Customization Agreement

Treatment Planning for Radiation Therapy at Oslo University Hospital Trust (OUS)

Case # 2018/1216

Government Standard Terms and Conditions

for IT-procurement SSA – T

T Appendix 3a Customer's technological platform

Version 1.0, July 2019

Oslo University Hospital HF

Description of Customer's technological platform

Contents

1 Introduction

This document describes the ICT platform established at Oslo University Hospital HF (the "Customer") on an overarching level. Sykehuspartner HF is the Customer's service provider, and is responsible for the establishment, operation and management of the ICT platform, as well as many of the Customer's solutions established as part of the platform. The service provider's operations responsibilities include data centres established on premise at the Customer's location and common regional data centres established for the health enterprises in the South-Eastern Norway Regional Health Authority. The Customer has in addition some local operation and management units for ICT systems e.g. systems and medical technical devices that are closely connected to clinical use in laboratories and radiation therapy.

Suppliers are made aware that the ICT platform is continuously evolving and that changes and upgrades to the infrastructure may occur during the period of the agreement.

1.1 Green IT

The South-Eastern Norway Regional Health Authority wishes to promote sustainable use of IT and refers to Green IT guidelines (https://www.ikt-norge.no/bransjenormer-guider/gronn-it/) (in Norwegian only) for procurement, creation, operation and management of the ICT platform and solutions established as part of the ICT platform.

1.2 Lifecycle management

The South-Eastern Norway Regional Health Authority is concerned that solutions should be maintained and developed on an ongoing basis, so-called "Lifecycle Management". In normal circumstances, the current and previous versions of operating systems and software will be supported (n, n-1). For example, this applies to components and services:

- provided by the Customer's service provider, and not part of the delivery of the solution
- provided as part of the solution
- provided by a third party

The solution must therefore be continually updated and maintained to accommodate this principle. Note that this also means that the solution must support ongoing patching and upgrades to the Customer's technical platform.

2 Architectural principles

The South-Eastern Norway Regional Health Authority considers certain properties to be important for all solutions to be introduced. These properties are architectural principles, and are described in detail in the following documents (in Norwegian only):

- The DIFI (Agency for Public Management and eGovernment) guidelines, "Overarching architectural principles for the public sector"

- DIFI's "Architectural principles for interaction"
- The National ICT guidelines "Architectural Principles in specialist health services»

3 Data centres

The Customer has two main locations, each containing two separate geo-redundant data centres (SHKR):

- OUS Rikshospitalet: SHKR1 and SHKR2
- OUS Ullevål Hospital: SHKR3 and SHKR4

Two shared regional data centres (SDS) have been established within the South-Eastern Norway Regional Health Authority:

- SDS1 located at Digiplex
- SDS3 located at Basefarm

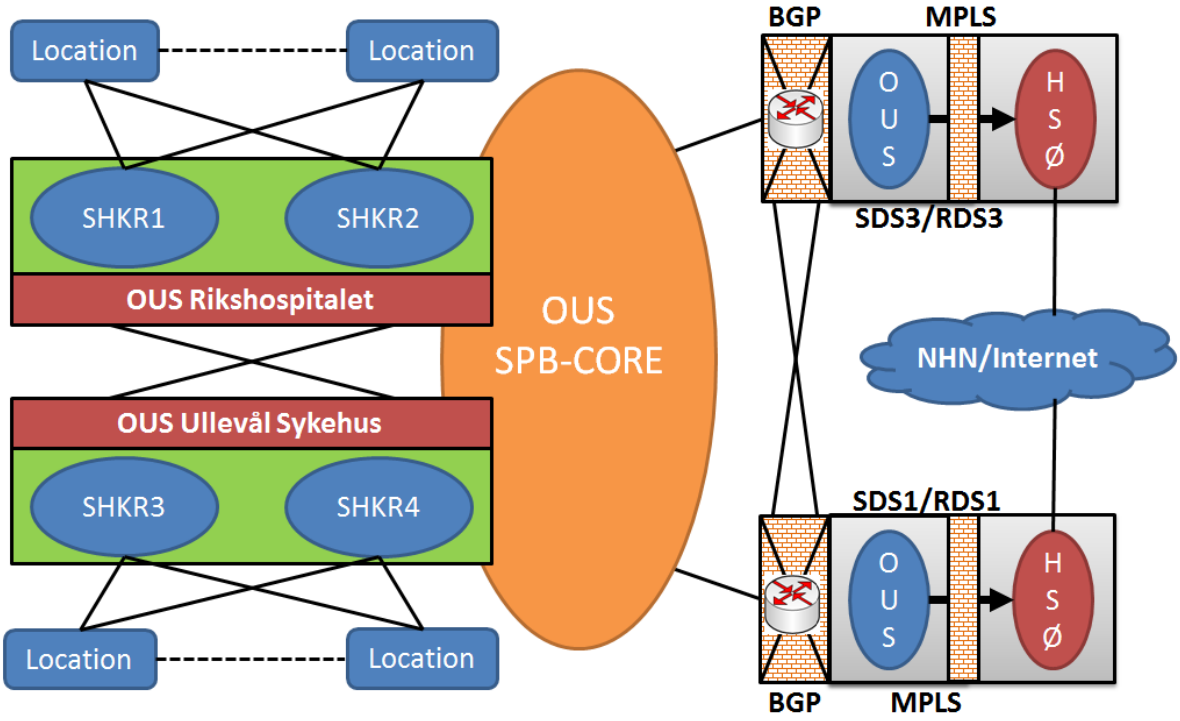

FIGURE 1 - OVERALL TOPOLOGY VIEW

In addition, an external data centre has been established for disaster recovery (cold backup), SDS2 at Akershus university hospital HF (Ahus).

The Customer's local data centres are connected to the common regional data centres as illustrated below:

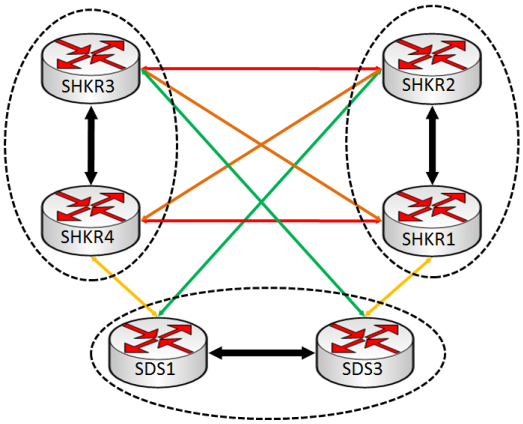

FIGURE 2 -SHKR AND SDS FIBRE LINKS

4 Network infrastructure

4.1 Overarching

The Customer's network has been built up with network elements from Extreme Networks (formerly Avaya). There is extensive use of Shortest Path Bridging (SPB) in the network. SPB allows any VLAN to be migrated to any other part of the network as an L2VSN (L2 Virtual Service Network) without having to reconfigure all the nodes in the network.

Fabric Attach and Fabric Connect are also used in the Customer's network to automate network configuration, for both wireless and wired networks.

The shared regional data centres (SDS) utilise network elements from Cisco and the use of MPLS. This means that communication between the Customer's network and HSØ is based on IPv4 and not Layer 2.

4.2 Firewalls

Standardised Cisco firewalls are used internally, while Palo Alto firewalls are used for the connection to the Internet. The Cisco firewalls are configured with a TCP idle timeout of two hours on the Customer's network, and an idle timeout of 1 hour in the shared regional data centres.

4.3 Access control

IEEE 802.1X EAP-TLS is used for all the wired and wireless networks on the customer site. For equipment that does not support IEEE 802.1 X, MAC authentication is used to assign the correct VLAN. Devices that fail authentication are currently placed in the guest network, but a quarantine zone is currently being established. Use of EAP-TLS authentication with machine certificates is currently only used for standardised PC clients located in the same VLAN. This solution is currently undergoing change so as to be able to move machines into separate VLANs based on X.509 OU.

CRL checking and VLAN allocation is performed by an Avaya IDE RADIUS. DNS machine names are also looked up in AD using LDAP via the same RADIUS.

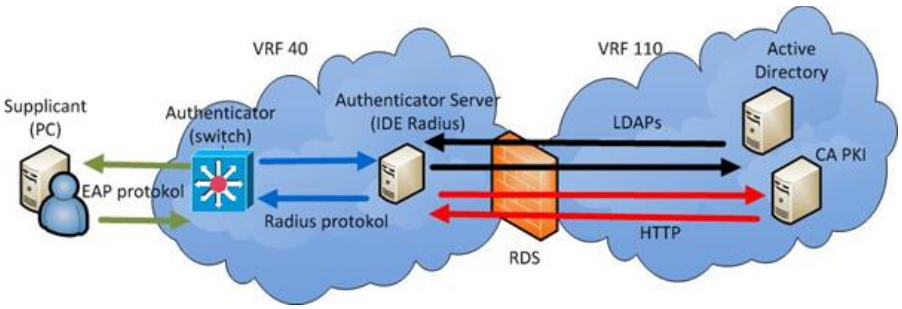

FIGURE 3 - OVERARCHING DATA FLOW 802.1X

4.4 Load balancing

Alteon is used for load balancing in the Customer's local data centres (SHKR), while F5 BigIP is used in the shared regional data centres (SDS).

4.5 Wireless network

The Customer's wireless network consists of wireless access points from Extreme Networks. The same security principles and security mechanisms introduced for wired networks have also been established for wireless networks.

The following SSID and associated networks are in existence:

SSID	Description	Authentication
Internal OUS	Internal OUS network for administrative and clinical services	IEEE802.1X/EAP-TLS + AD
HelseSorOst	Guest network for patients and relatives	None, but captive portal with user authentication is being established
Eduroam	World-wide network for academic and research related activities	Authentication takes place via Eduroam and depends on the user's affiliation with an organisation involved in the Eduroam collaboration

4.6 Regional WAN aggregation central

All remote network connections, including VPN-based remote access for employees and suppliers, terminate in the regional WAN aggregation central. The Regional WAN aggregation central is part of the core infrastructure provided by the Customer's service provider.

Only IPv4 traffic is possible between the WAN aggregation central and the Customer's network.

5 PC clients

5.1 Standard PC clients

Windows 7 64-bit is currently used as the operating system for standard PC clients, but a process is underway to upgrade standard PC clients to Windows 10, to be completed Q1 2020. Users are not permitted to be local administrators, and only authorised software can be run on the clients.

The standard PC client uses a local Windows firewall, as well as System Center Endpoint Protection (SCEP) for antivirus/anti-malware. Client-to-client traffic is not permitted.

Peripherals, such as optical drives or USB storage, which are identified by Windows as storage devices, are blocked by default. Encrypted USB storage devices from IronKey are permitted, provided that they are ordered through and managed by the Customer's service provider. All laptop PC clients are encrypted with BitLocker Drive Encryption.

5.2 Medical device client

A medical device (MD) client is defined as a client that is initially "single-purpose" and is used for dedicated tasks related to MD, such as:

- monitoring or managing a medical device
- running medical device-related client applications for the processing of data where the medical device is the data source
- pre-processing of data to be used by medical devices

Windows 7 is used as standard (English Windows 7 Enterprise, 64-bit edition with SP 1, with the option of a Norwegian language pack). The use of Windows 10 is currently being planned. MD clients cannot be used primarily for office administrative tasks, but a Citrix workspace can be accessed that allows the user to access administrative and professional clinical systems.

MD clients are based in their own MD client zones in accordance with the zone model set up on the Customer's network, and may have reduced or changed functionality to the OUS Standard client with respect to:

- Antivirus
- Security patching
- Local storage – including the storage of sensitive information
- Backup
- Client setups due to supplier software requirements, such as lack of support for RES and SCCM

- Extended or customised access and rights
- The functional user concept (common user, typically user sessions spanning multiple shifts or required due to work processes)
- Screensavers and automatic locking
- Management:
    - remote access for Customer employees with responsibility for MD operations and management
    - remote access for MD suppliers
- Internet access

Three variants of the Windows 7 MD client are primarily used:

- MD Standard – based on the Customer's standard Windows 7 PC client, but with certain options for simple customisation in terms of security, operations and management. This is the preferred MD client type.
- MD GPO – This client type is used if one or more of the SCCM, RES and SCEP services are unavailable/should not be used. Instead, the client is hardened with a set of GPOs and is remotely managed where possible.
- MD Clean – This is a stand-alone client variant, which can not be a member of the domain and does not use GPO.

In order to protect MD clients with functional users (PCs permanently logged in using non-personal logins) against accidental disclosure, as well as to log user activity, an AD-controlled screen lock is being developed, which can be unlocked by all users identified as belonging to the correct AD group.

5.3 Functional users

The Customer has established a standardised concept for the management of shared users on operating systems, called "functional user".

The use of functional users on the operating system should preferably be avoided, and individual logins should be used to improve secure access, checks and traceability. For individual applications, however, it is appropriate to use a functional user, such as in the context of PC clients used for activities that overlap multiple work shifts.

A number of restrictions have been introduced for functional users:

- A functional user is associated with one specific PC client, and the PC client is set up with auto-login. The PC client cannot be used for individual logins when it has been set up with a functional user
- There is no Internet access
- There is no access to file storage
- There is no access to email

- It is a requirement that applications allowing access to personal data must be secured using individual logins to the central authentication solution (IAM or AD)
- File storage, email and applications can be accessed via a Citrix workspace, which requires individual user login.

5.4 Software deployment and patching

Microsoft System Center Configuration Manager is used for the administration, deployment, and patching of *locally-installed* software in MSI-format. Microsoft App-V is used for centrally-*streamed* applications. The programs are packaged in MSI/App-V format using AdminStudio. App-V is the preferred method of application deployment.

Applications to be deployed to multiple standard PC clients should normally be packaged by the Customer's service provider and distributed via approved deployment methods. All applications to be used must be "whitelisted" in RES One Suite.

5.5 Dynamic workspace

RES One Suite from Ivanti, in later versions the name Ivanti Workspace Control, (ivanti.com) is used to adapt and deliver workspaces arising from functional needs and the user's organisational access. This includes the availability and "whitelisting" of applications.

5.6 Internet access

Internet access is permitted from PC clients on port 80 and 443 (http/https) and URL filtering is used with external firewalls (Palo Alto). Internet Explorer 11 is standard browser, and locally-installed Java runtime is not permitted.

With the introduction of Windows 10, Microsoft Edge will be the default browser. Google Chrome will be introduced as a secondary web browser on Windows 7 and will be continued on Windows 10.

5.7 Printing

The centralised print solution is based on Canon Uniflow Pull print/follow-me print, multifunction printers based in central locations are primarily used.

For requirements not covered by the centralised printing solution, such as label printers and specialist printers, these can be established locally. A risk assessment should be carried out.

5.8 AD structure

OUS utilises one common domain for all new services: ous-hf.no

There are still other domains in use, but these are being phased out and must not be used when setting up new services.

5.9 Central Driver Store

Standard PC clients are not permitted to download or install drivers from the Internet. All approved and updated drivers must be made available in the locally-established Central Driver Store.

5.10 Remote access for employees (always-on VPN)

Big-IP Access Policy Manager, along with Big-IP Edge Client are used in the remote access solution for employees of the Customer. Access is authenticated using the "ID-porten" service (provided by Difi, the Agency for Public Management and eGovernment) at security level 4, providing access to the Customer network from laptop clients. In addition, users can log into virtual work surfaces based on Citrix terminal access.

The principle behind VPN access is that a PC client is automatically connected to the Customer's network via VPN (so called "always-on") and is always subject to the same security provision for network access regardless of where in the world the user is located. This also means that Internet access is always regulated via the outer firewall (Palo Alto).

BYOD devices are not permitted on the Customer's network, apart from on the wireless Guest network.

6 Servers

Servers are mainly run as virtual machines under VMware. The preferred operating system for new servers is:

- Windows server 2019 and Windows Server 2016
- Redhat Enterprise Linux (RHEL) 7.5

Other operating system versions are still in use, but these will gradually be migrated to the last supported version or phased out. It is not desirable for new solutions to be based on older operating system versions, or other operating systems.

7 Database platform

The following database platforms are supported:

- Microsoft SQL Server 2016, including Always-On cluster
- Oracle 12, including Maximum Availability Architecture (MAA)

8 Storage, backup and archiving

8.1 Storage

Storage capacity is available both at a local data centre (SHKR) and the shared regional data centre (SDS). Both NAS and SAN based storage are used.

8.2 Backup

Symantec NetBackup is used for all backups.

Two regional backup environments have been set up in SDS1 and SDS3, while SDS2 is used for replication.

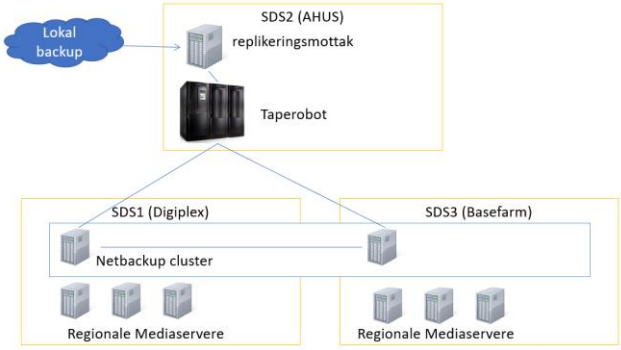

FIGURE 4 -BACKUP AND REPLICATION AT SDS

Backups are normally set to run outside of normal working hours (between 17:00 and 05:00), with the bulk of jobs taking place after midnight. In exceptional circumstances, jobs can be set up to run during the daytime, providing the requirements are documented.

Different levels of backup have been defined (gold, silver and bronze). The different levels will normally reflect the criticality of the service.

The backup status of both the regional and local backup environments is monitored daily via NetBackup OpsCenter.

8.3 Archiving

The archiving of little-used or historical data can be ordered as an option.

9 Operations and management

9.1 Overarching

The Customer's service provider is responsible for the operation and management of the customer's technical platform and is normally responsible for the operation and management of solutions established in the platform. It is important for the Supplier to adhere to the technical solutions established on the Customer's technical platform as well as existing routines, within the operation and management of solutions established on the Customer's technical platform.

There is also the option to apply the "shared management" principle, where the Customer's service provider can provide everything from Network as a Service up to Software as a

Service. Operations and/or application management for a service delivery (client/server/devices/applications) can thus be performed by an external supplier.

Typical examples of shared management are solutions for medical devices (MD), building automation (BA) and other technical administrative devices (TD), where the Customer's service provider manages the Customer's technological platform to the desired level, while the Customer manages the system solution. A dedicated server zone model for solutions using shared management is being established. It ensures the necessary separation and access control in relation to solutions that are hosted and managed entirely by the Customer's service provider.

Operation and management must not be carried out via direct access. Instead, a compulsory management solution has been set up based on Citrix XenDesktop, ensuring access control as well as necessary traceability and the logging of activities. In addition, there is a VPN portal for external suppliers which requires two-factor authentication when attempting to log in.

Furthermore, the Customer has a standardised managed file transfer service (MFT service) for the controlled and secure transmission of authorised data between the Customer and the Supplier.

The Customer's service provider has established fixed freeze periods, where there is strict regulation of the changes that can be made to the infrastructure or to established solutions. In the event of larger operational events within the Customer's platform, temporary freeze periods may be established.

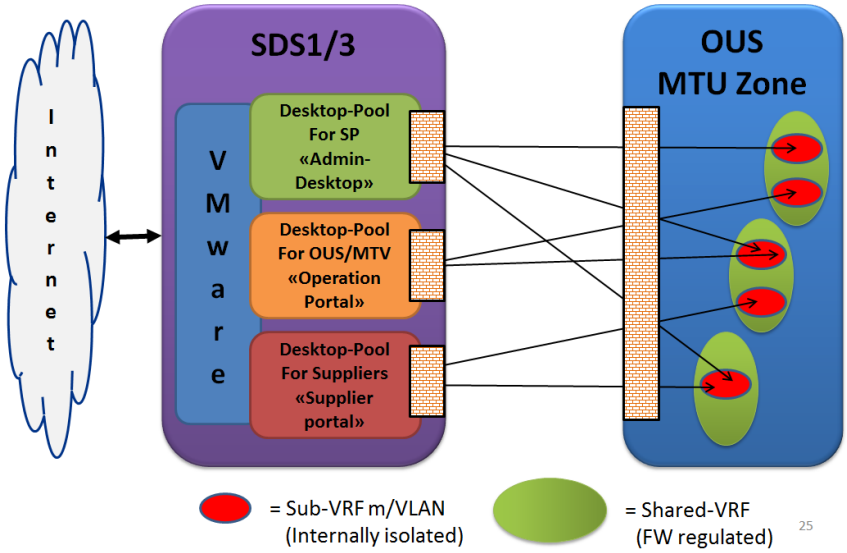

FIGURE 5 - MD MANAGEMENT PRINCIPLE

9.2 Remote access for suppliers

The South-Eastern Norway Regional Health Authority has standardised remote access via solutions from F5 BigIP and Citrix terminal access for external suppliers. This is known as the "Supplier portal" and must be used for all supplier-specific operations and management where personal attendance on Customer premises is not expected.

In order to use this solution, the Supplier must be able to use the F5 BigIP Web plugin for SSL-VPN and the Citrix Receiver web client on PCs. A Supplier portal user must be registered with the Customer's personnel system, PAGA, and be assigned a personal user ID. The supplier will then have access to a Customer access server, where approved remote control applications (RDP, SSH, WinSCP, UltraVNC) are available. In the case of special needs, other software can be made available after approval by the Customer.

All use of the Supplier portal should be linked to named, identified users employed by the Supplier. A Supplier portal user ID will initially be disabled, and can only be enabled upon agreement with the Customer and/or Customer's service provider. Users can be enabled for up to 72 hours at a time for regular support needs. Longer periods (up to 6 months) can be granted e.g. when installing, testing and validating larger systems

Use of the Supplier portal requires the signing of a confidentiality statement and the entering into of a Data processor agreement between the Customer's service provider and Supplier.

9.3 Remote access for operations and management

The Customer's service provider will perform operations and management of the Customer's technological platform and solutions based on the platform via an "AdminDesktop" based on Citrix XenDesktop.

A separate "Management desktop" has been established for Customer employees responsible for the operation and/or management of internally-established solutions, such as MD and TD.

9.4 Monitoring

The Customer's service provider has established centralised solutions for the monitoring of the Customer's network infrastructure and ICT platform, as well as underlying components and services on the Customer's technological platform. Monitoring is performed via a number of agent-based and agent-less solutions on various components of the infrastructure, where alerts and alarms are aggregated and sent to Micro Focus Operations Bridge.

9.5 Logging

It is of central importance to both the Customer and the Customer's service provider that systems based on the Customer's technological platform can provide operational and

management-related logging functionality on multiple levels, such as in the event of errors or warnings connected with hardware, operating systems, services in the system, malfunctions and other alerts which may contribute to malfunctions being prevented, or the obtaining of information relevant to identifying the cause of the error.

The Customer's service provider has established a central logging system for the management of relevant system and security logs from Customer systems. The central logging system is based on Splunk.

10 Medical devices (MD), Building automation (BA) and Technical administrative devices (TD)

10.1 Zone model

A zone model has been established for use with MD, SA and TD solutions, which ensures security, traceability, and shared management requirements.

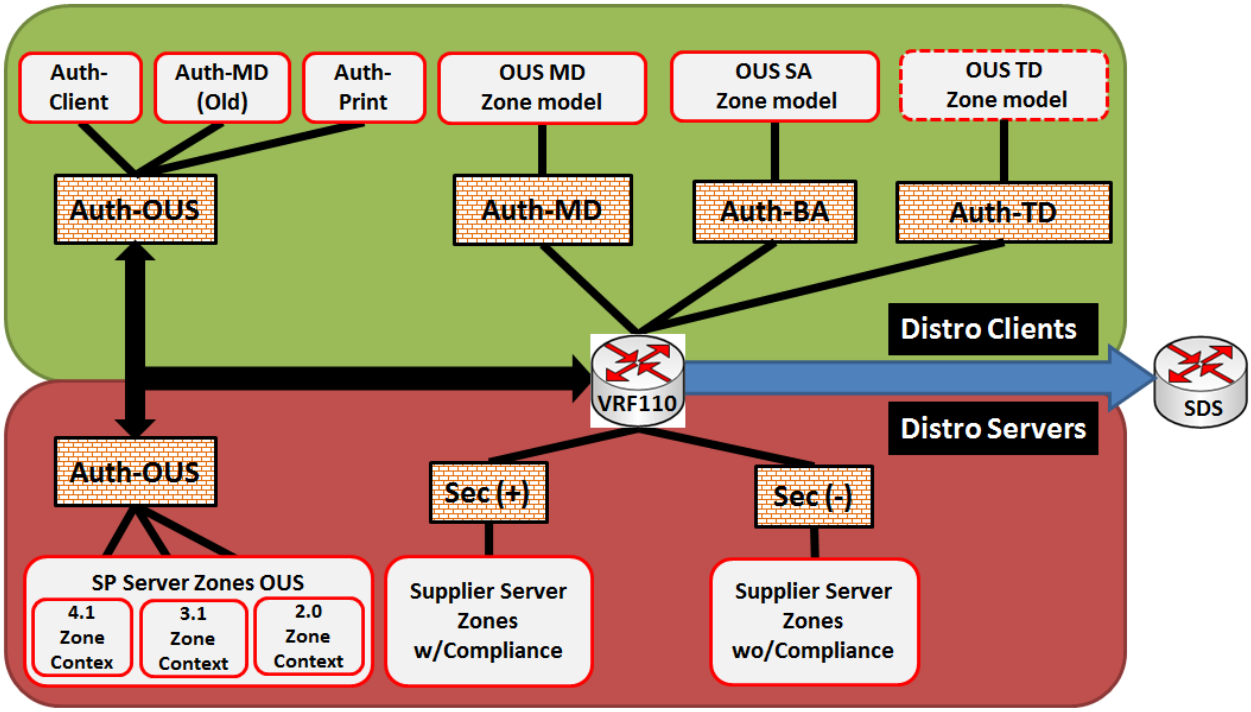

FIGURE 6 - ZONE DIVISION PRINCIPLE WITHIN AN SHKR

The zone model creates two levels, i.e. with main zones and sub zones within each individual main zone:

- Between the main zones (level 1, data traffic is regulated by firewall rules
- Between underlying zones under a main zone (level 2), "Black Hole Routing" is used as a local isolation mechanism to prevent traffic between the underlying zones.

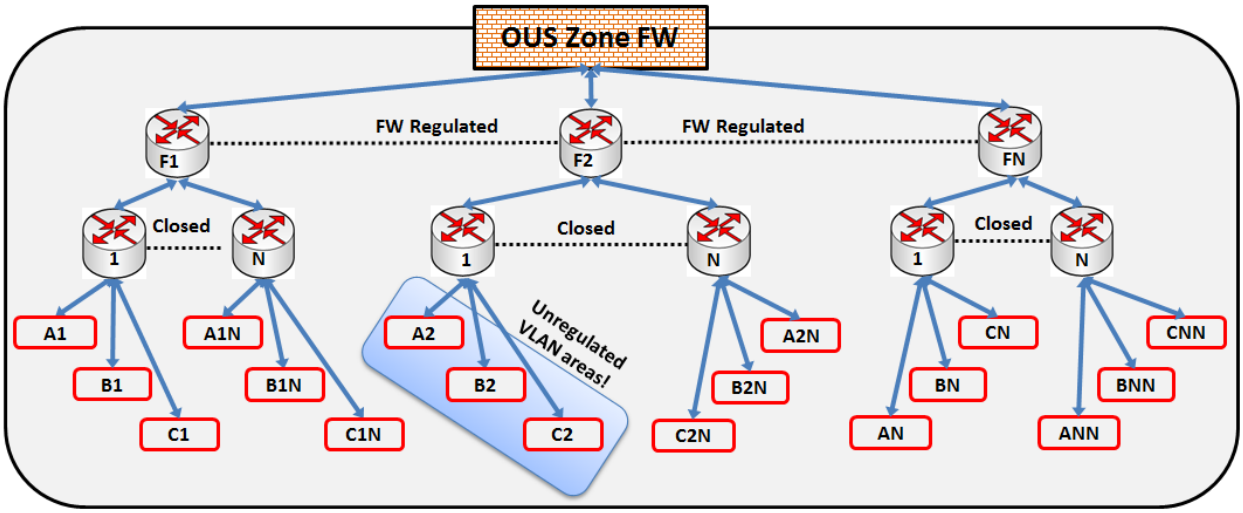

FIGURE 7 - ZONE SEPARATION PRINCIPLE

This means that in order to exchange data, components within a system solution must either be in:

- the same underlying zone, or
- in different underlying zones (in different main zones), where access is regulated via the firewall outside the main zones

If the established solution requires isolation from other solutions in the same underlying zone, the solution must have its own protection, for example by using an internal firewall or separate firewall appliance. This is a consequence of access regulation at VLAN level not being possible.

Exchange of data between solutions based in the zone model or with outside solutions must as far as possible be performed using the Regional integration platform or the managed file transfer service.

10.2 Medical Devices

Medical devices are defined as any instrument, apparatus, aid, material or any item used to diagnose, monitor, process or change a patient's anatomical or physiological processes.

There is a great deal of variation in medical device data communication methods. Certain equipment is directly connected to the network, while many medical device solutions consist of a PC client connected to instruments via USB, RS232, Firewire etc, or indirectly connected via Ethernet via conversion solutions from MOXA/Digiboks, etc.

OUS has established security principles and mechanisms to manage any deviations, as not all medical device solutions follows established data communication standards.

10.3 Building automation equipment (BA) and Technical devices (TD)

Building automation and Technical devices (e.g. parking systems, kiosk solutions etc.) are organized in separate network zones designed for the purpose and are managed according to the same principles as medical devices.

11 Licencing

For solutions with a licencing mechanism, it is preferred that licensing is set up centrally to ensure effective licence management. This means that:

- the use of physical licence dongles should be avoided, due the challenges this involves in a virtualised server environment
- the use of distributed licence files should avoided, due the challenges this involves in the maintenance of licence files and application packages the licence file may be part of

12 Information security and data protection

12.1 Overarching

The Customer is obliged to comply with Norwegian laws and regulation, and imposes strict requirements on compliance with relevant laws regarding information security in the procurement, establishment, operation, management and disposal of its systems. Information security is about ensuring that the information processed by the system:

- cannot be accessed by unauthorised persons (confidentiality)
- cannot be altered inadvertently or by unauthorised persons (integrity)
- is available on demand (accessibility)

A requirement is for the solution offered to satisfy the requirements of section 25 of the General Data Protection Regulation (GDPR) – Data protection by design and by default, see:

- The Data Protection Authority guidelines on Data Protection by Design and by Default - https://www.datatilsynet.no/en/regulations-and-tools/guidelines/data-protection-by-design-and-by-default/
- Data Protection Authority information about GDPR requirements on data protection by design and by default in the healthcare sector - https://www.datatilsynet.no/personvern-pa-ulike-omrader/forskning-helse-og-velferd/leverandorer-og-utviklere-i-helse--og-omsorgssektoren/ (in Norwegian)
- GDPR – Article 25, Data protection by design and by default - http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL

The Customer is required to comply with the Code of Conduct for information security from the Norwegian Directorate of eHealth, see:

- The "Code of conduct" Normen - https://ehelse.no/normen/documents-in-english https://ehelse.no/normen

To support the customer's commitments and information security requirements, the South-Eastern Norway Regional Health Authority has defined a set of information security requirements in the "Security framework management system". The set of requirements includes requirements for infrastructure, systems and service, as well as for suppliers and persons responsible for the operation and management of infrastructure, systems and services for the Customer, see also:

- https://www.helse-sorost.no/informasjonssikkerhet-og-personvern/ledelsessystem-for-informasjonssikkerhet

The supplier is expected to have incorporated these principles and ensure that they are complied with.

The Customer's service provider uses ISO 27001 as a standard for security management.

12.2 Risk management

Before the solution can be established, and in the event of any changes to the solution, an approved risk assessment must be completed and approved. The risk assessment is based on the final design of the solution, with all its components, services and configuration, as the establishment of the solution is planned for the Customer. This will normally be prepared by the Customer's service provider, in cooperation with the Customer and Supplier. Final approval of the risk assessment is done by the customer.

It is a goal for medical devices also to take ISO/IEC 80001 ("Risk Management of Medical Devices on a Network") into account.

12.3 Identity and access management

Identity and access management (IAM) within the South-Eastern Norway Regional Health Authority consists of a number of components and services, but the three most important services are the Regional Provisioning Service, the Regional Authentication Service and the Regional Authorisation Service. These services are completely dependent on, and thus integrated with, authoritative information sources and processes.

For a further description, see *Appendix 3C: Customer's technological platform – Identity and access management (in Norwegian only).*

13 Integration

To ensure that the technical infrastructure is built into the enterprise architecture with a focus on services, the South-Eastern Norway Regional Health Authority has established service-oriented architecture (SOA) for integrations with administrative and clinical systems.

The South-Eastern Norway Regional Health Authority has created its SOA by establishing a regional integration platform and an integration policy. The integration policy establishes clear requirements and guidelines on how integrations are to take place, and how they are to use the integration platform.

For a further description, see Appendix 3B: Customer's technological platform - Integration (In Norwegian only).

14 Abbreviations and terms

Abbreviation / Term	Description
AD	Active Directory – Microsoft's catalogue service for authentication and authorisation of users in a Windows domain
App-V	Microsoft applications virtualisation and streaming technology.
BA	Building automation, i.e. centralized control of a building's heating, ventilation and air conditioning, lighting etc
BYOD	Bring Your Own Device – privately owned PC clients, tablets or mobile phones that are not owned by or controlled by the customer.
CDS	Central Driver Store
CRL	Certificate Revocation List
The Customer	In this document, this is used as a term for the healthcare company Oslo University Hospital
Customer service provider	The company/organization that at any time is responsible for operation and administration of The Customer's collective ICT infrastructure and ICT service catalogue In this context, the service provider is Sykehuspartner.
DNS	Domain Name System - System service for translating between machine name and IP address
EAP-TLS	Extensible Authentication Protocol – used in conjunction with NAC
Fabric Attach	The Extreme Network implementation of IEEE Auto Attach, used for policy-based connectivity and authorisation of supported networking components in a Fabric Connect-based network.
Fabric Connect	The Extreme Networks implementation of IEEE Shortest Path Bridging.

Abbreviation / Term	Description
IAM	Identity and Access Management, the Customer's systems for central authentication, authorisation and federation of users and access rights.
ID porten	The DIFI "ID porten" is used for the authentication of users at security level 4 (BankID, BankID for mobile, Buypass and Commfides)
IDS	Intrusion Detection System
IEEE 802.1x	Standard for authentication of hardware connected to network. Must not be confused with standards for wireless networks (WLAN).
LDAP	Lightweight Directory Access Protocol – Standard protocol for connection/integration with Active Directory
MAC address	Unique ID assigned the network interface at layer 2 in the OSI model
MPLS	Multi Protocol Label Switching
MSI	Format of application packages to be installed locally on PC clients
MD	Medical device
NAC	Network Access Control – See IEEE 802.1x
PAGA	The Customer's personnel system
RADIUS	Remote Authentication Dial-In User Service – Network protocol used for the authentication of machines in connection with use of NAC.
RDP	Remote Desktop Protocol – the Microsoft protocol for the remote control of Windows PCs/servers, available from the Supplier portal
SDS	Central Data Centre - South-Eastern Norway Regional Health Authority shared regional data centres operated by Sykehuspartner.
SHKR	Central Main Communications Room - Data centers established on Customer premises.
SOA	Service Oriented Architecture
SPB	Shortest Path Bridging
SSH	Secure Shell - Application protocol with encrypted communication for access to login and command line on remotely controlled client/server

Abbreviation / Term	Description
SSID	Service Set Identifier – wireless network
TD	Technical administrative devices, such as parking systems, kiosk solutions etc.
UltraVNC	Remote control tool, available from the Supplier portal
VLAN	Virtual LAN - a method for logical separation of a network in broadcast domains
VPN	Virtual private network – encrypted, private network connection
WAN	Wide Area Network - in this context used as a VPN termination point
WinSCP	Remote control tool available from the Supplier portal
X.509 OU	The standard for certificates used in conjunction with NAC for the establishment of PC clients in the correct VLAN, where the OU (organisational unit) attribute is used to identify the zone