer is vrij, mits deze AMC- en VUmc-pas uitleest op de wijze zoals beschreven in de overige eisen. Het heeft de voorkeur dat nieuwe paslezers, passend bij de functionaliteit van de te vervangen paslezers, worden toegepast (nieuw te leveren door de Opdrachtnemer). |
| 7.2 | Bestaande kasten (enkelvoudig of dubbelvoudig uitgevoerd) zijn voorzien van een intercom met video per bedienpaneel (waar de paslezer en het pincodetableau zijn geplaatst). Deze voorzieningen moeten worden overgezet (hergebruikt). Zowel intercom- als videostream komen binnen op het bestaande Commend-platform op locatie AMC, en op het bestaande Alphacom-stentafon platform op locatie VUmc. Dit dient na de overplaatsing/migratie van de posten volledig werkend te worden opgeleverd. Hiervoor kunnen bestaande netwerkaansluitingen gebruikt worden. Aan de zijde van VUmc zijn deze posten niet aanwezig. |
| 7.3 | Het systeem dient gekoppeld te worden aan het nog in ontwikkeling zijnde PIAM-systeem van Amsterdam UMC. Dit kan plaatsvinden middels een API of een SCIM-koppeling. De mate waarin deze koppeling wordt gerealiseerd vormt een gunningscriterium( zie leidraad). Een REST API is de minimale eis. |
| 7.4 | Op locatie VUmc wordt een koppeling met de aanwezige applicatie Winguard gerealiseerd.<br>Op locatie AMC wordt een koppeling met de aanwezige applicatie Inter gerealiseerd. |

| **8**. | **Levering en installatie** |
|---|---|
| 8.1 | Levering en installatie vinden uitsluitend plaats binnen reguliere werktijden (ma-vr tussen 7-17h) van Amsterdam UMC. |
| 8.2 | Bulkleveringen voorafgaand aan de installatie zijn niet toegestaan. Levering van de kasten vindt plaats per kast, rond de montagedatum van de betreffende kast. |
| 8.3 | De totale levering, inclusief installatie, vindt plaats in Q1 van 2027 in overleg met Amsterdam UMC. |

| | |
|---|---|
| 8.4 | Ten aanzien van de technische projectbeheersing stelt de leverancier een projectimplementatieplan op, met als doel dat de totale levering en installatie (inclusief alle koppelingen) beheerst en bedrijfszeker te laten plaatsvinden. Onderdeel hiervan zien we minimaal:<br>• 230V en data-aansluitingen reeds beschikbaar;<br>• FAT test;<br>• SAT test met alle koppelingen werkend;<br>• Eerst één kast als proof of concept met alle koppelingen werkend, bijvoorbeeld V01;<br>• Hersteltijd (bijvoorbeeld 2 weken) voor implementeren lessons-learned uit de proof of concept;<br>• Meenemen overzetten intercom en video (locatie AMC) en koppelingen met andere systemen;<br>• Uitrol overige sleutelkasten volgens een vastgestelde watervalplanning (conform het proces zoals in de punten hierboven, zonder hersteltijd). |
| 8.5 | Leverancier neemt onderstaande mee in projectimplementatieplan:<br>• Overzetten bestaande sleutelbossen op nieuwe ringen en identifiers van kasten;<br>• Tijdelijke handmatige uitgifte bossen;<br>• Bewaking op tijdelijk uitgegeven sleutelbossen;<br>• Communicatie naar Opdrachtgever over implementatiestappen en planning;<br>• Opleiding en training;<br>• Demarcatie wie doet wat: welke taken worden door leverancier uitgevoerd, welke taken zijn voor Opdrachtgever;<br>• Planning alle onderdelen (totale doorlooptijd, watervalplanning). |
| 8.6 | Installatie omvat het volledig werkend opleveren van zowel de hardware als bijbehorende software. Inclusief koppelingen en het overzetten van sleutelposities. |
| 8.7 | De opdrachtnemer wordt gezien als hoofdaannemer en heeft coördinerende taken voor de totale opdracht met eventuele onderaannemers. De hoofdaannemer is het enige aanspreekpunt van Opdrachtgever. |
| 8.8 | Een van de partijen waarmee afstemming moet plaatsvinden is Intragen voor de ontwikkeling van de koppeling met One Identity Manager (de PIAM-applicatie). |
| 8.9 | De opdrachtgever verzorgt, voor zover deze ontbreken, de benodigde data aansluitpunten, activatie van de aansluitpunten (MAC-adres), 230V-aansluitpunten en de bouwkundige afwerking op aanwijzing van de Opdrachtnemer (Opdrachtnemer coördineert dit conform eis9.7). |
| 8.10 | Op verzoek van Opdrachtgever levert Opdrachtnemer van de aangeboden apparatuur die beschikt over een MAC-adres - voorafgaand aan levering en installatie, het MAC-adres per serienummer aan, teneinde netwerktoegang te bespoedigen. |
| 8.11 | De opdrachtnemer dient de opdrachtgever te begeleiden middels instructie in het gebruik van de sleutelkasten en de bijbehorende systemen. Qua opleiding wordt voorzien in trainingen voor:<br>• Servicemedewerkers HVT: eerste lijns storingen (2 dagdelen)<br>• FAB-medewerkers SRM: gehele systeem (4 dagdelen)<br>• Gebruikers (centralisten Meldkamer/beveiligers): monitoren, noodprocedures en vrijgave posities op afstand (8 dagdelen) |
| 8.12 | Bij oplevering dient de Ultimo upload lijst (Bijlage 3.4) volledig ingevuld te worden door Opdrachtnemer. |
| 8.13 | De gegunde Opdrachtnemer dient voorafgaand aan levering de locaties in te meten en de maatvoering te verifiëren. Indien na deze verificatie blijkt dat geleverde kasten niet passend zijn voor de betreffende locatie, ligt het risico en de verantwoordelijkheid hiervoor bij Opdrachtnemer. |

| **9**. | **Garantie en onderhoud** |
|---|---|
| 9.1 | Op de geleverde sleutelkasten en bijbehorende software geldt een garantieperiode van minimaal vijf (5) jaar, inclusief herstel van gebreken. De garantieperiode gaat in na oplevering. |
| 9.2 | Updates dienen gedurende de maximale looptijd van de overeenkomst (15 jaar) beschikbaar te zijn. |
| 9.3 | Gedurende de garantieperiode verzorgt Opdrachtnemer het kosteloos onderhoud, inclusief updates en noodzakelijke vervangingen. De aanbieding omvat derhalve vijf (5) jaar onderhoud, met een optie op nog |

| | |
|---|---|
| | eens tien (10) jaar. De onderhoudskosten zijn afzonderlijk gespecificeerd. Deze kosten worden jaarlijks gefactureerd. De voorgestelde indexering wordt eenmalig toegepast aan het einde van de looptijd. |
| 9.4 | Eventuele fabrieksgarantie (naar verwachting circa 1–2 jaar) maakt onderdeel uit van de totale garantie, maar laat de contractueel vereiste garantieperiode onverlet. |
| 9.5 | Onderhoud bestaat uit preventief onderhoud, correctief onderhoud en software assurance. De software assurance is inbegrepen bij de jaarlijkse SAAS kosten. Voor het preventieve onderhoud (volgens fabrieksvoorschriften) wordt jaarlijks een onderhoudsbeurt uitgevoerd. Bij storingen wordt correctief onderhoud uitgevoerd.<br>Preventief en correctief onderhoud vinden plaats binnen afgesproken responstijden, passend bij een kritische zorgomgeving. |
| 9.6 | Ingeval van storing wordt verwacht:<br>• Responstijd: 4 uur (op werkdagen tussen 6:00 en 18:00)<br>• Responstijd: 8 uur (op weekend/feestdagen)<br>• Oplostijd: 12 uur of uiterlijk bij aanvang van de eerstvolgende werkdag |

| **10** | **Rapportage** |
|---|---|
| 10.1 | De beheerapplicatie kan rapportages maken en deze exporteren naar PDF en Excel.<br>Er zijn minimaal de volgende rapportages beschikbaar:<br>• Rapportages van handelingen per gebruiker en handelingen per sleutel.<br>• Overzichtsrapportages voor kastindelingen.<br>• Analyse gebruik van sleutels en sleutelposities<br>• Foutcodes registratie |

| **11.** | **Eisen gebruiksartikelen** |
|---|---|
| 11.1 | Gebruiksartikelen zijn van degelijke kwaliteit |
| 11.2 | De aangeboden en vastgelegde sleutelposities vormen geen belemmering voor de huidige sleutelaccesoiressen (momenteel worden Sensormatic -systemenen stevige relatief grote stalen ringen toegepast) |

| **12.** | **Eisen Infectiepreventie** |
|---|---|
| 12.1 | De aangeboden apparatuur is bestand tegen regelmatige reiniging en desinfectie met de in het Amsterdam UMC toegestane desinfectantia en schoonmaakmiddelen:<br>• Disposable microvezeldoek met water;<br>• Incidin Oxy middelen: Oxy wipes Oxy Foam en Oxy Can (met een minimale contacttijd van 30 seconden);<br>• Alcohol 70% (met minimale contacttijd van 1 minuut);<br>• Chlooroplossing 1000ppm (met minimale contacttijd van 5 minuten). |
| 12.2 | Oppervlakken zijn glad en goed bereikbaar voor reiniging en desinfectie. |
| 12.3 | Losse en zichtbare bedrading is niet toegestaan. |
| 12.4 | De aangeboden apparatuur wordt geleverd met een Nederlandstalig reinigings- en desinfectievoorschrift. |

| **13** | **Facturatie** |
|---|---|
| 13.1 | Leverancier dient zijn facturen,bij voorkeur digitaal (PDF bestand), te richten aan:<br>AMC<br>Crediteurenadministratie<br>Postbus 400<br>1115 ZJ DUIVENDRECHT<br>crediteuren.amc@amsterdamumc.nl<br>facturen.amc@amsterdamumc.nl |

| | |
|---|---|
| 13.2 | Op de facturen dienen specifiek de volgende gegevens te worden vermeld:<br>• Ordernummer AMC (Duidelijk zichtbaar en bovenaan iedere factuur);<br>• Leveringsdatum;<br>• Het aantal geleverde goederen of diensten;<br>• Een omschrijving van de geleverde goederen of diensten. |
| 13.3 | Voor het overige dienen uw facturen te voldoen aan de vereisten die de wet hieromtrent stelt, zoals:<br>• Uw naam, adres en btw-nummer;<br>• Uw KvK-nummer;<br>• Een uniek volgnummer;<br>• De datum waarop de factuur is gemaakt;<br>• De naam en het adres van het AMC;<br>• De datum waarop, of het tijdvak waarin de goederen of diensten zijn geleverd;<br>• Het btw-tarief dat u in rekening brengt;<br>• Het bedrag dat u in rekening brengt, exclusief btw;<br>• Het btw-bedrag. |
| 13.4 | Leverancier dient te voldoen aan inkoopvoorwaarden van Amsterdam UMC, waaronder:<br>• Geheimhouding;<br>• Personeel dient te beschikken over een VOG;<br>• Aansprakelijkheidsverzekering met een dekking van € 2,5 miljoen per gebeurtenis;<br>• Voor meerwerk dient hiervoor bij uitvoering vooraf opdracht te zijn verstrekt. |

| **14** | **Indexering** |
|---|---|
| 14.1 | Indexering is uitsluitend toegestaan indien en voor zover dit expliciet is vastgelegd in de Aanbestedingsdocumenten, het Prijzenblad en/of deze Overeenkomst. De tarieven kunnen jaarlijks per 1 januari worden geïndexeerd op basis van het Dienstenprijsindexcijfer (DPI) van het Centraal Bureau voor de Statistiek (CBS). De eerste indexering mag plaatsvinden per 1 januari 2028. |
| 14.2 | Leverancier dient een voorstel voor indexering uiterlijk één (1) maand voorafgaand aan de beoogde indexeringsdatum schriftelijk en gemotiveerd aan UMC voor te leggen, inclusief een onderbouwing van de toegepaste indexering. Indexering kan uitsluitend worden toegepast na voorafgaande schriftelijke instemming van UMC. Indien het toepasselijke DPI-percentage negatief is, blijven de geldende tarieven ongewijzigd. |

## 3 Deel 2 – ICT Eisen

| 1. | Algemeen |
|---|---|
| ICT.1.001 | De beantwoording van onderstaande eisen en wensen is van toepassing op alle onderdelen en componenten van de door leverancier aangeboden dienstverlening en/of oplossing. |
| ICT.1.002 | De door u aangeboden Systeem inclusief alle componenten - w.o. licenties - die worden geleverd e/o aangeschaft mogen worden gebruikt door alle gebruikers en op alle locaties van Amsterdam UMC. Hierop zijn geen uitzonderingen of restricties van toepassing in termen van gebruikersrecht, functionaliteit, ondersteuning/support of anderszins. |
| ICT.1.003 | Opdrachtnemer werkt conform onderstaande regelementen:<br>Bijlage 3.5: Richtlijn soevereiniteit UMC<br>Bijlage 3.6: Clouddiensten beleidskader ICT |

| 2. | Amsterdam UMC ICT - beleid |
|---|---|
| ICT.2.001 | Na eventuele gunning zal de leverancier zich committeren aan de aanwijzingen uit het “Self Assessment Leveranciers” en zal deze aanvullende checklist volledig invullen en waar van toepassing de gevraagde gegevens aanleveren. |
| ICT.2.002 | Leverancier heeft kennis genomen van ICT 'Beleidskader Cloud-applicaties" en conformeert zich daaraan. |

| 3. | ICT Applicatie |
|---|---|
| ICT.3.001 | Het webbased gedeelte van het aangeboden Systeem werkt met de meest recente versie van de internetbrowser Microsoft Edge. |
| ICT.3.002 | De applicatie van het aangeboden Systeem voorziet in gegevensvalidatie en ondersteunt uitsluitend de benodigde tekens voor de invoer van gegevens t.b.v. optimale gegevensregistratie. |

| 4. | Architectuur |
|---|---|
| ICT.4.001 | Het aangeboden Systeem voldoet aan de volgende security-aspecten:<br>• Security by design: leverancier houdt rekening met security aspecten bij het ontwerp naast de functionele eisen voor een goede werking<br>• Security by default: Alle standaard instellingen staan default op secure (veilig) ingesteld. |

| 5. | Authenticatie & Autorisatie |
|---|---|
| ICT.5.001 | "Het aangeboden Systeem kan voor authenticatie en autorisatie omgaan met Active Directory, eventueel via federatie.<br>1. In het geval van Active Directory ondersteunt de applicatie authenticatie respectievelijk Kerberos of LDAP<br>2. In het geval van Federatie ondersteund de oplossing respectievelijk: OpenID Connect (OIDC)/oAuth2 of SAML 2.0" |
| ICT.5.002 | Authenticatie van gebruikers op basis van cryptografische techniek, hardware tokens of challenge/response protocollen (sterke authenticatie) vindt in ieder geval plaats in de volgende situaties:<br>• wanneer Single Sign-On wordt toegepast;<br>• bij toegang vanuit een onvertrouwd netwerk;<br>• bij beheer van kritische beveiligingsvoorzieningen (zoals firewalls, Intrusion Detection and Prevention Systems en routers). |
| ICT.5.003 | Door het aangeboden Systeem specifieke accounts worden voorzien van sterke wachtwoorden. Deze wachtwoorden zijn instelbaar om zo te kunnen voldoen aan de Amsterdam UMC richtlijnen (w.o. minimale lengte, vereiste complexiteit, lock-out mogelijkheden). |
| ICT.5.004 | Wachtwoorden worden versleuteld gecommuniceerd over het netwerk tussen client en server. |

| | |
|---|---|
| ICT.5.003 | Aan de hand van het toegangsbeveiligingsbeleid richt de leverancier beveiligde inlogprocedures voor systemen en toepassingen in. De inlogprocedures omvatten ten minste een sterk wachtwoord in combinatie met 2-factor authenticatie. |
| ICT.5.004 | De bevoegdheid tot het uitvoeren van specifieke handelingen binnen het aangeboden Systeem, is per medewerker of groep medewerkers met behulp van privileges instelbaar. |
| ICT.5.005 | Het beheer van de rechten bij gebruikers binnen het aangeboden Systeem moet geregeld kunnen worden vanuit het centrale Amsterdam UMC IAM systeem. |

| **6.** | **Continuïteitsbeheer** |
|---|---|
| ICT.6.001 | De leverancier heeft aantoonbare preventieve en correctieve maatregelen geïmplementeerd, zodat de beschikbaarheidseisen effecitief worden beschermd. Denk bijvoorbeeld aan een bescherming tegen DDoS aanvallen. |
| ICT.6.002 | De leverancier heeft zich op de hoogte gesteld van en is bekend met de infrastructuur van de Opdrachtgever en onderkent eventuele single points of failure (SPoF) die het aangeboden Systeem met zich meebrengt. |
| ICT.6.003 | Het aangeboden Systeem heeft de mogelijkheid voor het continu bewaken van de beschikbaarheid en capaciteit van applicaties en systemen. Overschrijdingen van drempelwaarden worden tijdig gesignaleerd. |
| ICT.6.004 | De leverancier maakt minimaal dagelijks een back-up conform overeengekomen beschikbaarheidseisen. De resultaten van de back-up worden vastgelegd. |
| ICT.6.005 | De leverancier heeft voor de geleverde diensten, continuïteits- of disasterrecovery herstelplannen beschikbaar, mocht een calamiteit zich voordoen. Deze plannen zijn beschreven en worden geactualiseert en getest minimaal elke 2 jaar. |
| ICT.6.006 | Het aangeboden Systeem beschikt over de mogelijkheid voor back-up voor de configuratie, instellingen, rekenregels en (drempel)waarden van de ICT-oplossing. Bij uitval is het Systeem te herstellen met het terugzetten van deze back-up, die in voorkomend geval weer eenvoudig is in te lezen. |

| **7.** | **Data exit strategie** |
|---|---|
| ICT.7.001 | De data is exporteerbaar in een leesbaar en machine importeerbaar formaat. Het datamodel van de opgeslagen data is beschikbaar en kan op verzoek van opdrachtgever verstrekt worden. |

| **8.** | **Data integriteit** |
|---|---|
| ICT.8.001 | Misbruik van bestaande sessies dient aantoonbaar te worden tegengegaan door sessiemanagement in te richten.<br>- Dat kan middels het toevoegen van security headers bij gebruik van HTTP.<br>- Andere protocollen zoals SMTP, IMAP, HL7, FHIR en SSH moeten met andere methoden aantoonbaar worden beveiligd.<br>- Er worden geen verouderde (legacy) protocollen gebruikt die een beveiligingsrisico met zich meedragen. |
| ICT.8.002 | Alle in- en uitvoer van data binnen het aangeboden Systeem wordt aantoonbaar genormaliseerd, gevalideerd en ingeperkt waarbij data-integriteit aantoonbaar wordt gewaarborgd |
| ICT.8.003 | Voor webdiensten geldt:<br>Het lekken van configuratiegegevens in headers, banners en error foutmeldingen op webpagina's dient aantoonbaar met technische maatregelen voorkomen te zijn. |

| **9.** | **Datamigratie** |
|---|---|
| ICT.9.001 | De software van het aangeboden Systeem bevat functionaliteit die het mogelijk maakt om data te importeren. |

| | |
|---|---|
| | De functionaliteit om data te importeren, valideert en test de import data. Hierbij worden dezelfde validatieregels toegepast die normaliter ook in de front-end van de applicatie van toepassing zijn. |
| ICT.9.002 | Het is mogelijk het aangeboden Systeem te configureren en velden toe te voegen om referenties naar de oude applicaties te laden. |
| ICT.9.003 | Leverancier verantwoordelijk voor datamigratie<br>De leverancier levert specialisten die expertise bijdragen voor het mappen van datavelden tussen de uit te faseren systemen en het aangeboden Systeem. |
| ICT.9.004 | Leverancier vervantwoordelijk voor datamigratie<br>De leverancier draagt bij aan de ontwikkeling van het datamigratie implementie draaiboek en stelt i.v.m. mogelijke afhankelijkheden de volgordelijkheid van het laden van datasets vast. |
| ICT.9.005 | Leverancier vervantwoordelijk voor datamigratie<br>De leverancier is verantwoordelijk voor het laden van de data, waar bij gebruik wordt gemaakt van een data import functie. Tijdens de bouw- en testfase wordt verwacht dat datafiles regelmatig geladen worden, om migratie processen te testen. |
| ICT.9.006 | Leverancier vervantwoordelijk voor datamigratie<br>Toegang tot de data is beveiligd, alleen de leverancier en Amsterdam UMC hebben toegang tot de data en de datamigratie omgeving. |
| ICT.9.007 | Er is versiecontrole op alle documenten, code en configuraties die geproduceerd worden ten behoeve van de datamigratie en kwaliteitsanalyse. |
| ICT.9.008 | De leverancier kan een datamigratie specialist inzetten die het data mapping proces faciliteert. |
| ICT.9.009 | Het door Amsterdam UMC goedgekeurde datamapping document vormt de basis voor het bouwen en testen van het data transformatieproces. |
| ICT.9.010 | Het transformatieproces heeft een filter waarbij de scope van een data migratie run kan worden gemanipuleerd. Dit filter is minimaal gebaseerd op:<br>1. Datumbereik van de analyse (van en tot datum), en/of<br>2. Type analyse (bijvoorbeeld microbiologie), en/of<br>3. Een lijst met sleutel-Ids van entiteiten (bijv. analyses of patiënten), en<br>4. Het voldoen aan de minimale eisen aan datakwaliteit (bijv. grenswaarden) |
| ICT.9.011 | De leverancier levert een geautomatiseerd en herhaalbaar transformatierapport, met minimaal de volgende informatie:<br>1. Reconciliatie tellingen van de belangrijkste entiteiten<br>2. Overzicht van de records die niet zijn getransformeerd (aantal en reden)<br>3. Details van de records die niet zijn getransformeerd (sleutel-Id en reden). |
| ICT.9.012 | De leverancier levert een herhaalbaar, efficiënt proces met een minimum aan handmatige stappen om de datakwaliteit van de geleverde data te analyseren. |
| ICT.9.013 | De datakwaliteit regels worden geconfigureerd gebaseerd op de datakwaliteit analyse in het data mapping document. |
| ICT.9.014 | De leverancier toont aan middels een testrapportage dat het gehele datakwaliteit analyse proces is gebouwd volgens specificaties uit het data mapping document en correct functioneert. |
| ICT.9.015 | Naast de output files wordt een datakwaliteit rapport geleverd als onderdeel van het datakwaliteit analyse proces. Dit rapport wordt automatisch gecreëerd met minimale handmatige stappen. Het rapport heeft minimaal de volgende informatie:<br>1. Overzicht van de records die voldoen aan de eisen<br>2. Overzicht van de records die niet voldoen aan de eisen (aantal en reden)<br>3. Details van de records die niet voldoen aan de kwaliteitseisen (sleutel-Id en reden) |

| **10.** | **Fysieke toegangsbeveiliging** |
|---|---|
| ICT.10.001 | Van het aangeboden Systeem zijn alle door de leverancier toegepaste IT-voorzieningen en apparatuur aantoonbaar fysiek beschermd tegen toegang door onbevoegden en tegen schade en storingen. De leverancier kan de werking van deze maatregel aantonen. |

| 11. | ICT - Netwerk |
|---|---|
| ICT.11.001 | Alle netwerkverbindingen naar de ICT-omgeving van Amsterdam UMC lopen altijd door een door Amsterdam UMC beheerde Firewall. Dit geldt ook als de leverancier als onderdeel van het aangeboden Systeem eigen netwerk componenten zoals Firewalls, Routers of Switches aanbiedt. |
| ICT.11.002 | Communicatie tussen systemen vindt plaats op basis van Fully Qualified Domain Name (FQDN DNS naam). |

| 12. | Incidentbeheer |
|---|---|
| ICT.12.001 | Datalekmeldingen<br>Er is aantoonbaar een procedure ingericht om de opdrachtgever tijdig en adequaat te informeren over potentiële datalekken waarvan hij kennis krijgt (inclusief die bij sub-verwerkers) en documenteert bij een incident alle stappen die zijn ondernomen in het kader van de meldplicht datalekken. |
| ICT.12.002 | Security incidenten melden<br>Er is aantoonbaar een procedure ingericht om de opdrachtgever tijdig en adequaat te informeren over potentiële securityincidenten waarvan hij kennis krijgt (inclusief die bij zijn sub-verwerkers) en documenteert bij een incident alle stappen die zijn ondernomen in het kader van de meldplicht Cyberbeveiligingswet (NIS2) melden security incidenten. |
| ICT.12.003 | Incidentbeheer<br>De leverancier heeft aantoonbaar een proces voor incidentenbeheer in gebruik met functiebeschrijvingen, waarin de taken met betrekking tot incidentenbeheer zijn opgenomen. In het proces wordt onderscheid gemaakt tussen de activiteiten classificeren, prioriteren, diagnosticeren, communiceren en dossiervorming. |

| 13. | Integratie |
|---|---|
| ICT.13.001 | Het aangeboden Systeem biedt ondersteuning bij het uitvoeren van een harmonisatieslag. Een harmonisatieslag houdt ten minste in, het samenvoegen van afdelingen met hun processen, werkwijzen en inrichting van systemen en datasets. |
| ICT.13.002 | Ingeval koppelingen vereist zijn maakt het aangeboden Systeem gebruik van één van onderstaande integratie-standaarden:<br>- HL7 v2 of v3 conformance statement<br>- HL7 FHIR<br>- XML<br>- ASTM<br>- DICOM<br>- Bestand import |

| 14. | Licenties |
|---|---|
| ICT.14.001 | Het aangeboden Systeem bevat een site-licenties voor de alle aangeboden omgevingen (bijv. Acceptatie en Test (OTAP)), eventueel gesplitst per locatie van de Opdrachtgever en ongeacht het aantal gebruikers (gedurende de looptijd). |
| ICT.14.002 | Het aangeboden Systeem bevat alle licenties voor elke benodigde middleware toepassing ten behoeve van de Opdrachtgever (bijvoorbeeld als Oracle Java wordt gebruikt). Dit gedurende de looptijd van de overeenkomst en ongeacht het aantal gebruikers. |
| ICT.14.003 | De leverancier verzorgt alle licenties die nodig zijn voor de gewenste en gevraagde functionaliteit, het aantal gebruikers en het verwacht gebruik inclusief het onderhoud en support op de geleverde licenties. |

| | |
|---|---|
| ICT.14.004 | De toegang voor de gelicentieerde gebruikers tot het aangeboden Systeem en/of de in gebruik zijnde functionaliteit zal nooit blokkeren naar aanleiding van overschrijding van de licentievoorwaarden. |
| ICT.14.005 | Er worden geen licentie keys welke via een hardware oplossing werken gebruikt (Bijv. USB dongles). |
| ICT.14.006 | Indien er componenten worden geïnstalleerd voor automatische controle van licenties, mogen deze niet leiden tot single point of failure (SPoF) of het niet functioneren van het aangeboden Systeem op werkplekken van de Opdrachtgever. |
| ICT.14.007 | De leverancier ondersteunt het gebruik van het aangeboden Systeem of andere ICT-componenten behorende bij deze aanbesteding, inclusief updates/fixes/patches/upgrades/nieuwe versies voor die releaseversie, gedurende de gehele looptijd van het contract en eventuele verlenging. |
| ICT.14.008 | Desgevraagd ondersteunt Leverancier Amsterdam UMC bij de implementatie van aangeleverde Updates/patches/upgrades/nieuwe versies. Ondersteuning kan on- of off-site plaatsvinden ter beoordeling Amsterdam UMC. De kosten voor de ondersteuning zijn in de aanbieding opgenomen. |

| **15.** | **Logging** |
|---|---|
| ICT.15.001 | Integriteit: Logging events zijn beveiligd tegen onbedoelde aanpassingen, ook van beheerders met hoge rechten. |
| ICT.15.002 | Applicatie-beheerders van Amsterdam UMC kunnen zelf direct bij de logging van het aangeboden Systeem. |
| ICT.15.003 | Het aangeboden Systeem houdt logging bij over de prestaties van de apparatuur en eventuele foutmeldingen en technische storingen. |

| **16.** | **Logische toegangsbeveiliginig** |
|---|---|
| ICT.16.001 | Alle autorisaties vinden aantoonbaar plaats op basis van functiescheiding en volgens het least privilege principe. Er is scheiding van bevoegdheden rond taken, verantwoordelijkheden en bevoegdheden met aantoonbaar extra aandacht voor accounts met hoge privileges, zoals administrators. |
| ICT.16.002 | Voor het aangeboden Systeem geldt:<br>Rollen moeten op gebruikersniveau toegewezen kunnen worden waarbij het inzichtelijk moet zijn wanneer een gebruiker aan meerdere rollen gekoppeld wordt. Bijvoorbeeld bij het uitvoeren van beheerwerkzaamheden.<br>Rollen kunnen bijvoorbeeld op basis van modules/functionaliteiten (incl. lees- of wijzigingsrechten) op scherm/functie/tabblad niveau ingesteld worden. |
| ICT.16.003 | De inlogprocedures omvatten, gezien de gevoeligheid van deze gegevens, sterke authenticatie met minimaal multi-factor authenticatie. |
| ICT.16.004 | De leverancier volgt aantoonbaar een formeel proces voor het beheer van toegangsrechten van gebruikers en beheerders.<br>Het toegangsbeheerproces omvat tenminste:<br>• het registreren van gebruikers en de aan hen toegekende rechten,<br>• het toekennen van niet meer rechten dan nodig voor de uitoefening van taken en<br>• het wijzigen of intrekken van die rechten bij wijziging of beëindiging van het dienstverband of contract |
| ICT.16.005 | De beheerders die in dienst zijn van of namens de leverancier toegang tot het aangeboden Systeem hebben, worden aantoonbaar<br>• op de hoogte gesteld van het toegangsbeveiligingsbeleid en<br>• ondertekenen een verklaring dat zij persoonlijke geheime authenticatie-informatie geheimhouden en in geval van inbreuk direct maatregelen nemen om de gevolgen te beperken. |

| | |
|---|---|
| ICT.16.006 | De leverancier controleert van beheerders minimaal elke 6 maanden of de toegangrechten tot het aangeboden Systeem nog conform het toegangsbeveiligingsbeleid is en voert zonodig correcties uit. |
| ICT.16.007 | Bij multi-factor authenticatie (MFA) maakt de inlogprocedures gebruik van federatie op basis van Active Directory Federation Services (ADFS), Security Assertion Markup Language (SAML), FIDO2 of gelijkwaardige protocollen. |
| ICT.16.008 | Met betrekking tot Single Sign On (SSO).<br>De inlogprocedures die gebruik maken federatie op basis van Active Directory Federation Services (ADFS), Security Assertion Markup Language (SAML), FIDO2 of gelijkwaardige protocollen. Kan hiermee Single Sign LogOn (SSO) gefaciliteerd worden? |

| **17.** | **Normen en kaders** |
|---|---|
| ICT.17.001 | Leverancier zal geen persoonsgegevens verwerken of laten verwerken door hemzelf of door derden in landen buiten de Europese Economische Ruimte ('EER') noch doorgifte van persoonsgegevens naar een land buiten de EER toestaan of toegang verlenen tot persoonsgegevens, vanuit een land buiten de EER, zonder dat aan de AVG eisen die daarvoor gelden is voldaan en Amsterdam UMC daarvoor voorafgaand contractueel toestemming heeft gegeven. |
| ICT.17.002 | Het aangeboden Systeem dient functionaliteit te bieden waarmee Amsterdam UMC invulling kan gegeven aan "het recht op vergetelheid" conform de betreffende richtlijnen geformuleerd door de Autoriteit Persoonsgegevens. |

| **18.** | **Opleidingen** |
|---|---|
| ICT.18.001 | Opleiding van functioneel en (wanneer relevant) technisch beheerders is onderdeel van uw aanbieding. |

| **19.** | **Organisatie van informatiebeveiligingsbeleid** |
|---|---|
| ICT.19.001 | Rollen Informatiebeveiliging<br>De leverancier heeft de verantwoordelijkheden met betrekking tot Informatiebeveiliging gedefinieerd en vastgelegd, en toegepast in de vorm van functiebeschrijvingen. |

| **20.** | **Performance** |
|---|---|
| ICT.20.001 | Het aangeboden Systeem kan omgaan met voorziene en onvoorziene toe- en afname in minimaal 25% van het in de overeenkomst overeengekomen aantal gebruikers, hoeveelheid gegevens en de belasting van het Systeem. |
| ICT.20.002 | De Leverancier checkt regelmatig of de performance prestaties gelijk zijn gebleven en/of geeft advies waarmee bestaande performance op peil gehouden kan worden. Denk hierbij aan veranderingen in productie, upgrades en updates. Afspraken hierover worden in de SLA vastgelegd. |
| ICT.20.003 | De leverancier neemt conform een af te sluiten Service Level Argeement (SLA) verantwoordelijkheid voor zijn invloed op de performance en werkt constructief samen indien er performanceproblemen worden ervaren. |

| **21.** | **Privacy** |
|---|---|
| ICT.21.001 | Het aangeboden Systeem voldoet aan de zeven principes voor privacy by design:<br>1. Proactive not reactive<br>2. Privacy as the default setting<br>3. Privacy embedded into design<br>4. Full functionality<br>5. Transparantie & recht op informatie |

| | |
|---|---|
| | 6. Respect for User Privacy<br>7. End-to-End security |

| **22.** | **Risico Analyse** |
|---|---|
| ICT.22.001 | Risico analyse<br>De leverancier voert aantoonbaar ten minste jaarlijks een risicoanalyse uit om de bedreigingen en kwetsbaarheden, de gevolgen daarvan voor de organisatie en de kans op die gevolgen in kaart te brengen. Op basis van de risicoanalyse worden adequate beveiligingsmaatregelen vastgesteld en ingevoerd. |

| **23.** | **SaaS oplossing** |
|---|---|
| ICT.23.001 | Het aangeboden Systeem betreft een SaaS oplossing waarbij de leverancier verantwoordelijk is voor het beschikbaar maken en beheren (operations, d.w.z. technisch beheer, inclusief serverbeheer en databasebeheer) en het door ontwikkelen (development). De kosten hiervan zijn opgenomen in het aanbod. |
| ICT.23.002 | In voorkomende gevallen kan de Opdrachtgever gebruik maken van de exit-strategie die de leverancier standaard aanbiedt.<br><br>In de verificatie fase wordt een exit-plan opgesteld. |

| **24.** | **Serviceverlening** |
|---|---|
| ICT.24.001 | Leverancier biedt een Service desk.<br>De Service desk is bemand met gekwalificeerd personeel van de Opdrachtnemer dat in staat is de meldingen van het Amsterdam UMC ten aanzien van de opdracht te behandelen (een zogenaamde skilled Service desk). |
| ICT.24.002 | De Service desk van de Leverancier is minimaal 5 x 9 telefonisch bereikbaar. |
| ICT.24.003 | Bij de Service desk kunnen beheerders van de Opdrachtgever meldingen doen (storing, ondersteuning, opdracht, kennisgeving, vraag, etc.).<br>Aanvragen aangaande onder meer offertes, bestelopdrachten, leveringen, gebreken, garantie, klachten en overige aspecten verlopen ook via de Service Desk. |
| ICT.24.004 | Opdrachtnemer biedt 5 x 9 ondersteuning waarbij de gestelde prioriteiten van meldingen in de SLA gelden.<br>Escalatiepaden zijn beschikbaar inclusief bereikbaarheidsinformatie. |
| ICT.24.005 | Opdrachtnemer behandelt incidenten op basis van een door het Amsterdam UMC aangegeven incident classificatie (Urgent, Hoog, Midden, Laag).<br>In onderling overleg tussen Amsterdam UMC en Opdrachtnemer kan de urgentie van een individueel incident worden aangepast. In geval geen overeenstemming kan worden bereikt, bepaalt Amsterdam UMC de incident classificatie. |
| ICT.24.006 | Opdrachtnemer levert probleemmanagement ten behoeve van het door Opdrachtnemer beheerde deel van het aangeboden Systeem. Repeterende incidenten worden voorkomen door het actief opsporen van structurele fouten (via root cause analysis) en het initiëren van de hiervoor benodigde wijzigingen (via change management) conform de in het SLA overeengekomen service-levels. |
| ICT.24.007 | Leverancier rapporteert schriftelijk in een vaste afgesproken frequentie (minimaal half jaarlijks) de ontvangen, opgeloste en in behandeling zijnde meldingen in het aangeboden Systeem en de aan Amsterdam UMC gemelde inbreuken op de informatiebeveiliging.<br>Alle gerapporteerde zaken worden binnen de vastgestelde termijnen in de SLA opgelost. |

| | |
|---|---|
| ICT.24.008 | Het aangeboden Systeem kan overal en 7 x 24 uur worden gebruikt. |

| **25.** | **Technische kwetsbaarheden** |
|---|---|
| ICT.25.001 | De leverancier voert aantoonbaar een intern proces ter voorkoming van het introduceren van technische (security) kwetsbaarheden in het aangeboden Systeem.<br><br>Het proces omvat in ieder geval een regelmatige evaluatie van het product op basis van het steeds veranderende dreigingslandschap die bij impact leiden tot een adequate aanpassing in het systeem teneinde de dreiging weg te nemen.<br>Het proces omvat in ieder geval:<br>• het regelmatig up-to-date houden van systemen en software (patching),<br>• het tijdig vergaren van informatie over nieuwe kwetsbaarheden (intelligence),<br>• het geautomatiseerd controleren van programmapakketten en infrastructurele programmatuur op bekende zwakheden,<br>• het continu testen van webapplicaties op kwetsbaarheden (Web vulnerability scanning) en het uitvoeren van een penetratietest ten minste eenmaal per jaar,<br>• het gebruik van anti-malware (inclusief antivirus) software van verschillende marktpartijen met verschillende engines die geactualiseerd zodra updates beschikbaar zijn,<br>• beperkingen op het installeren van (ongeautoriseerde) software. |
| ICT.25.002 | De leverancier inspecteert aantoonbaar alle gegevensverkeer vanuit externe en/of niet-vertrouwde netwerken in (near) real-time. |
| ICT.25.003 | De leverancier voert aantoonbaar een Intrusion Detection/Prevention Systeem dat netwerk gebaseerde aanvallen herkent op basis van:<br>• signatures,<br>• protocolvalidatie en<br>• anomaly detection. |
| ICT.25.004 | De leverancier gebruikt hardening van het aangeboden Systeem, zodat alleen de noodzakelijke software wordt geactiveerd en/of Indien het niet mogelijk is (het systeem of de virtualisatielaag staan dit niet toe zonder functionaliteit te verliezen), wordt de dienst(en) geblokkeerd via gedocumenteerde filters, op de meest nabijgelegen netwerkcomponent die deze filtering kan verschaffen.<br><br>Hiermee worden uitsluitend voor de dienst(en) noodzakelijke services/protocollen aangezet. Overige services worden bij voorkeur verwijderd en als dat niet mogelijk is uitgeschakeld. |

| **26.** | **Toegangscontrole en logging** |
|---|---|
| ICT.26.001 | De leverancier legt aantoonbaar activiteiten die gebruikers uitvoeren op (persoons-) gegevens vast in logbestanden en registreert goedgekeurde en geweigerde pogingen om toegang te verkrijgen tot bronnen van deze gegevens. |
| ICT.26.002 | De leverancier heeft maatregelen genomen om logfaciliteiten en loggegevens in logbestanden te beschermen tegen<br>- vernietiging<br>- vervalsing en<br>- onbevoegde toegang. |
| ICT.26.003 | Voor het aangeboden Systeem legt de leverancier activiteiten van systeembeheerders en -operators vast en beoordeelt deze op (mogelijk) misbruik van toegangsrechten. |

| | |
|---|---|
| ICT.26.004 | De leverancier gebruikt aantoonbaar één bron als referentietijd voor alle onderliggende systemen en systeemcomponenten. Hierdoor worden alle relevante informatieverwerkende systemen gesynchroniseerd, zodat de nauwkeurigheid van logbestanden gewaarborgd is. |
| ICT.26.005 | De leverancier levert aan de Opdrachtgever op verzoek een rapportage waarin ten minste zijn opgenomen. Het rapport wordt zo snel mogelijk, uiterlijk binnen 3 werkdagen aangeboden.<br>• Aantallen geslaagde en mislukte inlogpogingen;<br>• Data en tijden van niet succesvolle inlogpogingen;<br>• Gevraagde en verleende toegang tot gedeelde bestanden/informatie buiten de regulieren gebruikstijden;<br>• Activiteiten van beheerders;<br>• Significante gebruikershandelingen (zoals mutaties aan autorisaties, configuratieparameters en stamgegevens; afhankelijk van applicatie);<br>• Gedetecteerde malware (wormen/virussen/spyware e.d.) en storingen in de dienstverlening. |
| ICT.26.006 | De leverancier bewaart alle informatie in de logbestanden voor 6 maanden, tenzij wettelijke verplichtingen anders voorschrijven of de logbestanden nodig zijn voor onderzoek in het kader van een (vermoed) beveiligingsincident. Gedurende die periode kan deze informatie gegarandeerd worden ingezien door de Opdrachtgever. |

| **27.** | **Versleuteling** |
|---|---|
| ICT.27.001 | End-to-end versleuteling.<br>De leverancier versleutelt de privacygevoelige informatie over computernetwerken, in ieder geval in de volgende situaties:<br>• Alle internetverbindingen<br>• Sessies die beheerders opzetten naar computers voor het uitvoeren van beheerwerkzaamheden over het (eigen netwerk). Er worden dan encryptievoorzieningen binnen de beheertools (SSH bv) of door netwerkprotocollen zoals HTTPS toe te passen;<br>• Via draadloze datacommunicatie;<br>• Als er sensitieve informatie zoals wachtwoorden worden opgeslagen of verzonden via het netwerk |
| ICT.27.002 | De leverancier maakt gebruik van het versleuten van de verbinding en hashing algoritmen, bij externe verbindingen (bijvoorbeeld over het internet), die voldoen aan de huidige eisen en de OWASP standaarden. |
| ICT.27.003 | De leverancier verwijdert data van af te danken apparatuur en verwijderbare media, middels een secure erase procedure, voordat de hardware wordt afgevoerd of weggegooid.<br>Dit kan ook middels contractuele afspraken met een derde partij, die deze datadragers volgens een gecertificeerde methode (zoals WEEELABEX of gelijkwaardig) vernietigd. |
| ICT.27.004 | De leverancier hanteert een maximale geldigheidstermijn van 1 jaar voor cryptografische sleutels en certificaten. |

| **28.** | **Wijzigingsbeheer** |
|---|---|
| ICT.28.001 | De leverancier heeft aantoonbaar een proces ingericht voor wijzigingsbeheer, bijvoorbeeld op basis van ITIL v3 of hoger, danwel ISO 20000-1.<br><br>Er bestaan richtlijnen en procedures voor het wijzigen van hard- en software van de systemen. Hierbij wordt het change managementproces van Amsterdam UMC gerespecteerd. |
| ICT.28.002 | Leverancier houdt in haar software release en life-cycle rekening met de ontwikkelingen van onderliggende besturingssysteem, browsers, hardware en andere afhankelijkheden. |

| | |
|---|---|
| ICT.28.003 | Regulier onderhoud vindt buiten de reguliere werktijden plaats en kent een maximale downtime die aansluit bij het ondersteunde proces en nooit de 4 uur zal overschrijden. |
| ICT.28.004 | De leverancier voert wijzigingen uit binnen het overeengekomen service window (conform SLA). Indien een wijziging buiten dit service window moet plaatsvinden, is voorafgaande schriftelijke toestemming van de Opdrachtgever vereist. Wijzigingen mogen niet leiden tot onverwachte of ongeplande uitval. |
| ICT.28.005 | Na een update/aanpassing aan het systeem kan het systeem worden gecontroleerd d.m.v. vooraf opgestelde testprocedure. |
| ICT.28.006 | Tijdens het uitvoeren van updates is de leverancier desgewenst fysiek aanwezig op locatie. De kosten hiervoor zijn in de aanbieding verdisconteerd. |