Leveranciersvoorwaarden en checklist

Het Universitair Ziekenhuis Brussel (UZB) is bezorgd om de stabiliteit en veiligheid van zijn ICT-omgeving en om de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de gegevens van het ziekenhuis, zijn patiënten en medewerkers. Daarom wordt hieronder beschreven wat UZB verwacht wanneer opdrachtnemers of leveranciers (beide termen worden als synoniem van elkaar gebruikt) een oplossing – een applicatie, toestel, dienst, configuratie, … – voor UZB willen implementeren, ongeacht de gekozen of voorgestelde oplossing.

Op een intuïtieve wijze worden deze verwachtingen in verschillende hoofdstukjes telkens in de linkerkolom gekaderd waarna de opdrachtnemer in de rechter kolom en in bijlagen de gelegenheid krijgt om zijn keuzes te duiden door extra informatie te voorzien of gefundeerde alternatieven voor te stellen.

U zal merken dat UZB zich voor zijn verwachtingen op industry standards en best practices baseert. Het moedigt leveranciers aan om die standaarden ook zoveel mogelijk voor hun oplossing in te zetten. Dit verhoogt immers de efficiëntie voor alle betrokken partijen – niet alleen tijdens de selectie- en implementatiefase maar zeker en vast ook tijdens de gebruiksfase. Zo draagt u bij tot een stabiele en veilige ICT-omgeving. Medewerkers en patiënten zijn u dankbaar!

Een tijdig en kwalitatief ingevulde checklist, ten slotte, staat een kwalitatieve en vlotte analyse door UZB toe en draagt op die manier bij tot een goed begrip over de oplossing(en) en de leverancier en de eventuele risico's die met de oplossing(en) gepaard gaan. Dit zorgt dan weer voor een effectieve selectie en vlotte implementatie en samenwerking in een goede verstandhouding.

Heeft u bij het verwerken van de checklist bijkomende vragen of wenst u verduidelijking, contacteer dan uw contactperso(o)n(en) bij UZB die hiervoor werd(en) aangewezen. Belangrijk: gebruik steeds de referenties in de eerste kolom voor al uw vragen en bijlages. Uw contactpersoon zal u ook de timings communiceren voor de ontvangst van het ingevulde document. Het spreekt voor zich dat documenten die afwijken van de UZB-standaarden meer analyse- en overlegtijd zullen vergen.

Technologische verwachtingen

In dit luik wordt ingegaan op alle technische aspecten van de oplossing(en).

Kader

TK01	**Technologische oplossingen**	Vermeld hier welke oplossing(en) door u uitgewerkt wordt/worden in dit document: client/server (on-premise in de datacenters van UZB), XaaS, … Werkt u verschillende oplossingen uit, vermeld dan hier welke uw voorkeur geniet en waarom dat zo is.

TK02	**Evenwaardigheid** oplossingen. Indien de leverancier verschillende technologische oplossingen voorstelt, verwacht UZB dat alle oplossingen evenwaardig zijn op vlak van functionaliteit, technologie, beschikbaarheid, integriteit, vertrouwelijkheid en privacy.	Vermeld hier of en hoe de oplossingen al dan niet evenwaardig zijn.
TK03	**Ondersteuning in de tijd.** UZB verwacht dat voorgestelde oplossingen en al zijn componenten nog 5 jaar verkocht en 10 jaar ondersteund worden na aankoop.	Vermeld hier expliciet indien en voor welke (onderdelen van de) oplossing dit *niet* het geval is.

Client

TC01	UZB staat standaard in voor de aankoop en installatie/configuratie van alle client **hardware**, client licenties en verbonden apparatuur	Als dit in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TC02	UZB installeert en configureert zijn clients standaard op de meest recente **Windows** - release, hetzij op fysieke client hardware of op een VDI-oplossing. Updates worden automatisch en regelmatig toegepast.	Als dit in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB. Vermeld hier eventuele beperkingen om software op vmware horizon te draaien.
TC03	Clients worden standaard geïnstalleerd met (een/de meest recente) versie van deze **software**: - Microsoft Edge & Google Chrome - Adobe Acrobat Reader - TrendMicro ApexOne Antivirus - Office 365 - .net en worden door UZB geconfigureerd, beheerd en geüpdatet. Software voor remote monitoring en remote management wordt niet toegelaten. Remote toegang kan enkel toegestaan worden na overleg met en akkoord van UZB.	Andere software met dezelfde functionaliteit wordt niet toegestaan. Indien de hiernaast opgelijste software en zijn beheer in het kader van de voorgestelde oplossing niet wenselijk is, vermoed wordt problematisch te zijn, of indien specifieke configuratie (zoals antivirus exclusions en socket communication) wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB. UZB staat enkel open java versies toe zoals adoptium, amazon corretto of Microsoft java. We staan vooral geen Oracle Java

		versie toe na versie 8 u202 & versie 11.02 omdat deze betalend zijn.
TC04	Clients worden standaard in het UZB-**AD**-domein gejoind en via GPO's beheerd.	Als dit in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB. Clients die niet in het domein mogen, worden achter een netwerkfirewall gezet.
TC05	Windows firewall is actief op elke PC, enkel voor inkomend verkeer naar de PC.	Beschrijf hier poort en protocol indien een poort moet geopend worden.
TC06	Clients kunnen in een apart **VLAN** ondergebracht worden. Voor randapparatuur is dit altijd het geval.	Beschrijf hier in dit kader de vereiste firewall rules. Voeg een Windows update policy toe of argumenteer waarom dit niet kan.
TC07	**UZB geeft de voorkeur aan web based applicaties. Extra software** die op de client nodig is in het kader van de oplossing wordt centraal en geautomatiseerd aangeboden aan de client door UZB. Installatiepaden, bestandsstructuur en schijfindeling zijn in overleg met UZB te bepalen. **Software moet zonder local-adminrechten kunnen werken (non negotiable!) en moet met UAC overweg kunnen.** Op basis van de gemaakte afspraken biedt de leverancier UZB een MSI aan, vergezeld van de installatiehandleiding van de software als onderdeel van de as-built documentatie.	Als dit in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB. Bezorg de installatiehandleiding als onderdeel van de as-built documentatie.
TC08	In UZB is **internettoegang** aan een user account gekoppeld. Serviceaccounts hebben standaard geen internettoegang.	Als de toepassing of randapparatuur autonoom internettoegang nodig heeft, moet dit expliciet worden vermeld in de architectuurdocumentatie met inbegrip van de vereiste firewall rules.
TC09	UZB heeft een eigen **Certificate Authority** (CA) die door elk toestel in het domein automatisch is vertrouwd. Dit geldt ook voor mobile devices. Er moet gebruik gemaakt worden van certificaten van de UZB CA. Dit is met name relevant voor bv. websites en niet voor devices waarmee secure wordt gecommuniceerd. In het laatste geval, zoals bv. bij printers, kunnen self-signed certificaten gebruikt worden.	Als dit in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.

		Vermeld hier indien een publiek certificaat nodig is zo dat UZB dit met een externe CA (Sectigo) kan regelen.
TC10	UZB gebruikt Exchange online als **e-mail**oplossing. Standaard is ongeauthenticeerd e-mailen onmogelijk. Uitgaande mail naar Internet wordt beperkt tot mailadressen met suffix uzbrussel.be. Andere domeinnamen worden gefilterd door de mail gateway. Indien de applicatie moet kunnen mailen zijn er 2 mogelijkheden: a. Authenticated: via AD credentials met opgave van mailadressen (voorkeur) b. Non-authenticated: IP-adres wordt toegevoegd in een ACL op de loadbalancer en geen controle op mailadres. Voor cloudapplicaties via microsft graph api.	Documenteer hier de mogelijke noodzaak voor e-mailen, inclusief de vereiste technische informatie. Beschrijf hier of de oplossing MS Exchange Online (o365) compatible is. Indien non-authenticated: beschrijf hier de IP's die te whitelisten zijn.
TC11	**Toegangscontrole (access control)** UZB verkiest dat on premise authenticatie via AD gebeurt.	Beschrijf hier of in een bijlage hoe de toegang tot de applicatie op de client ingeregelde wordt. Voorziet de oplossing in Role Based Access Control (RBAC)? Wat is de procedure voor het offboarden van gebruikers?

Server

TS01	UZB verwacht een **architectuurdesign** te ontvangen: een duidelijk schema waarop *alle* componenten van de oplossing, informatiestromen, IP-adressen, protocols, poorten en dependencies zichtbaar zijn. Vermeld ook componenten die de oplossing gebruikt, zoals java, .net, webservers zoals nginx, apache, enz.	Documenteer dit in een bijlage aan dit document. Het design houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TS02	UZB gebruikt voor servers standaard geen bare metal hardware maar biedt **virtuele servers** aan via VMWare vSphere en met onderliggende AMD Epyc CPU. Alle bijhorende licenties ondersteunen HA, DRS & vMotion. Gezien het belang voor de regelmatige failovertesten in het ziekenhuis kan vMotion niet in vraag gesteld worden. Servers worden door UZB geïnstalleerd. Eigen installaties worden enkel voor hardenened oplossingen toegestaan en zijn onder de vorm van een OVA/OVF aan te leveren die aan de voorwaarden hieronder voldoet. UZB zet	Als dit in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB. Geef expliciet aan of VMWare Fault Tolerance nodig is. Geef expliciet aan of er nVidia GPU-kaarten nodig zijn, met hoeveel GB RAM, het aantal

	OVA-oplossingen bijna altijd achter een netwerkfirewall vanwege de updateproblematiek. OS-installaties via OVA/OVF dienen een admin account voor UZ Brussel personeel te voorzien. *Black box* OVAs waar niet op aan te melden valt op het systeem worden *niet* geaccepteerd. UZB gebruikt standaard geen nVidia GPU-kaarten. Indien UZB akkoord gaat met de installatie van server hardware, gebeurt deze door UZB, niet in het active directory domein, in een apart netwerk (VLAN) en achter een firewall.	gewenste CUDA cores alsook het type licentie voor nVidia Grid en het gewenste profiel.
TS03	UZB installeert en configureert zijn servers standaard op de meest recente versie van **Windows server, AlmaLinuxof RHEL**. Gezien het belang voor de informatieveiligheid staat UZB enkel een OS toe dat nog minstens 3 tot 5 wordt ondersteund na aankoop.	Documenteer hier het gewenste OS. Documenteer hier indien de standaard voorgestelde opties niet mogelijk of wenselijk zijn en beschrijf de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB
TS04	Elke server wordt binnen de geleverde applicatie of randapparatuur steeds aangesproken via zijn Fully Qualified Domain Name (**FQDN**) met uzbrussel.be. Er wordt gebruik gemaakt van split DNS voor FQDNs die op internet beschikbaar moeten zijn	Vermeld hier of er split DNS nodig is.
TS05	Windows servers zijn lid van het UZ Brussel **AD**-domein uzbrussel.be en worden via GPO's op basis van Microsoft secure baselines beheerd. Deze settings gelden voor alle toestellen: i. Disable SMBv1 (Windows filesharing). SMBv2 wordt gedoogd maar is niet wenselijk. ii. Disable LM (LanManager) & NTLMv1. NTLM wordt afgebouwd ten voordele van windows integrated authentication via kerberos. iii. UAC actief iv. Windows Firewall. TCP/UDP-poorten die moeten worden opgezet moet nauwkeurig worden omschreven. Het wordt toegestaan om eventueel een applicatie te definiëren in de Windows firewall. Alleen inkomend verkeer wordt gefilterd.	Als dit in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB. Vermeld hier eventuele Windows firewall settings.

	v. User Rights Assignment (Windows privileges) worden alleen beheerd via GPO en kunnen niet via een lokale GPO worden aangestuurd (bvb act as part of the OS, logon locally rights etc) vi. SSL2.0, 3.0, TLS1.0 & 1.1 worden standaard disabled. vii. Verbinden met AD gebeurt enkel via LDAPS – niet LDAP. viii. Credential guard is standard actief. ix. Print spooler staat uit. x. Er worden geen lokale users aangemaakt en accounts mogen niet aan de local admin group toegevoegd worden zonder expliciete goedkeuring van UZB. In geval van positief advies gebeurt dit via een AD group en niet rechtstreeks in local groups. Servers die niet aan deze voorwaarden voldoen, worden uit het domein verwijderd en achter een netwerkfirewall gezet.	
TS06	Servers worden standaard geïnstalleerd met **antivirussoftware** die door UZB geconfigureerd, beheerd en geüpdatet wordt. Periodiek wordt een full scan van de server gedaan die de performantie kan beïnvloeden. Dit heeft vooral belang voor eventuele socket-based communicatie. Indien deze communicatievorm gebruikt wordt, is dit expliciet in de designdocumenten te vermelden.	Vermeld hier eventuele scanning exceptions. Vermeld hier het eventuele gebruik van socket-based communicatie en de eventuele noodzaak voor een exclusionlijst.
TS07	UZB **updatet** autonoom, regelmatig en automatisch de servers onder zijn beheer. Het doet dit gefaseerd met het oog op de beveiliging van de netwerkomgeving. Security updates moeten toegelaten worden.	Als dit in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TS08	UZB installeert standaard 7zip, notepad++ en MS Edge. Eventuele **extra software** die op de server te installeren is, wordt door de opdrachtnemer in MSI-formaat voorbereid en vergezeld van een installatiehandleiding opgeleverd. De installatie van de software op de server dient te worden overeengekomen tussen UZB en de leverancier. De opdrachtnemer kan de software autonoom installeren, maar de	Beschrijf hier of/welke software te installeren is. Bezorg msi en installatiehandleiding aan de technische contactpersoon bij UZB.

	software moet steeds door een medewerker van UZB gecheckt worden voor ingebruikname in productie. Eventuele nieuwe versies/updates volgen hetzelfde pad. Services en taken draaien altijd met een overeengekomen serviceaccount **<u>zonder</u>** adminrechten.	
TS09	UZB maakt een zeer expliciet onderscheid tussen **installatie-/supportaccounts en service-accounts:** i. Het account dat voorzien wordt voor de installatie en support van de applicatie(s) wordt na de installatie disabled. Dit account mag dus niet worden gebruikt om bv. een service te draaien, een databaseconnectie te maken of om bv. een fileshare te mounten. ii. Local system accounts worden expliciet niet toegestaan. Er kan door UZB een serviceaccount aangemaakt worden indien een service domain credentials nodig heeft in plaats van het default system account. Dit wordt dan een Group Managed Service Account ***<u>zonder admin rechten</u>*** waarvan het password wordt beheerd door AD. iii. Het wachtwoord van een serviceaccount mag ***<u>niet</u>*** in clear text zichtbaar voorkomen in configuratie-bestanden. Applicaties draaien in productie als services zonder local adminrechten – (local service of network serviceaccount zijn toegestaan). Er hoeft dus niet persé een uzb ad account worden gebruikt en indien er een AD serviceaccount wordt gebruikt dan bij voorkeur MSA account en geen standaard AD account zodat password rotatie automatisch gebeurt. Opdrachtnemers krijgen het bijhorende paswoord niet ter beschikking. GUI-based executables (processen die niet als service kunnen worden gestart) worden niet geaccepteerd.	Beschrijf hier of en met welk doel/welke rechten (registry, configuratie bestanden, enz.) een serviceaccount nodig is. Spreek af met de technische contactpersoon bij UZB voor het delen van het wachtwoord van het serviceaccount. Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TS10	**Authenticatie** gebeurt met Windows integrated authentication via Kerberos en eventueel via NTLMv2 (geen NTLMv1 of LanManager)	Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief

	AD LDAP-authenticatie enkel via LDAPS en niet via plaintext LDAP.	uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TS11	Geen enkele server op het domein mag zonder voorafgaand overleg met UZB **remote overgenomen** worden: i. Tijdens de projectfase wordt voor de oplossing een domeinaccount voorzien waarmee de installaties zullen gebeuren. Na de projectfase wordt dit account gedisabled. ii. Om de stabiliteit van de oplossing te garanderen kan de leverancier na de projectfase toegang krijgen tot de omgeving volgens het proces dat UZB hiervoor standaard voorziet en via een VPN Pulse Secure Client (via TOTP) in combinatie met een PAM oplossing. Hiervoor moet de overnemer een plugin installeren op haar/zijn PC.	Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TS12	UZB **monitort** de volledige serveromgeving.	Vermeld hier of in een bijlage welke services & URL's van de dienst te monitoren zijn, welke thresholds gelden en de onderlinge relatie tussen de verschillende services en de user experience.
TS13	UZB ondertekent alle nodige certificaten intern met de UZ Brussel **Certificate Authority (CA)** die door elk toestel in het domain automatisch vertrouwd wordt, inclusief de centraal beheerde mobile devices. De leverancier gebruikt certificaten van de UZB CA. Als er een publiek certificaat nodig is, koopt UZB dit bij een externe CA.	Vermeld hier of er een publiek certificaat nodig is. Inclusief een subject & SAN-namen en waarvoor het certificaat wordt gebruikt: server authentication en/of client authentication en/of andere.
TS14	**Internettoegang** vanop servers of communicatie met specifieke publieke adressen op het internet is niet toegestaan.	Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB. Het voorstel omvat een detailconfiguratie van Windows firewall en netwerk firewall. Voor applicaties die van buitenaf beschikbaar moeten zijn, omvat dit ook de details zoals URL's, IP-adressen, poorten, protocollen, enz.

		om dit op een gecontroleerde manier mogelijk te maken.
TS15	**Niet-geëncrypteerde, bekend onveilige of verouderde protocollen** zoals ldap, http, ftp en telnet zijn niet toegestaan.	Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TS16	UZB **backupt** de systemen in zijn beheer als volgt: i. Van virtuele servers worden elke dag 3 snapshots op storageniveau gemaakt waarbij een crash consistent backup wordt genomen. ii. Databases die door UZB ondersteund worden (zie hierover verder "Databaseserver"): Voor MSSQL worden er elk half uur transaction backups voorzien.	Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB. Indien de leverancier andere DB-systemen gebruikt, verwijzen we naar de betreffende informatie onder "Databaseserver". In dergelijke gevallen zal ICT enkel zorgen voor een file-based back-up van een database-export die de leverancier voorziet.
TS17	**Applicatiedata** wordt altijd buiten de VM op een NAS-locatie opgeslagen zodat de VM niet te groot wordt en de storage efficiënt kan worden aangepast. UZ Brussel beschikt hiervoor over een high available storage platform en een langetermijnopslag op archief. Snapshots kunnen tot 3 jaar bijgehouden worden met kopie op een tier2 disk array en een offsite kopie op tier3 omgeving. Alle file serving/NAS-behoeften dienen op deze reeds aanwezige systemen voorzien te worden. Indien er weinig applicatiedata is (< 50GB), kan die lokaal opgeslagen worden.	Vermeld hier expliciet als er een aparte backup retention policy nodig is voor applicatiedata.
TS18	**Creatie en configuratie van Local SMB/CIFS shares** op Windowsservers zijn by default niet toegestaan zonder tussenkomst van UZB-personeel	Vermeld hier expliciet als en welke local shares nodig zijn. UZB maakt deze aan, rekening houdend met de aanmaak en toepassing van AD-groepen en NTFS-rechten. Vermeld welke personen toegang nodig hebben tot de service (of serviceaccount(s).
TS19	Voor het gebruik van e-mail gelden voor servers dezelfde regels als voor clients: UZB gebruikt Exchange online als **e-mail**oplossing.	Documenteer hier de mogelijke noodzaak voor e-mailen, inclusief de vereiste technische informatie.

	Standaard is ongeauthenticeerd e-mailen onmogelijk. Uitgaande mail naar internet wordt beperkt tot mailadressen met suffix uzbrussel.be. Andere domeinnamen worden gefilterd door de mail gateway. Indien de applicatie moet kunnen mailen zijn er 2 mogelijkheden: a. Authenticated: via AD credentials met opgave van mailadressen (voorkeur) b. Non-authenticated: IP-adres wordt toegevoegd in een ACL op de load balancer en geen controle op mailadres Voor cloudapplicaties via microsft graph api.	Beschrijf hier of de oplossing MS Exchange Online (o365) compatible is. Indien non-authenticated: beschrijf hier de IP's die te whitelisten zijn.

Gedeelde serverinfrastructuur

UZB consolideert een aantal kernfuncties op centrale systemen en moedigt leveranciers sterk aan deze te gebruiken:

TG01	**Communicatieserver** (**HL7**-berichten) Communicatie van de oplossing met de centrale UZB-systemen verloopt bij voorkeur over HL7 via Mirth. De leverancier voorziet de socket based communicatie met Mirth. Alternatief worden op het centrale storage platform of op (een van) de servercomponent(en) van de toepassing een of twee shares gedefinieerd voor in- en uitgaande file based communicatie.	Geef aan of de leverancier socket based Mirth communicatie of (een) share/s wil gebruiken. Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TG02	**Databaseserver** Microsoft SQL Server wordt door UZB aangeboden en ondersteund. De leverancier krijgt een of meerdere databases op de centrale SQL-database server ter beschikking. UZB gebruikt hiervoor een centrale SQL 2022 enterprise edition. i. UZB neemt de verantwoordelijkheid voor licenties, installatie van de database (SQL-script te voorzien door de leverancier), voor de availability en voor de back-up en restore van de omgeving. Eventuele report services en andere database activiteiten (SSIS, SSAS, SSRS, ETL…) worden vanop een andere server uitgevoerd. Voor installatie en eventuele troubleshootingactiviteiten krijgt de opdrachtnemer de juiste contacten.	Geef aan of/welke van de centrale databaseoplossingen de leverancier wenst te gebruiken. Geef de initiële en verwachte databasegrootte aan. Indien er andere databases nodig zijn zal de leverancier deze zelf installeren en onderhouden. De leverancier zal de databasesoftware regelmatig en op eigen verantwoordelijkheid updaten/patchen zodat veiligheid en stabiliteit gegarandeerd blijven. De licentie voor deze database wordt voorzien door de leverancier. De leverancier houdt hierbij rekening dat deze database server op een vmware virtueel platform

	Er worden geen sysadminrechten toegekend aan de leverancier op de centrale MS SQL server. ii. De opdrachtnemer reageert tijdig en efficiënt wanneer DBA-analyses aantonen dat een bepaalde query de performantie van het systeem bedreigt. In overleg kan MariaDB centraal aangeboden worden. Ook Postgresql, maar deze laatste niet centraal. Oracledatabases of producten zijn geen optie.	draait wat implicaties op de licentiëring kan hebben. Backup (scripts) moet worden voorzien door de leverancier en backups moeten worden opgeslagen op een locatie buiten de server op een NAS. Deze NAS-locatie wordt aangeleverd door UZ Brussel. Communicatie tussen applicatie en database servers moet worden geëncrypteerd met TLS1.2 of hoger. Indien de opdrachtnemer sql reporting services nodig heeft, moet de collation aangeven worden voor MS SQL (indien anders dan Latin1_general). Indien Oracledatabases of producten noodzakelijk zijn voor de oplossing, moet de leverancier UZB met een certificaat van Oracle garanderen dat deze kunnen draaien op vmware (embedded Oracle license). Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TG03	**Load balancer** Om een oplossing full tolerant en high available te maken biedt UZB zijn NGINX-software load balancer, HA Proxy of Reverse Proxy aan voor die applicaties die hiermee om kunnen	Vermeld hier expliciet indien en welke van deze oplossing u hiervoor wenst in te zetten.
TG04	**Fileserver** Zie hierover hoger onder “Applicatiedata”	-
TG05	**Webserver**	i. Vermeld hier of de oplossing een webserver gebruikt. ii. Vermeld de subject en SAN-namen waarvoor het certificaat wordt gebruikt. Zie ook TS13 over certificaten.

As-a-service-oplossing

TA01	UZB verwacht een **architectuurdesign** te ontvangen: een duidelijk schema waarop *alle* componenten van de oplossing, informatiestromen, IP-adressen, poorten en dependencies zichtbaar zijn.	Documenteer dit in een bijlage aan dit document. Het design houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.

TA02	**Informatiebeveiliging en privacy**. UZB verwacht dat de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van de gegevens van het ziekenhuis, zijn patiënten en medewerkers te allen tijde gegarandeerd zijn.	Beschrijf hier of in een bijlage: i. Beschrijf de encryptie van gegevens in transit en at rest ii. Waar worden de gegevens bewaard – inclusief de backup. iii. Met welke frequentie gebeurt de backup, hoe lang worden backups bijgehouden, wat zijn de typische restore/RPO/RTO windows? iv. Wie heeft toegang tot de data van UZB en met welke rollen en rechten? v. Is permanente verwijdering van gegevens mogelijk? vi. Wie is de eigenaar van de gegevens die in het kader van het contract verzameld en verwerkt worden? vii. Hoe wordt de integriteit van gegevens verzekerd tijdens de overdracht ("in transit") en bij opslag ("at rest")? viii. Worden gevoelige persoonsgegevens geanonimiseerd of gepseudonimiseerd om te voldoen met wet- en regelgevingen? ix. Hoe verzekert de leverancier dat geanonimiseerde gegevens niet opnieuw geïdentificeerd kunnen worden?
TA03	**Toegangscontrole (access control).** Authenticatie in de applicatie gebeurt bij voorkeur via EntraID en niet met lokale users in de applicatie	Beschrijf hier of in een bijlage: i. Voorziet de oplossing in Role Based Access Control (RBAC)? ii. Wordt Multi Factor Authenticatie (MFA) ondersteund, en zo ja: hoe? iii. Wordt Single Sign On (SSO) met EntraID (of andere IdP's) ondersteund, en zo ja: hoe? iv. Zijn SSO features compliant met securitystandaarden zoals SAML 2.0 of OpenID Connect? v. De procedure voor het offboarden van gebruikers.
TA04	**Beschikbaarheid en Continuïteit** UZB wenst te allen tijde een optimale beschikbaarheid van de oplossing.	Beschrijf hier of in een bijlage: i. Welke uptime biedt de leverancier over de totale oplossing? ii. Beschikt de leverancier over een gedocumenteerd disaster recovery plan voor het herstellen van de dienstverlening en de gegevens. Zo ja, gelieve dit in bijlage te bezorgen. iii. Met welke regelmaat wordt het disaster recovery plan getest?

		iii. Hoe is de oplossing beveiligd tegen distributed denial-of-service (DDoS) aanvallen?
TA05	**Infrastructuurbeveiliging** UZB wenst verzekerd te zijn dat de infrastructuur van waarop de oplossing wordt aangeboden, beveiligd is	Beschrijf hier i. Welke maatregelen heeft de leverancier getroffen om de onderliggende infrastructuur te beveiligen. Maak dit ook inzichtelijk in het architectuur design (zie hoger) ii. Waar (in welk(e) datacenter(s) de oplossing gehost wordt. iii. Hoe de oplossing die aan UZB aangeboden wordt gesegmenteerd wordt in de verschillende lagen van het OSI-model iv. Of en welke tools zoals Key Management Services of threat detection de leverancier gebruikt.
TA06	**Third party integraties**	Beschrijf hier en/of in een bijlage i. hoe de oplossing technisch integreert met oplossingen van derde partijen ii. hoe API keys en andere credentials opgeslagen worden iii. hoe de leverancier oplossingen van derde partijen beoordeelt
TA07	**Data recovery post contract.** UZB wenst duidelijkheid over het recupereren van haar data na het beëindigen van het contract	Beschrijf hier hoe dit typisch verloopt en welke mogelijkheden bestaat. Vermeld ook datatransmissiesnelheden.
TA08	**Netwerkbeveiliging**	Beschrijf hier of in een bijlage: i. Welke netwerkbeveiligingsmaatregelen zijn in voege om de communicatie tussen cloud resources mogelijk te maken? ii. Biedt de leverancier Virtual Private Cloud (VPC) of virtuele netwerken aan om beveiligde isolatie mogelijk te maken? iii. Biedt de leverancier een Web Application Firewall (WAF) aan voor web facing services? iv. Hoe wordt het netwerkverkeer gemonitord op potentiële bedreigingen zoals bv. DDoS-aanvallen?
TA09	**Gegevenssoevereiniteit en lokalisatie**	Beschrijf hier of in een bijlage i. Zijn er specifieke vereisten voor gegevensresidentie of -soevereiniteit waaraan de leverancier voldoet? ii. Is het mogelijk datacenters op specifieke locaties te kiezen om op die manier te voldoen aan wet- en regelgeving?

Oplossings-onafhankelijke verwachtingen

De maatregelen hieronder zijn verwachtingen van UZB over de leverancier en de oplossing die hij aanbiedt, ongeacht de voorgestelde oplossingen.

TO01	**Transparantie**. UZB verwacht een transparante houding van de leverancier op vlak van beveiliging. Dit omvat ook de melding door die leverancier van beveiligingslekken en kwetsbaarheden in de hardware, software, configuratie of dienstverlening van de oplossing, zo snel mogelijk na de vaststelling ervan.
TO02	**Auditing.** UZB verwacht dat de leverancier zich openstelt voor audits door UZB of door een derde partij die door UZB hiervoor wordt aangesteld, steeds binnen de grenzen van afspraken over scope, kosten en timing. De leverancier ondersteunt UZB hierin, bijvoorbeeld door toegang te geven tot relevante documentatie, logs, personeel of infrastructuur. De leverancier is ook beschikbaar voor ad hoc vragen van UZB over specifieke aspecten van de oplossing tijdens de duur van de samenwerking.
TO03	**Ethical hacking**. Oplossingen die onder het UZB-domein publiek beschikbaar zijn, worden getest door ethische hackers in opdracht van UZB. Kwetsbaarheden in de oplossing van de leverancier worden aan deze meegedeeld. UZB verwacht dat deze kwetsbaarheden onverwijld opgelost worden en verwacht ook transparante communicatie hierover. Als er een kwetsbaarheid teruggevonden kan worden binnen de software die onder beheer van de opdrachtnemer geplaatst werd, kan de bijhorende bounty doorgerekend worden aan de opdrachtnemer.
TO04	**Geschiktheid aangeleverde software en runtime environments.** Alle door de leverancier aangeleverde software en runtime environments (java, .net, python ...) dienen vrij te zijn van gekende security issues zoals o.a. in CVE-entries worden omschreven. Enkel ondersteunde versies van applicaties en runtime environments worden aanvaard. Van elk softwarecomponent verwachten we een beschrijving van de versie en nog lopende garantie/support. Het is aan de leverancier om alle softwarecomponenten up to date te houden. UZ Brussel beschikt over een vulnerability scanner tool die dit zal controleren.
TO05	**Geschiktheid personeel.** UZB verwacht dat alle werkzaamheden aan de oplossing door de leverancier of door een partij die door de leverancier werd aangesteld worden uitgevoerd door personeel dat hiervoor geschikt is. Met geschiktheid wordt bedoeld (a) dat deze personen technisch onderlegd zijn in de oplossing en alle componenten die er een onderdeel van vormen; (b) dat deze personen alle relevante wet- en regelgeving en UZB-specifieke instructies respecteren; (c) dat deze personen zich professioneel en ethisch gedragen. UZB behoudt zich het recht voor hierop toe te zien en personen die een of meerdere van deze vereisten niet respecteren de toegang tot zijn systemen of gebouwen te ontzeggen.

TO06	UZB verwacht dat **updates** aan de oplossing i. zoveel mogelijk zonder downtime kunnen uitgevoerd worden. ii. steeds terugrolbaar zijn	Beschrijf hier het updatemechanisme van de oplossing, inclusief of en hoeveel tijd te voorzien is aan onbeschikbaarheid tijdens een update. Voor DB-integraties verwacht UZB een script om ook DB-updates terug te draaien. Dit is een onderdeel van het as-builtdossier (zie elders)
TO07	**Beveiliging ongeautoriseerde wijzigingen.** UZB verwacht dat de oplossing beveiligd is tegen ongewenste en/of ongeautoriseerde	Beschrijf hier hoe de oplossing beschermd is tegen ongeautoriseerde wijzigingen.

	wijzigingen van de hardware, software, of configuratie van de oplossing	
TO08	**Security logging**. UZB verwacht de logging van mutaties van data in de oplossing zodat op elk gegeven ogenblik kan achterhaald worden wie wanneer welke wijziging uitvoerde.	Beschrijf hier de security logging van de oplossing: Wat wordt waar en hoe lang gelogd. Beschrijf hoe UZB hier toegang toe heeft zonder interactie met de opdrachtnemer
TO09	**Fouten en foutdetectie.** UZB verwacht dat de oplossing een systeem bevat voor de detectie en correctie van fouten in de invoer, de verwerking, de uitvoer en de verspreiding van gegevens. Dit systeem omvat middelen voor de verificatie van de volledigheid, juistheid en authenticiteit van de interne en externe verspreiding van de gegevens. Het systeem voldoet ook aan de geldende richtlijnen op moment van gebruik vanuit overheid voor onder andere het beveiligen van de informatiegegevens.	Beschrijf hier de middelen voor de detectie en correctie van fouten in de invoer, de verwerking, de uitvoer en de verspreiding van gegevens.
TO10	**Monitoring** UZB wenst een regelmatig overzicht op de gezondheid en veiligheid van de oplossing.	Beschrijf hier i. wie (UZB/leverancier) welke delen van de oplossing monitort. ii. welke parameters van de oplossing typisch en met welke frequentie gemonitord worden. iii. welke logs out-of-the-box beschikbaar zijn voor monitoring iv. of logs kunnen geïntegreerd worden in de Security Information and Event Management (SIEM) tool van UZB. v. of logs al dan niet geanonimiseerd worden om persoonsgegevens te beschermen.
TO11	**Authenticatie - algemeen** Authenticatie gebeurt via AD of entraID i. Wachtwoorden worden niet bij of in de oplossing bewaard. Alle wachtwoorden worden veilig met UZB gedeeld om in een password vault te bewaren. ii. Generieke accounts worden niet toegestaan; elke gebruiker heeft een unieke login/passwordcombinatie. iii. Wanneer applicatie logons aangemaakt worden, is salting en hashing verplicht.	UZB verwacht de lijst van accounts en paswoorden als onderdeel van het as-builtdossier (zie elders) Paswoorden die in files aan UZB aangeleverd worden, moeten encrypted zijn en vergezeld zijn van een instructie hoe een update mogelijk is.
TO12	**Authenticatie – Single Sign On (SSO)**	Beschrijf de mogelijkheden van de oplossingen voor SSO en de integratie met Imprivata in het bijzonder.

	UZB eist authenticatie bij elke opstart van een multi-user oplossing en geeft voorkeur aan oplossingen die met Imprivata integreren.	
TO13	**Authenticatie – Multi Factor Authentication (MFA)** UZB eist MFA voor oplossingen die via het internet ter beschikbaar gesteld worden aan de gebruikers ervan.	Als de UZB-aanpak in het kader van de voorgestelde oplossing niet mogelijk of wenselijk is, beschrijf dan hier de exacte beweegredenen met een exhaustief uitgewerkt alternatief voorstel. Dit voorstel houdt geen stilzwijgende acceptatie in maar is het voorwerp van overleg voorafgaand aan een eventuele instemming door UZB.
TO14	**Autorisatie** i. UZB verwacht een duidelijk overzicht van de autorisatiemogelijkheden in multi-user oplossingen. ii. Gebruikersbeheer wordt maximaal via Active Directory geautomatiseerd via Kerberos (voorkeur) of NTLMv2 – dus zonder manuele tussenkomst voor creatie, wijzigingen en stopzetten van gebruikers. iii. toegangsbeheer en rolverdeling zijn minstens gekoppeld aan de UZB AD via Entra ID. iv. De naamgeving wordt vooraf met UZB afgesproken. v. UZB verwacht dat de autorisatie via een beveiligde verbindingen met Active Directory gebeurt.	Beschrijf hier in geval van multi-user oplossingen de types gebruikers en (de inhoud/reikwijdte van) hun rechten (read/add/change). Beschrijf hier de alternatieve aanpak voor (delen van) multi-user oplossingen die niet kunnen geautomatiseerd worden via Active Directory.
TO15	**Incident response plan** **UZB** verwacht dat de leverancier over een up to date incident response plan beschikt dat getraind is aan zijn medewerkers en aan de gebruikers van de oplossing.	Beschrijf hier en/of in bijlage het incident response plan. Beschrijf hier hoe klanten geïnformeerd worden over een security incident. Vermeld hier de significante security incidenten waarmee de leverancier de voorbije 12 maand geconfronteerd werd. Dit zijn incidenten met een reële of potentieel grote impact.
TO16	**Applicatiebeveiliging** UZB verwacht dat de oplossing ontwikkeld werd op basis van secure development best practices. UZB behoudt zich het recht zelf de oplossing te laten pentesten door ethical hackers. Indien ernstige gebreken vastgesteld worden, kunnen de kosten op de leverancier verhaald worden.	Indien de leverancier de applicatie zelf ontwikkeld heeft, beschrijf hier dan i. Of en welke secure development best practices de leverancier volgt ii. Of en hoe de leverancier regelmatig code reviews uitvoert iii. Of en hoe vaak penetratietesten uitgevoerd worden op de oplossing. – Zo ja, gelieve ons het rapport te bezorgen over de meest recente test iv. Of de leverancier gebruik maakt van een bug bounty program.

		v. met welke regelmaat de leverancier security patches en updates uitbrengt vi. Hoe snel de leverancier kwetsbaarheden aanpakt.
TO17	**Handleidingen**	Bezorg in bijlage handleidingen voor beheerders en gebruikers.
TO18	UZB verwacht dat de leverancier de contactpersoon bij UZB informeert van zodra de configuratie of installatie is afgerond – ook al is dit tijdelijk, bv. wanneer gewacht wordt op deelleveringen – en in elk geval vóór de ingebruikname van de configuratie of installatie in de productieomgeving van UZB. UZB verwacht binnen de 4 weken na het afsluiten van de installatie en configuratie volgende informatie te ontvangen: **i. as-built-dossier**. Dit is een getrouwe weergave van installatie en configuratie zoals die door de leverancier werd achtergelaten. ii. **controleprocedure na patch/reboot**. Dit kort document geeft de controlepunten aan die UZB kan gebruiken om de beschikbaarheid van de oplossing te verifiëren na het patchen of herstarten van het systeem. De oplevering van deze documenten kan een voorwaarde zijn voor de eventuele betaling van een laatste schijf.	De documenten worden via e-mail aan de projectleider en de technische contactpersoon bij UZB bezorgd.

Leveranciersverwachtingen

In dit luik wordt ingegaan op alle niet-technische verwachtingen die UZB heeft over de oplossing en zijn leverancier.

Licentiemodel

LL01	ALGEMEEN. Beschrijf het **licentiemodel** van de oplossing(en) exhaustief.	Voorzie hier of in bijlage een lijst van alle componenten van de oplossing en hoe en door wie die gelicentieerd moeten worden. Geef hierbij ook licenties van eventuele OS, DB & andere ondersteunende producten duidelijk aan of voor alle nodige modules binnen het pakket. Houd hierbij rekening met actief/passief-omgevingen, overdracht van licenties, enz. Gezien UZB op haar eigen contracten een beroep kan doen om licenties te voorzien,

		vormen zij geen afdwingbaar onderdeel van de oplossing. Voorzie een bewijsstuk indien licentie(s) als pakket onder OEM door de leverancier voorzien worden. Geef aan of academic licensing mogelijk is. Beschrijf hierbij ook transparant voor alle mogelijke scenario's het kostenplaatje van alle licenties.
LL02	**Geldigheidsduur** van de licentie(s). UZB verwacht dat de geldigheidsduur van de licentie(s) in overeenstemming is met de verwachte levensduur van de oplossing.	Beschrijf hoelang de licentie(s) geldig blijven; hoe/wanneer en door wie ze geactiveerd worden; grace period; …
LL03	Wordt de licentie afgedwongen door **hardwarematige oplossingen** zoals keys & dongles?	Indien ja: beschrijf.
LL04	Zijn **specifieke eigenschappen** zoals MAC-adres of VM Hardware ID nodig?	Indien ja: verklaar *voor* de implementatie
LL05	UZ Brussel wenst **enkel de productie-omgeving** onder licentie te nemen. Zijn systemen die niet tot deze omgeving behoren te licentiëren?	Indien ja: beschrijf.

Zakelijke overwegingen

Belangrijk: Deze vragen moeten *niet* beantwoord worden in het kader van een aanbesteding waar ze al in dit proces opgenomen zijn.

LZ01	UZB wenst duidelijkheid over de **contracterende partij**.	i. Vermeld hier welke de contracterende partij is (naam/zetel). ii. Vermeld hier of en welke subcontracterende partij(en) de leverancier wenst in te zetten (naam/zetel).
LZ01	UZB wenst met **financieel gezonde organisaties** samen te werken.	Voorzie in bijlage een recent financieel overzicht van de organisatie die als contractant zal optreden.
LZ02	**Referentieklanten**	Voorzie de contactgegevens van 3 referentieklanten die onafhankelijk van de leverancier door UZB kunnen gecontacteerd worden in het kader van een mogelijke samenwerking.
LZ03	UZB wenst **contractuele duidelijkheid**	Documenteer hier een lijst en bezorg in bijlage een volledige set van *alle* typedocumenten (zoals contracten, SLA, gegevensverwerkingsovereenkomst) die in

		een contractfase zouden kunnen onderhandeld en ondertekend worden. Belangrijk: dit omvat ook documenten die stilzwijgend goedgekeurd worden door het ondertekenen van een contract.
LZ04	**Compliance en certificaten**	Voorzie hier een lijst van alle voor-deze-samenwerking-relevante nationale en internationale wetgeving, regelgeving en standaarden waarmee leverancier compliant is, inclusief de scope voor de compliance. Vermeld expliciet de geldende richtlijnen waarmee de leverancier van de oplossing *niet* compliant is. Voeg ook technisch relevante standaarden toe zoals over AWS, Azure en Google Coud. UZB behoudt het recht om ook de certificaten zelf en de bijhorende auditrapporten te bevragen.
LZ05	**Financieel overzicht**	Voorzie hier of in bijlage een lijst van alle diensten of interventies waarvoor leverancier een kost voorziet voor UZB.
LZ06	UZ Brussel **Privacybeleid**	Bevestig dat u kennis hebt genomen van het UZ Brussel privacyreglement en als leverancier ook deze voorschriften zal naleven. (Terug te vinden op UZ Brussel-website)
LZ07	**GDPR** - verwerkingscontract	In geval binnen uw oplossing persoonlijke gegevens worden verwerkt, en er is nog geen verwerkingscontract opgesteld, motiveer waarom u dit niet nodig acht.

Contactinformatie leverancier

Contracterende organisatie	Naam, adres zetel
Commerciële contactpersoon	Naam, telefoon, e-mail, datum
Technische contactpersoon	Naam, telefoon, e-mail, datum

Door het bezorgen van dit ingevuld formulier aan uw contactpersoon bij UZB verklaart u kennis genomen te hebben van de verwachtingen van UZB, deze begrepen te hebben, en ze naar verwachting en best vermogen geduid te hebben.

Onvolledig en/of niet tijdig ingevulde formulieren kunnen resulteren in een vertraagde analyse van de informatie en implementatie van de oplossing tot en met uitsluiting uit het selectieproces.