**UZ Brussel Installation Conditions**

**Checklist**

# Objective

This document contains a checklist that was drafted by the IT department of the UZ Brussel hospital.   
The goal is to ensure a more fluid implementation of a project after the acquisition procedure and to be able to anticipate the planning of resources.   
For further inquiries, you can contact the IT department at security@uzbrussel.be.

This checklist is a simplified version of the complete “Installation Conditions” document.   
Upon completion of het implementation, a UZB system engineer will make sure all guidelines were followed by verifying the installation together with the supplier.  
This can & will serve as a basic knowledge transfer of the environment.  
  
If one or more of the mentioned requirements are not met, this may result in a negative recommendation for purchase.

# Licenses

|  |  |
| --- | --- |
|  | Answer |
| Not enforced by hardware solutions like keys & dongles? |  |
| Fixed MAC address/VM Hardware ID necessary? |  |
| Only needed for production? |  |
| OS/DB/Supporting license needed? |  |
| Post mortem data recovery procedure? |  |

# Infrastructure

|  |  |
| --- | --- |
|  | Answer |
| Rollback scenario updates? (incl possible DB scripted rollback) |  |
| Update without downtime? (If not, what is the downtime?) |  |
| Total concept will be sold for at least 5 years,  supported for 10 years? |  |
| Access control & RBAC at least linked to UZB MS AD or via Azure AD? |  |
| Possibility to implement MFA? |  |
| MS Exchange 2016 compatible? (see installation requirements for limitations) |  |
| Client | Desktop/Laptop/Tablet/… |
| Client & license acquired by UZB? |  |
| Connected equipment provided by UZB? |  |
| Windows version (preference = 10 LTSB)? |  |
| Does the solution work on VDI  (vmware Horizon)? |  |
| Clients are member of uzbrussel.be AD-domain, managed by GPO’s. Adjustments needed? (if non-AD joined required, provide reasoning) |  |
| Client software in SCCM format? (Preferably MSI) including deployment manual? |  |
| Non-Edge or Google Chrome browser? |  |
| Objection to latest Adobe Acrobat Reader version? |  |
| Objection to use of standard UZB  anti-virus client? (TrendMicro ApexOne) |  |
| Exclusions needed for anti-virus client? |  |
| Is socket-based communication used? (On which the anti-virus full scan may have a negative effect)? |  |
| Can the solution handle UAC on the client? |  |
| Can the solution run without local administrator rights? |  |
| TeamViewer/WebEx/VNC/etc needed? (only after consulting with UZB ICT) |  |
| Other version than MS Office 2010/2016 32bit needed? |  |
| Java needed?  If yes, run it in addition to installed version. |  |
| Microsoft .NET needed? If yes, align with current UZB version or make sure it does not interfere with the UZB version. |  |
| Internet access required? (if yes, to what URL?) |  |
| Installation path, file structure and disk layout known? (if yes, explain) |  |
| Objection to use of UZB CA? Or is a public certificate required? |  |
| Objection to Windows security patching? |  |
| Server |  |
| Objection to a virtual server? |  |
| OVA/OVF, or server provided by UZB? |  |
| MS Windows 2019 (1809), 2022,  CentOS 8.x/Alma, RHEL8 of CentOS 7.x (conditional)? |  |
| Does solution run on OS that is still supported for at least 3 years? |  |
| Is the server within the delivered solution addressed with its FQDN? (domain name uzbrussel.be, FQDN that must be available on internet will use split DNS) |  |
| Does the solution support HA/vMotion on vSphere 7.x? (if not, argumentation required) |  |
| Is Fault Tolerance needed? |  |
| Servers are members of the uzbrussel.be AD domain, which is managed by GPOs (see installation conditions for listing). Adjustments needed? (if not AD joined required, please justify) |  |
| Software installation required? (If yes, MSI-format, accompanied by installation guide) |  |
| Objections to (certain?) MS Windows security patches? To be reported within 2 weeks after release by Microsoft. |  |
| Objection to use of standard UZB anti-virus client? |  |
| Exclusions needed on the anti-virus client? |  |
| Is socket-based communication used? (On which the anti-virus full scan may have a negative effect)? |  |
| No remote takeover of servers without consulting the UZB IT department. Access can be granted via VPN through the Pulse Secure Client & our PAM solution,  is this necessary? |  |
| Is another remote control system (e.g. Axeda) used? |  |
| Objection to disabling the installation account after the solution installation? |  |
| Service account(s) needed? \* If yes, which specific rights? (no local administrator rights will be granted)  \* UZB default standards:  Non-OS related services MUST run with a SA. Preferably MSA without admin rights (eg Windows APIs, services, IIS pools usage), otherwise a “classic” SA without admin rights. |  |
| Is the password of the service account(s) visible in clear text in configuration files? |  |
| Can the solution/application handle Active Directory Group Managed Service Accounts (gMSA, password managed by AD)?  If not, please explain why. |  |
| Does the solution/application run as a service? |  |
| Internet access needed? If yes, details are needed (incoming, outgoing, URL’s, IP’s, ports, protocols)? |  |
| What services & URLs are important to monitor with what thresholds (with what interrelationships between the services and the user experience) via MonitorNow? |  |
| Objection to use of UZB CA? Or is a public certificate required? |  |
| Usage of Kerberos authentication or NTLMv2? |  |
| Schema van server components, Information flows and dependencies? |  |
| Operational procedure supplied for system check after patching/rebooting the server? |  |
| Can the solution/application handle quiesce for snapshot/backups? |  |
| Does the solution/application use a web server?  If so, does it use HTTPS? In addition, what are the subject & SAN names for which the certificate (provided by UZB) is used? |  |
| Does the solution/application use HTTP/FTP/Telnet or any other insecure protocols? |  |
| Can the application data be stored outside the VM at a NAS location (NetApp Metro Cluster)? |  |
| Are local shares needed? |  |
| Is an Active Directory connection required? If so, does it use LDAPS? |  |
| nVidia GPU-cards needed?  If yes, type license for nVidia Grid & desired profile? |  |
| Communication server | (HL7 based messages) |
| Is socket-based communication with Mirth foreseen? If not, is a share provided on the central storage platform or on (one of) the server component(s) of the application one or two shares identified for in-and outgoing file based communication? |  |
| Database server |  |
| SAP ASE, MS SQL2016 (AlwaysOn, Availability Group)? |  |
| If no SAP ASE or MS SQL, what DB? Maintained by the supplier? Does the supplier provide the license as well? |  |
| Report services or other DB activities (SSIS, SSAS, SSRS, ETL, …) needed? |  |
| No sysadmin rights needed? |  |
| Communication between application and DB servers encrypted with at least TLS 1.2 or higher? |  |
| Load balancer |  |
| NGINX-software/HA Proxy load balancer or Reverse proxy needed? |  |
| File server |  |
| Fileserver or long-term file storage on archive (up to 1 year on tier2 disk array or tape if longer) needed? |  |
| Backup / Restore |  |
| Every virtual server managed by UZB gets daily 3 snapshots by default (6h-12h-18h),  is this sufficient? |  |
| Can the application handle quiesce or not? (results in application - or crash consistent backups) |  |
| If physical server, a Commvault agent must be installed. List of folders that need to be backed up? |  |
| Is the DB supported (see above)? Then UZB foresees complete backup & restore.  If other DB, the supplier needs to foresee this. UZB will take care of the file-based backup of the DB export that is to be foreseen by the supplier. |  |

# Security

|  |  |
| --- | --- |
|  | Answer |
| Are mutations of data in the system and/or on the equipment logged? |  |
| Is the equipment protected against by UZB unwanted installation of software unknown to the equipment by unauthorized persons? |  |
| Does the contractor commit to disclosing security breaches to UZB as soon as possible? |  |
| Does the contractor commit to paying the bounty if the public website/application provided by him would have a vulnerability (that could have been avoided) found by one of the ethical hackers (linked to the Intigriti Ethical Hackers platform, which UZB is client of) ? |  |
| Are only encrypted connections used?  (HTTPS, LDAPS, …) |  |
| Are all supplied software & runtime environments (java, .net, python, …) free of known security issues? |  |
| Is there a description given of every software component including its version & ongoing warranty/support? |  |
| Does the solution include means of detection and correction of errors on input, processing, output and the dispersion of data? |  |
| Does the solution comply with the applicable guidelines at the time of use from the government for, among other things, securing the information data? |  |
| Has the above-mentioned logging of activities been preserved and is UZB able to access this logging without interaction with the contractor? |  |
| Are the passwords, if stored within the application, salted and hashed? |  |
| Does authentication within the application use integration with UZB’s MS AD environment? If not, please specify the authorization options within the product, as well as the passwords to pass on. |  |
| Are only individual login/password combinations used and therefore no generic accounts? |  |
| Does the solution support multi-user? If yes: - Is there a minimal segregation in terms of user rights (read/write/modify/…)? - Are the type of user rights easily presented in a report? |  |
| Can the application handle Imprivata as a  Single-Sign-On solution? |  |

# Contact Details

Company: ……………………………………………………

Commercial:

Name & Surname: …………………………………………………………………

Date: …………………………

Signature for approval: …………………………………………………….

IT Technical:

Name & Surname: …………………………………………………………………

Date: …………………………

Signature for approval: …………………………………………………….