Medicoteknik
Region Syddanmark

IT STANDARD TERMS & CONDITIONS

These terms and conditions shall apply when the Region of Southern Denmark (the Customer) purchases medtech equipment with our without an associated IT system from a given supplier (Supplier).

Parts of the below terms and conditions may be omitted if the features are not included in the Solution on offer.

Definitions:
The Customer is defined as the Region of Southern Denmark.
The Supplier is defined as the offeror/bidder with whom an agreement is made.
The Solution is defined as the product offered by the Supplier. This may be independent medtech equipment, special computers, servers and/or client and server software.

1. GENERAL TERMS

The Solution shall use public and/or international standards (e.g. DICOM, HL7).

The Solution's user interfaces and API shall support character sets according to the UTF8 standard or equivalent; and all Danish special characters– such as æ-ø-å and Danish comma and thousand separator shall be supported. Furthermore, the Solution shall be able to handle Danish social security numbers (CPR No.) with and without hyphens.

It is a requirement that there is a non-disclosure agreement and possibly a data processing agreement based on the Region of Southern Denmark's standard template. The non-disclosure agreement and the optional data processing agreement must be signed before the order/contract is accepted.

2. COMMUNICATION

Modalities and workstations for imaging diagnostics shall as a minimum support the communication protocol DICOM version 3.0 for the exchange of information with other diagnostic imaging equipment, e.g. RIS, PACS, film printers, workstations etc.

The Supplier shall be able to present a DICOM Conformance Statement, which fully describes the DICOM implementation included in the Solution. The Conformance Statement shall fully comply with the guidelines for conformance claims described in the DICOM standard. If any of the described DICOM functionality is provided as an option, it must be clearly stated as an option.

Data communication via HL7 or a similar standard protocol is a requirement.

3. DATA COLLECTION FROM MEDTECH EQUIPMENT

The Region of Southern Denmark has a central platform for collecting patient and device data from medtech devices called MDIC. If the Solution can export patient or device data, the Supplier shall, upon request by the Customer, provide the API and documentation to the Region of Southern Denmark and the MDIC supplier, enabling transfer of patient and device data directly from the Solution to the MDIC platform.

4. SECURITY & ANTIVIRUS

The Solution shall at all times comply with Danish legislation, including the health sector, the Danish Data Protection Act, and GDPR (The General Data Protection Regulation).

The Supplier must be prepared to adapt the Solution to the current legislation. Adjustments are handled according to the change management provisions of the contract.

On a regular basis, the Customer scans Servers, clients, and medical devices for IT vulnerabilities. The Supplier is obliged to:
- continuously approve and release security patches for operating systems in the Solution within one month of release from the OS manufacturer (e.g. Microsoft).
- continuously develop, approve and release security patches for firmware and software in the Solution within 3 months after the request of the Customer.

Servers and clients in the Solution shall be protected by TrendMicro Antivirus or similar via an installed agent. Servers shall as a minimum be monitored using Chef and Zabbix agent. Clients shall be configured to install critical Windows updates.

The Solution shall comply with the Danish common regional information security policy, called **Fællesregional informationssikkerhedspolitik**.
https://www.regionsyddanmark.dk/dwn662754

5. NETWORK AND PDS WIRING

The Solution shall be implemented directly in the network infrastructure of the Region of Southern Denmark and shall use IP addresses from here. The solution may only contain router/firewall solutions for routing between the Region's network and the Solution if a special agreement has been made.

The Solution shall apply TCP/IPv4 communication between servers, clients and devices.

If the Solution is using multicast, a solution proposal must be prepared in collaboration with the Region of Southern Denmark, Regional IT.

The solution shall be fully operational on the Customer's existing WAN/MPLS network.

The Solution shall use NTP time synchronization via lookup in the Region/Hospital NTP Service.

The Solution shall apply DNS for name lookup.

The MAC address(es) of the Solution for wired or WIFI networks shall be stated when installed for the Customer.

The Solution connects to medico networks without Internet access. When Internet access is needed, destinations must be specified (IP, URL, ports.)

The Solution's host name(s)/computer name(s) must be provided by the Customer at the installation according to the following standard: "*MT*[*device number*]".

This requires that workstations and equipment included in the Solution shall use existing Medico network VLAN and CISCO switches**.**

Regarding the use of RJ45 on a wired network, the Solution shall be equipped with a Standard Ethernet Interface supporting 10/100 or 10/100/1000 Mbit/s.

Patch cables for wired networks shall be category CAT6a STP/FTP or CAT6 UTP and shall be green and of the type LSZH halogen free.

A diagram of the system layout (draft format accepted) must be submitted at least five working days before connection to the network, which describes all of the system's network components, including server connections, remote support, firewalls, etc.

6. WIFI

Regarding the wireless connection, the Solution shall use the Customer's existing Medico WI-FI network WLAN and CISCO Access Point.

The Solution shall be configured with dynamic channel change of 2.4Ghz and 5Ghz. Fixed channel selection requires a special agreement with the Customer.

Regarding WI-FI, the Solution shall support 802.1x authentication key with the validation type PEAP-MS-CHAPv2. User and password is provided by the Customer at the installation.

The Solution shall support WPA2/AES encryption.

The Solution shall support 802.11a/g/n at 2.4GHz and/or 802.11n/ac 5 GHz WLAN technologies.

The solution shall use the Customer's SSID for wireless connections to the Medico network.

7. REMOTE ACCESS

This requires that the Supplier can access the Solution located in the hospital network via a connection to the hospital network. The connection shall comply with the following as requested and accepted by the Region of Southern Denmark:
- an external VPN user access to the Region of Southern Denmark or
- a VPN Site-to-Site connection.

This requires that the Supplier's service access to the hospital network will be via the Region's firewall. The service connection must therefore be able to support the restrictions that a firewall may impose on it.

Remote support tools shall include logging and two-factor authentication and be approved by the Customer.

8. SERVERS AND DATABASE

Servers shall be able to run in the Customer's existing IT environment throughout the contract period.

As a starting point, servers must run as virtual servers in the Customer's VMware environment. If there are circumstances which make it impossible/not appropriate to run the server as a virtual server, a physical server can be used.

Application servers and database servers shall be installed and operated in one of the Region's IT operations centers.

Physical servers must be delivered as rack-mounted servers with full redundancy (mirrored disks, dual power supply, paired network card with two failover connections.) The Customer uses servers from DELL**.**

Servers must support Windows 2012 R2 Datacenter; Windows 2016/2019 Datacenter 64 bit or Linux Ubuntu 16.04 and 18.04 including CentOS 6.7.

SQL databases shall as a minimum support MS SQL Server 2012 SP4. The Customer uses Microsoft SQL hotel with MS SQL Server 2012SP4, 2014, 2016 or 2017.

OS drives for the operating system must not be used for installation of applications or as storage for application data. This shall be located on another drive, alternatively a CIFS/DFS share.

The Supplier undertakes to enclose a diagram of the servers and databases included in the Solution (e.g. Visio diagrams) to provide an overview of the operating interfaces, dependencies, integrations and components used in the solution description.

The solution description must include the following information as a minimum:
- Minimum RAM and CPU requirements for all servers included in the Solution.
- The physical implementation, i.e. how many physical or virtual servers to use.
- A list of all software products and any additional components and third party products described by product name, any minimum version and recommended version, etc.
- Requirements for the type of database, and a description of how the database is used.
- Devices to backup so that the Solution can restore/recover data after a disaster.

9. STORAGE, BACKUP AND RESTORE

This requires that the Supplier specifies the need for storage (disk space) for the operation of the Solution, divided into, e.g. operating system, basic software, data, etc., where applicable. The specification shall include the storage needs in the initial situation as well as the expected development of the need when usage of the Solution increases.

This requires that the Solution utilizes the Region's SAN installation for permanent data storage, i.e. no internal disk space on servers or stand alone dedicated disk systems.

This requires that the Supplier describes proposals for backup routines and policies.

This requires that the Supplier clarifies how the backup process will affect the accessibility of the Solution.

10. SOFTWARE & APPLICATIONS

Browser solutions must as a minimum support Internet Explorer v.11, Firefox v.67, or Google Chrome v.75 or later.

This requires that applications in the Solution shall be able to run on the supported operating system. The Customer uses Windows 10 Enterprise SAC 64 bit, but updates continuously as Microsoft releases new builds.

Platform products and operating systems, databases, browsers and other third party products used by the Solution shall follow the development so that the Customer is not tied to "end of life" products and operating systems.

If the Solution uses third party programs, the Solution must at all times be able to handle that these programs are updated to the latest version. For example: Java or Acrobat Reader.

11. LOGGING

The Solution shall be able to perform transaction logging of relevant events, including user events, events from other subsystems in accordance with applicable laws and regulations. This means that there must be full traceability of all transactions and registrations.

This requires compliance with the Security Order of the Danish Data Protection Agency. Machine registration (logging) of all use of personal data shall be provided. As a minimum, the registration shall include information about time, user, type of use and state the person who the information relates to or the search criteria used. The log shall be stored for 6 months and can be deleted after this period. Authorities with a special need can keep the log for up to 5 years. See link https://www.retsinformation.dk/Forms/R0710.aspx?id=1002

12. ACCESS CONTROL

This requires that the IT systems of the Solution shall require username and personal password, where there is access to patient data. Login information shall be stored in a log file and shall as a minimum contain username, date and time.

User access to the Solution shall be differentiable so that different users/user groups can have rights to different parts of the Solution and different rights within each section (query, add, edit/change, delete, etc.)

The default user login and password shall be changed to a minimum of 10 characters consisting of lowercase and uppercase letters and numbers.

User management on clients with user ID/password authentication shall be provided via. the Region of Southern Denmark's AD (Microsoft Active Directory) with LDAP.

If user login supports Single Sign On (SSO), user ID and password authentication must be provided via. the Region of Southern Denmark's AD (Microsoft Active Directory). The Region of Southern Denmark's AD (Microsoft Active Directory)

13. CHANGE

The Supplier is responsible for and must manage the Change process as well as use the Customer's Change Management tool when changes are made to the Solution.

The Supplier shall document all system dependencies and integrations both in writing and in system architecture drawing(s).

The Supplier shall, in collaboration with the Customer, prepare system documentation of the Supplier's and the Customer's areas of responsibility for operations. It is a requirement that this includes a design drawing.