Universitair Ziekenhuis Brussel

UZ Brussel Installatie Voorwaarden

Doelstelling

Dit document omvat de installatie voorwaarden opgesteld door de IT-dienst van UZ Brussel (UZB).
De bedoeling is om een vlotte doorstart van het project na de aankoopprocedure te kunnen uitvoeren en te plannen (resources etc …). Voor bijkomende vragen of info kan je contact opnemen met de systeem ploeg (security@uzbrussel.be).

1. Licenties

- ☐ Eenvoudig over te zetten op een vervangend systeem.
  (niet afgedwongen door hardware matige oplossingen zoals keys & dongles)
- ☐ Indien specifieke eigenschappen zoals MAC-adres of VM Hardware ID nodig zijn,
  op voorhand aangeven.
- ☐ Enkel aangevraagd voor productie.
  (en dus geen extra licenties vereist voor test/opleiding of acceptatie omgeving)
- ☐ Licenties van eventuele OS, DB & andere ondersteunende producten duidelijk aangeven,
  geen afdwingbaar onderdeel van de oplossing.
  (UZB kan op haar eigen contracten beroep doen om deze licenties te voorzien)
- ☐ Aangeven op welke manier data van oplossing na vervanging geraadpleegd & geëxporteerd kan worden.
- ☐ Indien licenties zoals Oracle DB, MS SQL Server etc. aangeschaft moeten worden, moet dit duidelijk aangegeven worden. Indien deze licentie via de leverancier van de oplossing loopt, moet dit in document (meestal afkomstig van de fabrikant) overhandigd worden aan UZB. Dit in geval van controles door desbetreffende softwarefabrikant.

2. Infrastructuur Integratie

- ☐ Updates kunnen zoveel mogelijk zonder downtime (indien onmogelijk, gealigneerd met UZB planning).
- ☐ Elke update moet terugrol-baar zijn (indien DB-integratie,
  moet er een script voorzien worden om deze updates op DB vlak ook terug te draaien.)
- ☐ Totaalconcept moet nog 5 jaar verkocht worden & 10 jaar ondersteund worden na aankoop.
  (voor maatwerk is bij opdrachtnemer een mechanisme van kennisoverdracht in plaats)

☐ Indien de oplossing buiten UZB omgeving gehost wordt,
moet deze aan zelfde voorwaarden als on premise voldoen &
hier kan ook een interne of externe audit op uitgevoerd worden.

☐ Toegangsbeheer en rolverdeling minstens gekoppeld aan de UZB Microsoft AD via MS Azure AD.

☐ Toepassen van multifactor authenticatie kan opgedrongen worden. Al dan niet op advies van de UZB DPO.

☐ Elke **client** (desktop, laptop, tablet, …) in UZB heeft volgende standaarden:

- Client & bijhorende licentie aangekocht door ICT
(tenzij ze deel uitmaken van oplossing die aangeboden wordt of expliciet anders overeengekomen is, licentiedocumenten van onderliggende producten dienen ter beschikking gesteld indien ze deel uit maken van de oplossing).

- Alle verbonden apparatuur (printers, leespennen, scanners, …) zijn voorzien vanuit ICT
(tenzij ze deel uitmaken van oplossing die aangeboden wordt of expliciet anders overeengekomen is).

- Standaard OS is MS Windows 10, voorkeur gaat uit naar de LTSB-versie.
Windows 7 is niet langer aanvaard.

- Voor sommige gebruikers wordt er met VDI gewerkt (op vmware Horizon). Eventuele beperkingen om software op deze platformen te draaien, moet expliciet doorgegeven worden in het designdocument.

- Clients worden gejoined in het AD-domein van uzbrussel.be & beheerd via GPO's. Deze settings gelden voor alle toestellen en kunnen niet zonder overleg met opdrachtnemer veranderd worden.

- Software die op clients in het domein geïnstalleerd wordt, aanleveren in een Microsoft SCCM compatibel formaat (bij voorkeur MSI). Verdeling van software gebeurt door ICT met SCCM. De installatiehandleiding van de software is onderdeel van de as-built documentatie.

- SCCM wordt gebruikt om alle domain clients van de reguliere Windows updates te voorzien. Uitzonderingen hierop komen niet voor tenzij grondig gemotiveerd.

- Alle clients zijn uitgerust met Microsoft Edge (Windows 10). Als alternatief wordt ook Google Chrome toegestaan. Indien een andere browser vereist of aangewezen is dient dit besproken te worden met ICT.

- Alle clients zijn uitgerust met de laatste versie van Adobe Acrobat Reader om eventueel gecreëerde PDF's te openen. Deze wordt via SCCM up-to-date gehouden.

- Alle clients zijn uitgerust met een centraal aangestuurde anti-virus client. Deze wordt door ICT geïnstalleerd, beheerd en up-to-date gehouden. Indien specifieke exclusions nodig zijn, dient dat expliciet in de designdocumenten vermeld te worden. Periodiek wordt een full scan van de client gedaan die de performantie van de client kan beïnvloeden (heeft vooral belang voor eventuele socket-based communicatie. Indien van deze communicatievorm gebruik gemaakt wordt, dient dit expliciet in de designdocumenten vermeld te worden). Andere antivirus systemen zijn niet toegelaten. Het uitschakelen van antivirus systemen is niet toegelaten.

- Geen enkele client op het domein kan of mag, zonder voorafgaand overleg met geautoriseerd UZ Brussel personeel, remote overgenomen worden door de opdrachtnemer.

- Het gebruik van TeamViewer, WebEX, VNC etc is niet toegestaan zonder overleg met UZ Brussel ICT.

- Door opdrachtnemers geïnstalleerde software op clients moet kunnen draaien zonder lokale administrator-rechten. Applicaties moeten overweg kunnen met UAC op de client.

- Alle clients zijn uitgerust met Office 2016 32bit of Office 365. Alle andere vereiste versies van Microsoft Office of analogen moeten expliciet aangegeven worden in het designdocument.

- Indien de oplossing gebruik maakt van Java, dient de oplossing de gebruikte Javaversie naast de reeds aanwezige Java te installeren. Er mag geen interferentie zijn tussen de verschillende Javaversies op een client.

- Indien de oplossing gebruik maakt van .Net, dient de oplossing zich naar de binnen UZ Brussel gangbare versie te aligneren, of ervoor te zorgen dat de gebruikte .Net versie niet interfereert met de standaard gangbare versie.

- Internet toegang is binnen UZ Brussel gekoppeld aan het persoonlijke gebruikersaccount. Serviceaccounts hebben dit privilege standaard niet. Indien de toepassing op de client of gekoppelde randapparatuur toegang tot het internet nodig heeft moet dit expliciet vermeld worden in de design documentatie, met een duidelijke opgave van de nodige firewall rules.

- Applicatie kan draaien zonder local administrator rechten & kan met UAC overweg.

- Installatiepaden, bestandstructuur en schijfindeling is in goed overleg te bepalen.

- Indien de oplossing een toestel vereist dat niet in het domain kan worden opgenomen moet dit expliciet worden aangegeven. Dit moet een uitzondering zijn.

- UZ Brussel heeft een eigen Certificate Authority (CA) die door elk toestel in het domain automatisch is vertrouwd. Mobile devices beheerd via Mobile Iron vertrouwen deze CA ook. Er moet gebruik gemaakt worden van certificaten van de UZ Brussel CA tenzij een publiek certificaat nodig is wat wij dan zullen verschaffen van een externe CA (Commodo).

- Voor email wordt binnen UZ Brussel gebruik gemaakt van MS Exchange
(hybride 2016/Exchange Online installatie).
By default kan geen enkele client of server ongeauthenticeerd mailen. Uitgaande mail naar internet wordt beperkt tot mailadressen met suffix @uzbrussel.be. Andere domein namen worden gefilterd door de mail gateway. Indien de applicatie moet kunnen mailen zijn er 2 mogelijkheden:

a. Authenticated

   i. Via AD credentials
   ii. Mailadressen moeten worden opgegeven

b. Non-authenticated

   i. Het IP-adres wordt toegevoegd in een ACL op de loadbalancer
   ii. Geen controle op mailadres

☐ Bovenstaande standaarden kunnen de toepasbaarheid van een aantal oplossingen beperken zonder dat dit de bedoeling is van ICT. Indien de opdrachtnemer voorziet dat de componenten die hij nodig heeft om zijn oplossing aan te bieden problemen zal ondervinden met hogerstaande standaarden, is het van het uiterste belang om dit bij de beantwoording van deze aanbesteding te signaleren. In overleg met ICT kan dan voor bepaalde standaarden een alternatief gezocht worden.

Afhankelijk van de problemen van de opdrachtnemer met deze standaarden kunnen in goed overleg de volgende alternatieven voorzien worden:

- Client ontvangt geen automatische updates:
  - Consequentie: Na een periode vormt dit een security risico
  - Verwachte actie: ICT zal samen met de opdrachtnemer en de betrokken afdeling(en) een strategie bepalen om deze risico's het hoofd te bieden en kijkt uit naar de voorstellen van de opdrachtnemer in zijn antwoord

- Client wordt uit het domein gehaald en in een apart netwerk (VLAN) gezet achter een Palo Alto firewall:

  - Consequentie: Het voornaamste gevolg is dat de eindgebruiker op deze PC zijn normale administratieve taken en/of patiëntadministratie niet meer kan uitvoeren. Dit houdt dan ook in dat hij/zij meerdere clients nodig heeft, om naast de oplossing van de opdrachtnemer ook zijn andere taken te verrichten. Dit wordt door ICT ten sterkste afgeraden.
  - Verwachte actie: Naast de in de vorige bullet vermelde acties verwacht ICT van de opdrachtnemer ook een compleet overzicht van de communicatie van de clients en de andere IT-componenten van de oplossing, op poort en (eventueel later in te vullen) IP-adres.

- Client wordt uit het domein gehaald, in een apart netwerk (VLAN) gezet achter een Palo Alto firewall en beheerd door de opdrachtnemer:
  - Naast de in de vorige bullet vermelde consequenties en acties verwacht ICT dat de opdrachtnemer SLA's voorstelt bij het beantwoorden van deze aanbesteding, en aan ICT de aanspreekpunten doorgeeft voor service en escalatie.
    Er wordt ook verwacht dat de nodige security maatregelen worden getroffen zoals bvb antivirus. Gebruik van strong passwords en gebruik van Windows firewall.

☐ **Servers** in het UZ Brussel zijn bij voorkeur virtueel en enkel fysiek indien er een zeer grondige reden is daartoe en vooraf goed werd aangegeven. Elke Server in het UZ Brussel domein, onafhankelijk van zijn functie, streeft naar de volgende standaarden:

- Elke door ICT onderhouden server heeft een Microsoft Server Operating Systeem, met Windows 2019 – 1809 of Windows 2022 als OS.

- Voor Linux wordt CentOS 8.x (Alma) of RHEL8 aangeboden.

- Indien er een OVA/OVF wordt aangeboden, verwachten we dat er wordt voldaan aan punten 1 en/of 2 hierboven tenzij hiervoor een grondige reden is.

- Elke server wordt binnen de geleverde applicatie of randapparatuur steeds aangesproken via zijn Fully Qualified Domain Name (FQDN). De domainname is uzbrussel.be. Er wordt gebruik gemaakt van split DNS voor FQDNs die op internet beschikbaar moeten zijn.

- ICT begrijpt dat vooral de validatie van medische apparatuur tijd vergt, en dat daardoor de roadmap van Microsoft niet altijd op de voet kan gevolgd worden. Ondanks dat begrip wordt door ICT geen OS ondersteund dat niet meer door Microsoft zelf ondersteund wordt. Voor nieuwe toepassingen hanteert UZ Brussel de regel dat door de opdrachtnemer geoffreerde oplossingen draaien op een OS dat nog minstens 3 jaar gesupporteerd wordt.

- In principe is elke server gevirtualiseerd via VMware vSphere. Alle bijhorende software licenties ondersteunen het HA & VMotion principe, en er worden geen eisen gesteld die VMotion in gedrang kunnen brengen.
  a. Indien VMware Fault Tolerance nodig is, moet dit worden aangegeven.
  b. Indien VMotion niet is ondersteund, moet dit worden aangegeven en verwachten we hiervoor een uitgebreide uitleg.
     → VMotion is heel belangrijk voor UZ Brussel, daar er iedere 3 maanden gebruik van wordt gemaakt voor redundantietests tussen de computerzalen.

- Servers worden altijd geïnstalleerd door UZ Brussel personeel. Eigen installaties worden niet toegestaan behalve in vorm van een OVA/OVF voor een hardened oplossing (typisch voor Linux servers maar niet voor Windows servers).

- Windows servers zijn gejoined in het UZ Brussel AD-domain uzbrussel.be en worden via GPO's beheerd. Deze settings gelden voor alle toestellen en kunnen niet zonder overleg met de opdrachtgever veranderd worden.
  a. In de baseline GPO wordt onderstaande afgedwongen:
     i. Disable SMBv1 (Windows filesharing)
     ii. Disable LM (LanManager) & NTLMv1
     iii. UAC wordt afgedwongen
     iv. Windows Firewall wordt afgedwongen.
         TCP/UDP-poorten die moeten worden opgezet moet nauwkeurig worden omschreven.
         Het wordt ook toegestaan om eventueel een applicatie te definiëren in de Windows firewall.
         → Alleen inkomend verkeer wordt momenteel gefilterd, in de toekomst kan ook uitgaand verkeer

worden gefilterd & ook hiervan verwachten we gedetailleerde informatie.
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.

- Eventuele specifieke software die geïnstalleerd wordt, zal door de opdrachtnemer in een MSI-formaat opgeleverd worden. De installatiehandleiding van de software is onderdeel van de as-built documentatie. Installatie van de software op de server zelf dient te worden overeengekomen tussen ICT en de opdrachtnemer. Eventuele nieuwe versies/updates volgen hetzelfde pad.

- Alle servers krijgen op reguliere tijdstippen Windows patches. Indien bepaalde patches uit het verleden niet mogen geïnstalleerd worden is het aan de opdrachtnemer om ICT te verwittigen via het designdocument. De opdrachtnemer zal zich organiseren om naar UZ Brussel een duidelijke en gerichte communicatie te doen over toekomstige patches die niet mogen geïnstalleerd worden, en dit binnen de 2 weken nadat Microsoft ze uitbrengt. Indien de opdrachtnemer niet communiceert, zijn de eventuele gevolgen van het patchen voor de opdrachtnemer.

- Alle servers zijn uitgerust met anti-virus software. Deze tool wordt door ICT geïnstalleerd, beheerd en up-to-date gehouden. Indien exceptions moeten ingesteld worden dient dat in de designdocumenten vermeld te worden. Periodiek wordt een full scan van de server gedaan die de performantie kan beïnvloeden (dit heeft vooral belang voor eventuele socket-based communicatie. Indien van deze communicatievorm gebruik gemaakt wordt, dient dit expliciet in de designdocumenten vermeld te worden).

- Geen enkele server op het domein kan of mag, zonder voorafgaand overleg met geautoriseerd UZ Brussel personeel, remote overgenomen worden door de opdrachtnemer. Tijdens de projectfase wordt voor de oplossing een domein account voorzien waarmee de installaties zullen gebeuren. Na de projectfase wordt deze account disabled. Na het project kan de leverancier toegang krijgen tot de omgeving op de standaard UZ Brussel manier; Indien dit nodig is moet dit in overleg met ICT besproken worden gedurende het project. Men kan gebruik maken van een SSLVPN of een VPN Pulse Secure Client (hetzij via One Time Password, eID of TOTP) in combinatie met onze PAM oplossing.

- Indien men gebruik maakt van een eigen remote control systeem zoals bvb Axeda moet dit worden beschreven en goedgekeurd door UZ Brussel. UZ Brussel moet ten allen tijden weten wie heeft aangelogd op de systemen.

- Er wordt een duidelijk verschil gemaakt tussen installatie/support accounts en service accounts:
  a. Er wordt een account voorzien voor de installatie en support van de applicatie(s) maar dit account wordt na de installatie disabled. Dit account mag dus niet worden gebruikt om bvb een service te draaien, een database connectie te maken of om bvb een fileshare te mounten.
  b. Indien een service domain credentials nodig heeft ipv de default system account wordt hiervoor een service account aangemaakt.
  c. Het wachtwoord van een service account mag niet in clear text zichtbaar zijn in configuratie bestanden.
     i. Er wordt duidelijk aangegeven waar deze service accounts worden gebruikt (registry, configuratie bestanden etc).

- In operationele fase (productie) draaien alle applicaties als services die géén administrator rechten nodig hebben om hun functie uit te voeren. GUI-based executables die gebruikt worden op de servers (processen die niet als service kunnen worden gestart), worden niet geaccepteerd. Indien nodig wordt steeds gebruik gemaakt van domein serviceaccounts die door UZ Brussel aangemaakt zijn. De

omschrijving van de rechten van deze service-accounts zijn onderdeel van de as-built documentatie.

a. Bij voorkeur wordt er gebruik gemaakt een Group Managed Service Account waarvan het password wordt beheerd door AD.
b. Indien er geen gebruik kan worden gemaakt van een (g)MSA-account moet dit worden verantwoord.

- Internet toegang van op operationele servers of communicatie met specifieke publieke adressen op het internet, is standaard niet toegestaan. Indien de leverancier dit onmisbaar acht voor zijn applicatie kan hij dat aangeven. In dat geval wordt er een uitzondering op deze regel gemaakt en verwachten we van de leverancier:

a. Voor verkeer naar het internet: Een voorstel voor detail configuratie van onze firewall (zowel Windows firewall als netwerk firewall).
b. Voor applicaties die van buitenaf beschikbaar moeten zijn: de details om dit op een gecontroleerde manier mogelijk te maken (URL's, IP-adressen, poorten, protocollen, …)

- Alle resources, services en alle server operating systemen worden gemonitord via MonitorNow. In het designdocument geeft de opdrachtnemer aan welke services, URLs er van belang zijn voor zijn toepassing, de te meten thresholds en de onderlinge relatie tussen de verschillende services en de user experience.

- Alle nodige certificaten worden intern ondertekend door de UZ Brussel certificate authority.

- UZ Brussel heeft een eigen Certificate Authority (CA) die door elk toestel in het domain automatisch is vertrouwd. Mobile devices beheerd via Mobile Iron vertrouwen deze CA ook. Er moet gebruik gemaakt worden van certificaten van de UZ Brussel CA tenzij een publiek certificaat nodig is wat wij dan zullen verschaffen van een externe CA (Commodo).

- Er wordt bij voorkeur gebruik gemaakt van Kerberos authenticatie en niet van NTLMv2.

- De leverancier zal naast een as-built documentatie ook een duidelijk schema voorzien waar de server componenten en informatiestromen en dependancies zichtbaar zijn.

- Er moet een korte operationele procedure worden aangeleverd zodat de beschikbaarheid van het systeem snel kan worden gecontroleerd na het patchen/rebooten van de server.

- Als backup oplossing wordt CommVault gebruikt. Er worden voor virtuele servers default 3 snapshots per dag voorzien waar een application consistent backup wordt genomen wat inhoudt dat de applicatie tijdens de snapshot actie een quiesce moet kunnen verwerken. Indien de applicatie hier niet tegen kan moet dit worden aangegeven.

- Bij het gebruik van webservers moet er gebruik worden gemaakt van HTTPS. UZ Brussel kan een certificaat aanleveren van de interne CA of indien nodig van een externe CA.

a. Hiervoor verwachten van de leverancier een subject & SAN namen en waarvoor het certificaat wordt gebruikt (server authentication en/of client authentication of andere).

- Er mogen geen onveilige protocollen worden gebruikt zoals bvb http, ftp, telnet ...

- Applicatie data wordt bij voorkeur altijd buiten de VM opgeslagen op een NAS lokatie zodat de VM niet te groot wordt. UZ Brussel beschikt voor een hoog beschikbaar storage platform (MetroCluster) waar deze data kan worden opgeslagen. Deze aanpak zorgt ervoor dat de VMDK disken niet te groot worden

en dat de storage snel en efficiënt kan worden vergroot. Voor applicatieve data kan dan een apart retention policy voor backup worden gebruikt.

- Er mogen geen local shares worden aangemaakt op windows servers zonder kennis van UZ Brussel. Indien deze nodig zijn worden deze aangemaakt door UZ Brussel zodat de nodige AD-groepen kunnen worden aangemaakt en NTFS-rechten kunnen worden gezet.

- Er moet gebruik worden gemaakt van LDAPS indien men wil verbinden met Active Directory (geen LDAP).

- Voor email wordt binnen UZ Brussel gebruik gemaakt van MS Exchange (hybride 2016/Exchange Online installatie). By default kan geen enkele client of server ongeauthenticeerd mailen. Uitgaande mail naar internet wordt beperkt tot mailadressen met suffix @uzbrussel.be. Andere domein namen worden gefilterd door de mail gateway. Indien de applicatie moet kunnen mailen zijn er 2 mogelijkheden:

a. Authenticated

i. Via AD credentials
ii. Mailadressen moeten worden opgegeven

b. Non-authenticated

i. Het IP-adres wordt toegevoegd in een ACL op de loadbalancer
ii. Geen controle op mailadres

- Indien er nood is aan het gebruik van nVidia GPU-kaarten moet dit worden aangegeven. Het type licentie voor nVidia Grid moet worden doorgegeven, net als het gewenste profiel.

☐ Een aantal servers bieden specifieke functies. UZ Brussel moedigt consolidatie hiervan sterk aan. In dit geval zijn:

- Communicatieserver (HL7 gebaseerde berichten)
Alle communicatie van de oplossing van de opdrachtnemer met de centrale systemen verloopt over HL7 of bij hoge uitzondering een ander overeengekomen protocol. Mirth is facilitair aan deze communicatie binnen UZ Brussel. Ofwel voorziet de opdrachtnemer socket-based communicatie met Mirth (voorkeur), ofwel wordt een share voorzien op het centrale storage platform of op (een van) de servercomponent(en) van de toepassing één of twee shares gedefinieerd voor in-en uitgaande file gebaseerde communicatie.

- Database server
Vanuit ICT wordt enkel Microsoft SQL Server & SAP ASE als standaard ondersteund. ICT stelt de opdrachtnemer een of meerdere databases op zijn centrale SQL 2016 database (AlwaysOn Availability Group) cluster ter beschikking en neemt de verantwoordelijkheid voor licenties, installatie van de database (SQL-script te voorzien door de opdrachtnemer), 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 troubleshooting activiteiten krijgt de opdrachtnemer de juiste contacten.
Als DBA-analyses aantonen dat een bepaalde query de performantie van het systeem bedreigt verwachten we van de opdrachtnemer een tijdige en efficiënte reactie. Er worden geen sysadmin rechten toegekend aan de leverancier op de centrale MS SQL cluster.
Indien er andere databases nodig zijn zal de leverancier deze zelf moeten installeren en onderhouden. De leverancier zal op regelmatige basis ook de database software moeten updaten/patchen op eigen

verantwoordelijkheid (security patches).
De licentie voor deze database moet worden voorzien door de leverancier. De leverancier moet rekening houden met het feit dan deze database server op een vmware virtueel platform 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 minstens TLS1.2 of hoger.

- Load balancer
Om een oplossing full tolerant en high available te maken biedt UZ Brussel zijn NGINX-software load balancer, HA Proxy of Reverse Proxy aan voor die applicaties die hiermee om kunnen.

- File server
UZ Brussel bezit centrale fileserver-systemen (metro cluster) en een lange termijn file opslag op archief. Data kan tot een jaar worden bijgehouden op een tier2 disk array en voor langere termijn wordt tape voorzien. Alle file serving / NAS-behoeften dienen op deze reeds aanwezige systemen voorzien te worden.

- Back up / restore
  a. Van elke virtuele server in beheer van UZ Brussel, worden er standaard dagelijks 3 snapshots voorzien.
     i. Deze zijn default application consistent (applicatie mag geen problemen hebben met een quiesce) of eventueel crash consistent. De keuze moet worden aangegeven door de leverancier.
  b. Van fysieke servers wordt door UZ Brussel een CommVault agent geïnstalleerd. ICT verwacht een lijst van de folders die meegenomen moeten worden in de backup in de as-built documentatie.
  c. Voor databases voorziet ICT de volledige back-up en restore op voorwaarde dat de database gesupporteerd wordt (zie hoger). Voor MSSQL worden er transaction backups voorzien elk half uur. Indien er toch andere DB-systemen gebruikt worden, vervalt de paragraaf over databases hoger in dit document en dient de leverancier zelf voor de installatie, back-up en ondersteuning in te staan. In dergelijke gevallen zal ICT enkel zorgen voor een file-based back-up van een database export die de leverancier voorziet.

☐ Bovenstaande standaarden kunnen de toepasbaarheid van een aantal oplossingen beperken zonder dat dit de bedoeling is van ICT. Indien de opdrachtnemer voorziet dat de componenten die hij nodig heeft om zijn oplossing aan te bieden problemen zal ondervinden met hogerstaande standaarden, is het van het uiterste belang om dit bij de beantwoording van deze aanbesteding te signaleren. In overleg met ICT kan dan voor bepaalde standaarden een alternatief gezocht worden.
Afhankelijk van de problemen van de opdrachtnemer met deze standaarden kunnen in goed overleg de volgende alternatieven voorzien worden:

- Indien er om een voldoende gemotiveerde reden toch door een opdrachtnemer server hardware aangeleverd wordt, gebeurt de installatie en plaatsing op het domein altijd door de ICT-dienst, en dienen de onderstaande ICT-richtlijnen gerespecteerd te worden.
- Server wordt uit het domein gehaald in een apart netwerk (VLAN) gezet en achter een firewall gestoken.
Naast het hoger vermelde punt verwacht ICT van de opdrachtnemer ook een compleet overzicht van de communicatie van de server(s) en de andere IT componenten van de oplossing, op (eventueel later in te vullen) IP adres en poort.

3. Beveiliging

☐ Traceerbaarheid.
Mutaties van data in het systeem en/of op de apparatuur wordt gelogd. Op ieder ogenblik is te achterhalen wat er gebeurd is, wanneer het gebeurd is en wie de wijziging uitgevoerd heeft.

☐ Installaties.
De apparatuur is beschermd tegen door UZ Brussel ongewenst installeren van apparaat-vreemde software door onbevoegden.

☐ Beveiligingslekken in hard- en software.
De opdrachtnemer verbindt zich ertoe om deze lekken zo snel mogelijk kenbaar te maken aan UZ Brussel

☐ Ehtical Hacking platform:
UZB maakt gebruik van een Ethical Hacking platform waarbij ethische hackers kwetsbaarheden opsporen bij publieke websites onder ons domein.
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.

☐ Er wordt enkel gebruik gemaakt van ge-encrypteerde verbindingen. Er wordt dus geen gebruik gemaakt van http maar van https, van ldap ipv ldaps etc. Indien dit niet het geval is moet dit worden aangegeven door de leverancier

☐ 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 nog gesupporteerde 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.

☐ Fouten en foutdetectie.
Het systeem bevat middelen voor de detectie en correctie van fouten in de invoer, de verwerking, de uitvoer en de verspreiding van gegevens. Het systeem bevat middelen voor de verificatie van de volledigheid, juistheid en authenticiteit van de interne en externe verspreiding van de gegevens.Het systeem voldoet aan de geldende richtlijnen op moment van gebruik vanuit overheid voor onder andere het beveiligen van de informatiegegevens.Hoger vermelde logging van activiteiten worden bewaard en UZ Brussel is in staat om deze logging te consulteren zonder interactie met de opdrachtnemer.

☐ Authentificatie en authorisatie.
- Bij voorkeur worden wachtwoorden niet binnen de toepassing zelf bewaard.
  Indien dit toch het geval is, dienen deze te worden gesalt en gehasht.
- Er wordt bij voorkeur gebruik gemaakt van Kerberos authenticatie over NTLM-authenticatie.
- Iedere gebruiker heeft zijn unieke login/paswoord combinatie; er worden geen generieke accounts toegestaan. Authenticatie binnen de applicatie wordt bij voorkeur geïntegreerd in de Microsoft Active Directory omgeving van UZ Brussel.
- Autorisatiemogelijkheden binnen het aangeboden product dienen duidelijk aangegeven te worden.

Binnen een multi-user applicatie kan de functioneel beheerder de bevoegdheden van de (types)gebruikers systematisch vastleggen en via rapportage inzichtelijk maken aan het management. Er is minimaal een onderscheid in rechten voor lezen, toevoegen, wijzigen en verwijderen van gegevens Idealiter kunnen de (types) gebruikers gerelateerd worden aan een Microsoft Active Directory groep. Gebruikersbeheer moet maximaal geautomatiseerd worden via Active Directory, zonder dat manuele tussenkomst nodig is bij creatie, wijzigingen en stopzetten van gebruikers. De naamgeving wordt vooraf met de ICT-dienst afgesproken.

- Er wordt bij het aanloggen in de applicatie een beveiligde verbinding met Active Directory gemaakt, waarbij aan AD gevraagd wordt of de betrokken gebruiker toegang krijgt, op welk niveau, en of zijn opgegeven wachtwoord klopt. Indien dat niet mogelijk is, moet dit expliciet vermeld worden in de design documentatie.
- Paswoorden voor administratie doeleinden gebruikt in de applicaties moeten worden meegedeeld aan UZ Brussel (non AD based accounts).
- Bij voorkeur worden installaties uitgevoerd onsite met een UZ Brussel system engineer die de installatie superviseert.
- Bij oplevering wordt de installatie met een system engineer van UZ Brussel overlopen om te kijken of alle guidelines zijn gevolgd. Deze kan/zal ook dienen als een basiskennis overdracht.
- Binnen een multi-user applicatie dient altijd een authenticatie plaats te vinden bij het opstarten van de applicatie. We bieden Single-Sign-On aan voor onze gebruikers via Imprivata. Integratie met SSO draagt de voorkeur. Gebruikers authentiseren zich via hun personeelsbadge.

<u>Indien één of meerdere van bovengemelde vereisten niet wordt voldaan kan dit resulteren tot een negatief advies voor aankoop.</u>