UZ Brussel IT installation conditions

1. Licences
The licensing mechanism may not impose any restrictions on the operation of systems and/or equipment. In other words, the continuity of the solution must always be ensured.
Licences should be easily transferable to replacement systems and such transfer should preferably not be enforced through hardware-based solutions (keys, dongles, etc.).
To prevent licence-related issues during migrations, a specific mention should be made wherever it is necessary for licences to have specific properties such as e.g. MAC address or VM hardware ID, etc.
No licensing issues should arise during upgrades e.g. VM hardware compatibility – in case there are known issues, the company should specifically state this and should also provide a solution.
No additional licences should be required in order to set up a test, training or acceptance environment. Licences shall only be requested for the production environment.
If supporting products (operating systems, database systems, etc.) require licences, this must be clearly stated and must not be an enforceable part of the solution – consequently, UZ Brussel must be free to provide the necessary licences under its own contracts with the necessary suppliers.
Whenever a solution is introduced, information should be provided concerning how it will still be possible to access data from the solution even after its replacement.

UZ Brussel must be clearly notified if licences have to be purchased for certain software such as Oracle database, Microsoft SQL Server, etc.
If the company offers the licence, it shall provide UZ Brussel with a document that can be presented to the relevant software manufacturer for verification purposes.

2. Integration with the infrastructure.
2.1 General: every device/system shall be prepared for the future
The total concept shall guarantee maximum flexibility to meet the rapid developments in the field of IT. The concept shall provide a mechanism to systematically develop new functionalities and options, which can be added via updates/upgrades.
- It should be possible to conduct updates without downtime; if such downtime cannot be avoided, it should be aligned with the maintenance windows that the IT department has agreed upon with its internal customers.
- It should be possible to roll back all updates. Wherever updates involve changes to the database, a separate script to roll back these updates must also be provided.

The total concept will be sold for another 5 years and support for it will be provided for the next 10 years. In case of customised work, the contractor has a knowledge transfer mechanism in place.

2.2 SaaS and PaaS solutions
Solutions hosted outside the UZ Brussel environment must comply with the same standards as UZ Brussel and as such it must be possible for the same to be audited by internal or external auditors. As a minimum requirement, it must be possible to resolve the access management and role distribution in such solutions via user groups linked to the UZ Brussel Microsoft Active Directory via Microsoft Azure AD.
It should be possible to impose multi-factor authentication according to the recommendations of DPO of UZ Brussel.

2.3 Clients
2.3.1 Client Standards
Every client in the UZ Brussel domain strives to achieve the following standards:

1. In principle, all desktops, laptops, tablets, etc. (abbreviated as “clients” in what follows) and any associated OS licences shall be purchased by the IT department, unless they are an intrinsic part of the solution offered by the contractor or unless explicitly agreed otherwise and approved by the IT department of UZ Brussel.

2. In principle, all equipment connected to a client (such as printers, reading pens, barcode scanners, etc.) shall be purchased or provided by the IT department from standard solutions, except where:
   a. they constitute an intrinsic part of the solution offered by the contractor, or
   b. it is explicitly agreed otherwise.

3. The standard client operating system shall be Microsoft Windows 10. Windows 7 shall no longer be accepted. An LTSSB (long-term servicing branch) version shall be preferred for Windows 10.

4. For some mobile users, we also use virtualisation via VMware VDI (Horizon). The design document, discussed later, must explicitly mention the restrictions if any on running the software on these platforms.

5. The clients in UZ Brussel shall be joined under the Active Directory domain of uzbrussel.be and managed via GPOs. These settings shall apply to all devices and it should not be possible to change the same without consulting the contractor.

6. The contractor shall deliver all software installed on clients within the domain, in a format that can be distributed using Microsoft SCCM (preferably MSI format). The IT department shall distribute the software with SCCM. The relevant software installation manuals shall be included in the as-built documentation.

7. Regular Windows updates shall also be provided to all domain clients via SCCM. Exceptions shall only be permitted provided a comprehensive statement of the reasons for the same is given.

8. All clients shall have Microsoft Internet Explorer 11 (Windows 7 and 10) and Microsoft Edge (Windows 10) installed on them. Internet Explorer (IE) 11 shall be the default browser. Google Chrome is also permitted as an alternative.
   The use of older versions of IE (Internet Explorer) is not permissible. If another browser is required or appropriate, it shall be necessary to discuss the same with the IT department.

9. All clients shall be equipped with the latest version of Adobe Acrobat Reader to open any PDFs created. Both shall be kept up to date via SCCM.

10. All clients shall be equipped with a centrally controlled antivirus environment. The IT department shall install, manage and update this tool. Wherever it is necessary to establish specific exclusions, this should be explicitly mentioned in the design documents.
    A full scan of the client, which can influence the performance of the client, shall be carried out periodically. This is especially important in case of socket-based communications if any.
    The design documents must explicitly mention the use of this form of communication.
    Other antivirus systems are not permitted. It is not permissible to disable antivirus systems.

11. The contractor cannot/may not be able to remotely take over any client on the domain without first consulting the authorised UZ Brussel personnel.

12. TeamViewer, WebEX, VNC, etc. may only be used after first consulting the IT department of UZ Brussel.

13. It should be possible to run software installed by contractors on clients without local administrator rights. There must be compatibility (interoperability) between applications and UAC on the client.
14. All clients shall be equipped with Microsoft Office 2010 or 2016 32 bits. The design document must specifically mention any other versions of Microsoft Office, etc. that may be required.

15. If the solution uses Java, it must install the Java version used in addition to the existing Java. There should be no interference between the different Java versions on a client.

16. If the solution uses .Net, the solution must be aligned with the current version in use within UZ Brussel, or it must be ensured that the used .Net version does not interfere with the standard current version.

17. Internet access within UZ Brussel must be linked to the personal user account. By default, service accounts shall not have this privilege. If Internet access is required for the application on the client or connected peripherals, this and the required firewall rules must both be explicitly mentioned in the design documentation.

18. Installation paths, file structure and disk layout shall be determined through mutual agreement.

19. If the solution requires a device that cannot be included in the domain, this must be explicitly stated. This must only happen in exceptional cases.

20. UZ Brussel has its own Certificate Authority (CA) which is automatically trusted by every device in the domain. Mobile devices managed through Mobile Iron must also trust this CA. Certificates from the UZ Brussel CA must be used except where a public certificate is required – if so, we will provide this via an external CA (Commodo).

21. UZ Brussel uses Exchange2016 (on premise installation) for email. By default, no client or server can conduct mail correspondence without authentication. Outgoing mail to the Internet is limited to mail addresses with suffix @uzbrussel.be. Other domain names shall be filtered by the mail gateway. If mail correspondence is necessary for the application, there should be two options:

   a. Authenticated
      i. Via AD credentials
      ii. Mail addresses must be specified
   b. Non-authenticated
      i. The IP address is added in an ACL on the load balancer
      ii. No monitoring of mail address

4.3.2 Exceptions and alternatives to client standards

Client standards may limit the usability of some solutions – in a manner not intended by the IT department. It is crucially important that in his tender, the contractor should explicitly mention the possibility of compatibility issues between his aforementioned standards and the components he needs to use in his solution. Alternative standards can then be sought in consultation with the IT department.

Depending on the contractor’s problems with these standards, the following alternatives may be provided after close consultations:

- **Client does not receive automatic updates.**
  
  **Consequence:**
  After a period of time, this constitutes a security risk.
  
  **Expected actions:**
  The IT department, together with the contractor and the department(s) concerned, will define a strategy to deal with these risks and looks forward to the contractor’s proposals in its response.

- **Client is removed from the domain and put into a separate network (VLAN) behind a Palo Alto or Juniper firewall.**
Consequence:
The principal consequence is that the end user can no longer perform his normal administrative tasks and/or patient administration on this PC. This will mean that apart from the contractor’s solution, he/she will need to use several clients in order to perform his/her other tasks. The IT department strongly disapproves of this.

Expected actions:
Apart from the actions specified in the previous bullet point, the IT department also expects the contractor to provide a complete overview of the communication of the clients and the other IT components of the solution, on the port and (possibly to be filled in later) IP address.

- The client shall be removed from the domain, placed in a separate network (VLAN) behind a Palo Alto or Juniper firewall and managed by the contractor.
  Apart from the consequences and actions mentioned in the previous bullet point, the IT department expects the contractor to propose SLAs when responding to this tender, and to notify the IT department of the contact points for service and escalation.
  It is also expected that the necessary security measures such as antivirus shall be taken.
  Use of strong passwords and use of windows firewall.

4.4 Server equipment

4.4.1 Server standards
Servers at the UZ Brussel shall preferably be virtual and shall only be physical provided there is a well-founded reason for the same, which shall be stated in advance. Each server in the UZ Brussel domain, irrespective of its function, strives to conform to the following standards:

1. Every server maintained by IT department has a Microsoft Server Operating System, with Windows 2016 - 1607 or Windows 2019 - 1809 as OS.
2. If Windows is not an option, we can also offer a Linux server. For Linux, CentOS 8.x or RHEL8 shall be offered. CentOS 7.x shall be accepted under certain conditions.
3. If an OVA/OVF is offered, we shall expect compliance with one and/or two above, unless there is a well-founded reason for the same.
4. Each server within the delivered application or peripherals shall always be addressed via its Fully Qualified Domain Name (FQDN). The domain name is uzbrussel.be. Split DNS shall be used for FQDNs that must be available on the Internet.
5. The IT department appreciates that the validation of medical equipment is a time-consuming process, and consequently that strict adherence to Microsoft’s roadmap cannot always be ensured. Notwithstanding the above, the IT department does not support an OS that will no longer be supported by Microsoft itself.
   In case of new applications, UZ Brussel requires that solutions offered by the contractor must run on an OS that is supported for at least another three years.
6. Basically, every server is virtualised via VMware ESX 6.5 or 6.7. All associated software licences shall support the HA and VMotion principle, and no requirements that could compromise VMotion shall be imposed.
   a. If VMware fault tolerance is required, this must be specified.
   b. If VMotion is not supported, this must be stated and we shall expect a detailed explanation.
      i. VMotion is very important for UZ Brussel because we carry out a redundancy test every quarter, in which a computer room is emptied – we rely on VMotion for the same.
7. Servers shall always be installed by UZ Brussel personnel. The contractor may not bring along its own installations except in the form of an OVA/OVF for a hardened solution (typical for Linux servers but not for Windows servers).

8. The windows servers shall be joined under the UZ Brussel AD domain uzbrussel.be and shall be managed via GPOs. These settings shall apply to all devices and may not be changed without first consulting the customer.
   a. The following shall be enforced in the baseline GPO
      i. Disable SMBv1 (windows file sharing)
      ii. Disable LM (LanManager) and NTLMv1
      iii. UAC shall be enforced
      iv. Windows Firewall shall be enforced. TCP/UDP ports to be set up must be precisely defined. It shall also be permissible to define an application in the Windows firewall if necessary.
         1. Only incoming traffic is currently filtered, but it should be possible to filter outgoing traffic in the future and we also expect detailed information concerning the same.
      v. User Rights Assignment (Windows privileges) shall only be managed via GPO and it should not be possible to control them via a local GPO (e.g. act as part of the OS, local login rights, etc.)
      vi. SSL2.0, 3.0, TLS1.0 and 1.1 shall be disabled by default.

9. The contractor shall deliver all specific software installed on servers in the domain in an MSI format. The relevant software installation manuals shall be included in the as-built documentation. Installation of the software on the server itself must be agreed between the IT department and the contractor.
   Any new versions/updates shall follow the same path.

10. All servers shall receive Windows patches at regular intervals.
    If certain patches from the past may not be installed, the contractor shall be responsible to notify the IT department via the design document.
    The contractor shall organise itself to communicate with UZ Brussel clearly and in a targeted manner concerning future patches that it is not permissible to install, within two weeks after being released by Microsoft.
    If the Contractor does not notify the same, it shall bear all the consequences of patching if any.
11. All servers shall be equipped with antivirus software. The IT department shall install, manage and update this tool. Exceptions if any shall be stated in the design documents.
   A full scan of the server, which can influence the performance, shall be carried out periodically. This is especially important in case of socket-based communications if any. The design documents must explicitly mention the use of this form of communication.
12. The contractor cannot/may not be able to remotely take over any server on the domain without first consulting the authorised UZ Brussel personnel. During the project phase, a domain account shall be provided for the solution with which the installations will take place. This account shall be disabled at the end of the project phase.
   After the project, the supplier shall be able to access the environment according to normal UZ Brussel procedures; if necessary, this must be discussed with the IT department during the course of the project. An SSLVPN or a VPN Pulse Secure Client may also be used.
   a. One Time Password
   b. eID
   c. TOTP
13. If an independent remote control system like e.g. Axeda is used, this needs to be described and approved by UZ Brussel. UZ Brussel must always know who logged on to the systems.
14. UZ Brussel makes a clear distinction between installation/support accounts and service accounts.
   a. An account shall be provided for the installation and support of the application(s) – it shall be disabled after installation. This account may not be used to run a service, make a database connection, or to mount a file share.
   b. A service account shall be created in case a service needs domain credentials instead of the default system account.
   c. It should not be possible to view service account passwords in clear text in configuration files.
      i. It shall be clearly indicated where these service accounts shall be used (registry, configuration files, etc.).
15. GUI-based executables shall not be used on the servers during the operational phase (processes that cannot be started as a service). All applications that do not require administrator rights to perform their functions, shall be run as services.
   If domain services accounts are required, only those created by UZ Brussel shall be used. The as-built documentation must contain a description of the rights of these service accounts.
   a. It shall be preferable to use a Group Managed Service Account with a password that is managed by AD.
   b. If a (g)MSA account cannot be used, this must be justified.
16. By default, Internet access from operational servers or communication with specific public addresses on the Internet shall not be permissible. If in the opinion of the supplier, this is indispensable for his application, he shall state this. In such case, an exception shall be made to this rule, in which case we shall expect the following from the supplier:
   a. For traffic to the Internet: A proposal for detailed configuration of our firewall (both windows firewall and network firewall).
   b. With regard to applications that must be available from outside: the details required to make this possible in a controlled manner (URLs, IP addresses, ports, protocols, etc.)
17. All resources, services and all server operating systems shall be monitored via MonitorNow.
   In the design document, the contractor shall specify which services and URLs are important
for his application, as well as the thresholds to be measured, and the relationship between
the different services and the user experience.
18. All the required certificates shall be signed internally by the UZ Brussel certificate authority.
19. UZ Brussel has its own Certificate Authority (CA) which is automatically trusted by every
device in the domain. Mobile devices managed through Mobile Iron must also trust this CA.
Certificates from the UZ Brussel CA must be used except where a public certificate is
required – if so, we will provide this via an external CA (Commodo).
20. It shall be preferable to use Kerberos authentication and not NTLMv2.
21. Apart from as-built documentation, the supplier shall also provide a clear diagram showing
the location of the server components and information flows and dependencies.
22. A short operational procedure must also be provided to enable a quick check on system
availability after patching/rebooting of the server.
23. CommVault shall be used as a backup solution. For virtual servers, three snapshots (6 a.m.,
noon, and 6 p.m.) per day shall be provided by default where an application is consistently
backed up, which means that the application must be able to process a quiesce during the
snapshot. If the application cannot handle this, this must be specified.
24. HTTPS must be used when using web servers. UZ Brussel can provide a certificate from the
internal CA or, if necessary, from an external CA.
   a. In this connection, we shall expect the supplier to provide a subject and SAN (Subject
      Alternative Name) name, and to state the purpose for which the certificate is used
      (server authentication and/or client authentication or other).
25. Unsafe protocols such as HTTP, ftp, telnet, etc. must not be used.
26. It shall be preferable to always store application data on a NAS location outside the VM, in
order to prevent the latter from inflating to an excessive size. UZ Brussel has a high
availability storage platform (Netapp MetroCluster) in which this data can be stored. This
approach shall prevent VMDK disks from becoming disproportionately large, and also that
the storage can be expanded quickly and efficiently. A separate retention policy for backup
can then be applied for applicative data.
27. No local shares may be created on windows servers without the knowledge of UZ Brussel. UZ
Brussel shall create the same wherever required, in order to ensure that the necessary AD
groups can be created and NTFS permissions can be set.
28. LDAPS must be used to connect to Active Directory (not LDAP).
29. UZ Brussel uses Exchange2016 (on premise installation) for email. By default, no client or
server can conduct mail correspondence without authentication. Outgoing mail to the
Internet is limited to mail addresses with suffix @uzbrussel.be. Other domain names shall be
filtered by the mail gateway. If mail correspondence is necessary for the application, there
should be two options:
   a. Authenticated
      i. Via AD credentials
      ii. Mail addresses must be specified
   b. Non-authenticated
      i. The IP address is added in an ACL on the load balancer
      ii. No monitoring of mail address
30. If it is necessary to use nVidia GPU cards, this must be stated. The type of licence for nVidia
Grid, as well as the desired profile must both be notified.

A number of servers offer specific functions. UZ Brussel strongly encourages consolidation. In this
case, the following shall apply:
- Communication server (HL7 based messages)
  All communication of the contractor’s solution with the central systems shall be via HL7 or, in exceptional cases, through a different agreed protocol. Mirth shall facilitate this communication within UZ Brussel.
  Either the contractor shall provide socket-based communication with Mirth (preferred), or a share shall be provided on the central storage platform, or one or two shares shall be defined on (one of) the server component(s) of the application, for in- and outbound file-based communication.

- Database server
  The IT department only supports Microsoft SQL Server and SAP ASE. The IT department shall provide the contractor with one or more databases on its central SQL 2012 or SQL 2016 database (AlwaysOn Availability Group) cluster, and shall assume responsibility for licensing, for installing the database (SQL script to be provided by the contractor), as well as for the availability and for the backup and restore of the environment.
  All report services and other database activities (SSIS, SSAS, SSRS, ETL, etc.) if any shall be performed via another server.
  The contractor shall provide the right contacts for all installation and troubleshooting operations if any required.
  We shall expect a timely and efficient response from the contractor in case DBA analyses reveal that certain queries and the performance of the system.
  No sysadmin rights on the central MS SQL cluster shall be granted to the supplier.
  The supplier shall install and maintain any other databases that may be needed. The supplier shall also be solely responsible for regularly updating/patching (security patches) the database software.
  The supplier shall provide the licence for this database. The supplier must take into account the fact that this database server runs on a VMware virtual platform, which may have licensing implications.
  The supplier must provide backup (scripts), and backups must be stored on a NAS location outside the server. UZ Brussel shall provide the aforementioned NAS location.
  Communication between application and database servers must be encrypted with at least TLS1.2 or higher.

- Load balancer
  In order to make a solution fully tolerant and highly available, UZ Brussel offers its F5 Hardware load balancer for such applications that are compatible with the same. An NGINX software load balancer may also be used.

- File server
  UZ Brussel has central file server systems (8 node Netapp Metro cluster) and long-term file storage on archive (CommVault). Data can be maintained for up to a year on a tier2 disk array and tape is provided for longer-term storage. All file serving / NAS needs must be provided on these already existing systems.

- Backup / restore
  a. 3 snapshots shall be provided each day for each virtual server managed by UZ Brussel, at 6 a.m., noon, and 6 p.m.
These must be default application consistent (the application must not have problems with a quiesce) or crash consistent, wherever required. The choice must be specified by the supplier.

b. UZ Brussel shall install a CommVault agent for physical servers. The IT department shall expect the as-built documentation to contain a list of the folders that must be included in the backup.

c. The IT department shall provide full backup and restore for databases – provided the same are supported (see above). Transaction backups shall be provided every half hour in case of MSSQL. If other DB systems are used anyway, the section on databases earlier on in this document shall be deleted and the supplier shall be responsible for the installation, backup and support. In such cases, the IT department will only provide a file-based backup of a database export provided by the supplier.

4.4.2 Exceptions and alternatives to server standards

Client standards may limit the usability of some solutions – in a manner not intended by the IT department. It is crucially important that in his tender, the contractor should explicitly mention the possibility of compatibility issues between his aforementioned standards and the components he needs to use in his solution. Alternative standards can then be sought in consultation with the IT department.

Depending on the contractor's problems with these standards, the following alternatives may be provided after close consultations:

- If for a reason for which sufficient justification is provided, a contractor supplies server hardware, the IT department shall always be responsible for the installation and placement of the same on the domain, and conformity with the following IT guidelines shall be ensured.
- The server shall be removed from the domain in a separate network (VLAN) and placed behind a firewall.

In addition, the contractor shall also be expected to provide a complete overview of the communication of the server(s) and the other IT components of the solution, at the IP address and port (which may be entered later).

5. Protection

- Traceability.
  Data changes in the system and/or on the equipment shall be logged. Thus it shall be possible at all times to find out what happened, when, and who made the change.

- Equipment
  The equipment shall be protected against unauthorised installation of device-foreign software by UZ Brussel.

- Security breaches in hardware and software
  - The contractor undertakes to notify UZ Brussel of such breaches as soon as possible

- Only encrypted connections shall be used. Thus HTTPS will be used and not HTTP, Idaps and not Idap, etc. If not, the supplier must state this fact.

- The software and runtime environments (java, .Net, python, etc.) provided by the supplier must be free of known security issues as described in CVE entries. Only supported versions of applications and runtime environments shall be accepted. The supplier shall be expected to provide a description of the version and ongoing warranty/support for each software...
component. The supplier shall also be responsible to keep all software components up to date. UZ Brussel has a vulnerability scanner tool that will verify this.

- Errors and error detection
  The system shall include means for the detection and correction of errors in the input, processing, export and dissemination of data.
  The system shall include means for verifying the completeness, accuracy and authenticity of the internal and external dissemination of the data.
  The system shall comply with the guidelines in force at the time of use by the government for, among other things, securing the information data.
  The logging of the activities mentioned above shall be maintained and UZ Brussel must be able to consult this logging without interacting with the contractor.

- Authentication and authorisation
  - Passwords shall preferably not be kept within the application itself. If this is the case, they must be salted and hashed.
  - Kerberos authentication shall be preferred over NTLM authentication.
  - Each user shall have his unique login/password combination; no generic accounts shall be permitted. Authentication within the application shall preferably be integrated into the Microsoft Active Directory environment of UZ Brussel.
  - Authorisation options within the offered product must be clearly indicated. Within a multi-user application, the functional administrator shall be able to systematically record the authorisation levels of the (type of) users and provide the management with information in the form of reports.
    A distinction shall at least be made with regard to rights for reading, adding, modifying and deleting data.
    Ideally, it should be possible to relate the (types of) users to a Microsoft Active Directory group.
    User management should be automated via Active Directory to the maximum extent, without the need for manual intervention when creating, modifying or stopping users.
    The nomenclature shall be agreed in advance with the IT department.
  - When logging on to the application, a secure connection to Active Directory shall be established, querying AD whether the user in question has access, at what level, and whether his specified password is correct. If this is not possible, this must be explicitly stated in the design documentation.
  - Passwords for administration purposes used in the applications must be defined to UZ Brussel (non-AD based accounts).
  - Installations shall preferably be carried out onsite with a UZ Brussel system engineer who shall supervise the installation.
  - Upon delivery, the installation shall be checked with a system engineer from UZ Brussel, to verify compliance with all applicable guidelines. This shall serve, or be capable of serving, as a basic knowledge transfer.
  - Within a multi-user application, authentication must always take place at the start-up of the application. We offer Single-Sign-On for our users via Imprivata. Integration with SSO shall be preferred. Users shall authenticate themselves via their personnel badge.