SJÚKRAHÚS
VERKIÐ

General description of the IT environment: HEILSUNET

IT Department:

Development, operations, architecture, and design.

Contents

Revision history

Editors: Annfinn Thomsen (AT), IT department head

Abraham Vijayavarathan (AV), IT network administrator

Latest version

Date	**Editors**	**Changes**
15. July 2021	AT	- Initial draft
21. August 2021	AV	- Spelling and grammar correction
23. August 2021	AT	- Version 1 released

Introduction

This document describes in general the IT infrastructure for Sjúkrahúsverkið and those principles and methods that form the basis for the IT deliveries that are produced and used. The IT infrastructure has been given the name HEILSUNET.

The document is intended as a clear introduction to the IT environment HEILSUNET for suppliers, consultants, employees, and others. The document is updated and maintained regularly, and the latest version can always be downloaded from the intranet: Heimabeitið:

https://heimabeitid.heilsunet.fo

Updates and additions are sent to one of the editors mentioned in the Revision section, who is then responsible for updating the document accordingly.

Demographics

The HEILSUNET IT environment comprises around 2500 IT users, who are divided into several different organizational units. The geographical spread of these users is divided into several locations across the Faroe Islands, with one location located in Copenhagen, Denmark.

Approximately 1500 of the 2500 users work at Sjúkrahúsverkið, whereas Landssjúkrahúsið, the National Hospital, has the largest concentration of users. The other hospitals are Suðuroyar sjúkrahús and Klaksvíkar sjúkrahús. The location in Copenhagen is Hotel Torshavn.

The IT department, which operates the HEILSUNET also provides IT services, mostly limited to the national-wide EPJ system, *Cosmic*, to the following external areas:

- Municipal doctors / general practitioners
- Municipal nursing homes
- The Faroese Pharmacy Service
- And other public institutions that need access to the National EPJ.

However, these external areas are mostly exempt from the description in this document unless expressly and specifically mentioned.

Contact for further information

For further information about the IT architecture at Sjúkrahúsverkið, please contact the IT department:

Sjúkrahúsverkið
c/o Landssjúkrahúsið
IT Department
J.C. Svabosgøta 41-49
100 Tórshavn

Overall description of the HEILSUNET IT environment

The IT department provides IT services for the entire Sjúkrahúsverkið.

A key and central principle for HEILSUNET is that the similar services must use uniform processes across the entire organisation, whereby the same tasks are supported by the same systems. The unification of the IT organisation thus aims to achieve increased efficiency, greater joint sustainability, and operation of business-supporting information technology solutions throughout the organisation.

The aim is to consolidate IT operations centrally in modern operating environments, and thus, the main IT operation is hosted at the National Hospital's two datacentres. These datacentres are located in building B11 and B22. A new datacentre is underway, which will replace the datacentre located in B11. However, to limit network delay or lag and jitter between locations, the locations in Suðuroy, Klaksvík and Copenhagen have small operations centres each equipped physically with a server, which is part of the centralised virtual environment, VMware.

Transverse IT systems such as network, collaboration platforms (Exchange, Sharepoint, Teams and Video conference), EPJ, radiology systems and X-ray archives, case management, and other centralised IT systems have been introduced. As part of HEILSUNET infrastructure, a common HEILSUNET ID has been introduced i.e., coordination of user IDs and passwords for central systems.

Standards have been introduced for models of PCs, printers, mobile phones, etc. applicable to new purchases. All new IT systems purchased and commissioned must operate in the central HEILSUNET environment and be able to provide services to clients across all locations.

Overview of Common IT Platform

The PC client platform is based on Windows 10 in 64-bit version with methodology for rolling out software and applications based on IXP's EasyInstall. All PC clients are joined in the same Active Directory and are to be considered as one installation.

Applications are primarily executed via Microsoft Remote Desktop Services on virtual servers in 64-bit version with applications rolled out isolated / virtualised for both clients and application servers. However, due to compatibility issues or other restrictions, some applications are installed and executed locally from the PC client.

Architectural principles for the HEILSUNET IT installation

The IT department aims for a system architecture that can contribute to realising the following goals:

Business Continuity: Despite hardware failure, natural disasters, or data corruption, these should not be allowed to disrupt or stop enterprise activities or services provided to employees and patients.

Benefit maximisation: All decisions about IT must be made based on the benefit of Sjúkrahúsverkið as a whole, which means that the needs and requirements of the organisation take precedence over individual departments or individual needs.

Data as an Asset: Data is concrete and an asset to Sjúkrahúsverkið. Since all employees rely on data as a real and measurable resource, it needs to be carefully organised and managed, and simultaneously presented as reliable and accurate.

Data accessibility: Services and data must be able to be deliverable, at the right time in the right place to the right extent.

Standardisation: The aim is for data to be used across systems, and thus, open standards are employed wherever possible. One goal is for data such as employee information and personal register (p-tal) to be retrieved from common resources. For example, personal register data is fetched from the centralised national registrar, while employee information is fetched from a centralised internal system called Tardis. The goal helps to avoid redundant, inconsistent data. Standardisation also helps to support interoperability between systems.

Scalability: Systems must be expandable to the extent required to meet requirements for larger volumes in production.

The IT department's IT operations are based on ITIL and principles of Prince2 when building structures and processes in the IT organisation. Principles and terminology from these frameworks can therefore be used to advantage in connection with documentation and design as well as building processes for development, operation, and maintenance.

Service provider and operational responsibility

For clinical systems, the operational responsibility up to and including the operating system lies with the IT department, whereas operational responsibility for the application is typically anchored in clinical product groups and with underlying agreements with the service provider. However, in some cases, the IT department acts as first and second level support to clinical systems, before contacting service providers.

In practise, this means that regular maintenance of underlying operating systems, management systems and other software such as anti-virus, etc. is handled by the IT department. Additionally, the IT department monitors specified IT services in accordance with OLA and service level (provider) agreements.

Interoperability

Interoperability - or in other words components and subsystems being able to communicate with each other - is a crucial prerequisite for the realisation of the service-oriented system architecture and for the realisation of several the aim and goals stated above.

The requirement for interoperability implies preconditions:

- On the 'business side' there are open, documented data models (data definitions with definition of context in which data is used) and open, documented interfaces and protocols for use / communication of data.
- On the technical side there are similarly open, documented definitions of how components in the delivery's technical platform (middleware layer and operating platform) interact, defined in the form of standards.

An open standard is thus a standard that is documented (in sufficient detail), freely available and remains freely available. An important distinction is made between 'proprietary' standards (having an owner with the possibility of restricting the use of the standard), 'de facto' standards (dominant standards without being publicly adopted) and 'de jure' (public) standards (adopted by public Nordic or international) standardization bodies.

Unless otherwise stated the Sjúkrahúsverkið aims to apply 'de jure' standards, and secondarily to apply 'de facto' standards with a sufficient degree of openness.

The objective of using open standards, open interfaces and open data models is a crucial precondition for the interoperability requirement and thus for the realisation of a service-oriented system architecture. The use of open standards, open interfaces and open data models is also crucial in order to achieve greater supplier independence and realize a multi-supplier strategy for both the viability of the investment and the possibilities for further development and expansion of the system solution in line with changing needs and new opportunities.

It is recommended that clinical systems aim to use established and standardised interoperability standards, preferably based on the initiative by healthcare professionals and industry, IHE. The aim is to follow these standards:

- Interfaces follow IHE's profiles
- HL7 FHIR / DICOM / HL7v2

Compliance with legislation, common public standards and recommendations

Systems established in the HEILSUNET IT environment must comply with current Faroese legislation concerning Safety and security regarding processing personal information, as well as all GDPR regulations. In addition, international standards such as ISO 27002 are also employed, and the information security function regularly prepares guidelines and guidelines for work with and requirements for data-bearing systems under the responsibility of Sjúkrahúsverkið.

Datacentre

The datacentres hosting the HEILSUNET IT installation are built around two network layer-2 operating centres, which are interconnected by fast network connections. The operating centres are equipped with central emergency power, cooling, access control and other safety systems such as automatic fire protection, various alarms, and CCTV.

Servers

The primary hosting cluster is based on physical servers from HP and run VMware as the virtualization hypervisor. All virtual servers are hosted in the hosting centres and are all based on Intel x64 platform. A few special purpose physical servers are also deployed. These special servers either run Windows server or Redhat Enterprise operative systems.

Both Windows and Redhat server operating systems are installed, operated, and maintained in a prescribed and standard manner, and are monitored by the centralised SolarWinds Orion software. All Windows and Redhat servers have being installed with Bitdefender Anti-virus, SolarWinds monitoring Agent, Asset management agent, etc.

There is no Database cluster available; however, most databases are based on Microsoft SQL server. Wherever possible, it is a requirement that the application itself and database to be separated upon implementation, i.e., one or more servers for the application and the Database on one of the available SQL servers.

While Microsoft SQL server is the go-to Database system, some application require SQL servers based on other vendors or technology. Therefore, in special cases, such as the applications MADS or BBC LAB special purpose virtual machines have been created to fulfil the requirements of the applications.

Server operating systems

Due to legacy systems, a few operating systems differ from the minimal requirements; however, as these are being replaced, older operating systems are prohibited and therefore not allowed. The following server operating systems are supported (these are supported on physical servers as well as on virtual servers):

- Windows Server
- Linux: RedHat Enterprise

Currently, the following operating systems are allowed:

- Microsoft Windows server 2012 R2 (*considered legacy and no new installations are allowed*)
- Microsoft Windows server 2016 (*if absolutely necessary*)
- Microsoft Windows server 2019 1809 (*default server operative system*)
- RedHat Enterprise Linux (RHEL) 7.x
- RedHat Enterprise Linux (RHEL) 8.x

Windows Server 2019 and RedHat Enterprise can be installed as virtual servers and on physical servers. Virtual Appliances containing other server operating systems are accepted, as these are delivered ready-made by suppliers as an image for installation in the HEILSUNET IT environment. Operating, maintenance and security updates will be required of these devices in accordance with general IT security policies.

Server operating systems maintenance

Windows and Redhat servers are categorised by importance and business impact and are updated in accordance with pre-approved service windows. The categories are low, medium, high, and critical impact servers.

Low impact servers download and install updates automatically every Wednesday between 00:00 and 01:00. Medium impact servers download and install updates automatically every third Wednesday between 00:00 and 01:00. High and critical servers consist of clinical applications or critical infrastructure services and follow change management processes. The aim is to minimum update these servers at least once every three months.

Windows servers are updated using Windows Server Update Services (WSUS) while Redhat Enterprise updates are deployed using Ansible. Currently, Windows servers are required to be updated with the following Update classifications:

- Critical updates
- Security updates
- Update rollups

Critical updates that require an immediate response will be installed and the associate system or servers restarted if deemed necessary by the IT department or IT security department. This action usually bypasses any service window or change management procedures in place.

Databases

As mentioned in the section above, HEILSUNET primarily uses Microsoft SQL Server technology; however due to specific application requirements, some clinical systems are based on SQL servers, such as Oracle or Progress. These systems often, while not always, have a dedicated virtual Windows server for the installation of SQL server.

Larger systems such as Cosmic (EPJ) and Sectra (radiology) run on dedicated Microsoft SQL servers, while quite a few smaller applications run on shared Microsoft SQL servers. These smaller applications are split between SQL servers, depending on whether they are clinical or non-clinical applications.

The shared SQL servers run Microsoft SQL server 2014, 2016 and 2019 Enterprise. Access to the shared SQL servers is through SQL Management Studio. No direct access is allowed (remote desktop) unless monitored by an employee of the SQL server administrator. The SA role is prohibited and limited to SQL server administrators. Service providers and others are allowed DBo (database owner) privileges to databases.

Storage

SAN and NAS are used for all storage purposes.

The entire virtual platform (VMware) uses a two-site 3PAR all flash storage from HPE. The SAN storage is an active-active solution which replicates the data live between the two datacentres. The SAN is based on 16Git Fibre Channel connections and consists of redundant fibre fabrics / switches.

The NAS solution is based on EMC Isilon technology and is primarily used for archiving and long storage data. The Isilon setup is a failover setup, where one Isilon acts as the primary and the other one as a failover. The data from the primary Isilon is mirrored to the secondary Isilon. No backup is taken; however, daily snapshots are taken and stored locally on Isilon.

Connection to NAS can be established via the NFS or CIFS protocols. This can be combined with an archive solution where active data is backed up through the operative system.

Backup

Data backup system is centralised around Veeam Enterprise backup. Each datacentre has two physical servers which handles backup of locally stored servers and data. One of the server acts as a Veeam proxy while the other is a data repository.

The data is stored locally in the datacentres for 30 days, and after that the data is copied to a third site and stored for 5 years. The common Grandfather-father-son backup rotation scheme is used.

Restore requests are allowed, and requests should be sent to the HEILSUNET Servicedesk.

Printing

Printing is centralised around Microsoft Windows servers. In addition, print management is centred around the print application software PaperCut, which enables follow me printing, a shared print queue, etc. All printing is monitored for statistical purposes.

Network

The two datacentres at Landssjúkrahúsið are interconnected in a redundant ring structure. The design architecture follows Cisco Medical-Grade Network.

Physical LAN Design

The LAN design consists of five different types of blocks. Core block, distribution block, Access block, Server block and WAN block. Single mode optic fibre cables are established between all buildings. These are routed different ways, to optimize redundancy. To further optimize redundancy, the different network blocks need to split their uplink to the core, to be sure that not a single damaged fibre cable can put down a complete network block.

All three hospitals follow a traditional LAN design, where access switches are placed in patch rooms (X-field rooms), which are connected to centralised distribution switches. However, at the Main Hospital, Landssjúkrahúsið, work has started to convert LAN to the more contemporary Fibre to Office.

WAN connections

In addition to Suðuroyar sjúkrahús, Klaksvíkar sjúkrahús and the Patient Hospital in Copenhagen, several smaller satellite offices are also connected to HEILSUNET. The two smaller hospitals are each connected through an ISP provided MPLS 1Gbit connection, while the satellite offices range from 10Mbit to 20Mbit. All connections are VPN L2L IPSec encrypted. All WAN and associated remote subnets are IPv4 routed networks.

Connecting equipment to HEILSUNET

Vendor-specific VLANs are not part of the network design.

HEILSUNET wired network is divided into three main network security zones controlled by Cisco Identity Service Engine (ISE), which is an advanced RADIUS / TACACS+ server focused on network policy (artificial intelligence) decisions:

- Trusted – Access Controlled
- Trusted – Internet Access Only
- Untrusted – Internet Access Only

ISE policies consist of three concepts consisting of authentications, authorisation, and accounting. These Authentication Mechanisms are 802.1X, Mac Authentication Bypass and Profiling.

Most equipment use IP address via DHCP, are registered in DNS and operate in a complete routed environment. However, some medico modalities use statics IP addressing. No custom VLANs, private networks or IP addresses are allowed within HEILSUNET.

Service providers who require their own VLAN or local LAN for their equipment are required to provide the necessary network equipment as an integral part of the delivery and service. The interface can for example be established as a firewall / NAT router. The IT department will consider this unit as the interface to the service provider’s equipment in troubleshooting contexts. All required network ports and IP addresses will be made available by network administrators employed at the IT department. To communicate with services on HEILSUNET internal net, service provider’s own equipment needs to NAT to the provided IP address.

Legacy equipment, whether Medico modalities or IT equipment, who do not meet the requirements of the IT security policy, e.g., obsolete protocols or no antivirus, will be placed on an isolated VLAN behind a firewall, in which only the required port will be able to communicate with its destination.

Firewalls and Citrix Netscaler

All services which are accessible from the outside (from the Internet to HEILSUNET) are terminated at the Enterprise Edge Firewall and, if possible, load balanced with HEILSUNET central load balancer, Citrix Netscaler.

Wireless (Wi-Fi)

All Wi-Fi connection are managed by centralised Cisco 9800-LF Wireless LAN Controllers as a High Availability cluster. The access points are based on Cisco Catalyst 9120AX Series and are the next generation of enterprise access points. These are resilient, secure, and intelligent and offer the latest technology support like full WiFi6 feature sets.

The Wi-Fi is logically divided into several networks, e.g., general, modality, IOT and guest. The network is primarily based on 802.11ax in the 5GHz range, but coverage on the 2.4GHz band is also possible. All alternative Wi-Fi infrastructures are strongly prohibited and therefore not tolerated.

The guess network is open on new TCP protocol and is free to use, while the internal Wi-Fi SSID are accessible either with passwords (typically legacy modalities) or certificated based authentication (modern modalities, computers, and mobiles phones via MDM).

Mobile network and access to HEILSUNET

The Main Hospital, Landssjúkrahúsið, is fitted with indoor mobile coverage systems (DAS) to provide full GMS and LTE coverage. In addition to full coverage, DAS also helps to lower electromagnetic (EMC) exposure for all mobile devices, regardless of mobile operator.

Mobile devices have access to selected HEILSUNET services through Mobile Device Management (MDM) controlled by the IT department.

VPN, service provider access and data processor agreement

Service providers are given necessary access via Virtual Private Network (VPN). The VPN connection is based on username/password and Active Directory group membership. The access is strictly personal and is given based on a signed declaration of good faith to the individual employee at the service provider.

Additionally, VPN L2L IPsec connections can also be established if the need arises. Only access to specific IP addresses belonging to the equipment that needs access is provided.

Work done outside of the HEILSUNET network, which requires that service providers to store or process personally identifiable data, are required to sign a data processor agreement with Sjúkrahúsuverkið. The Data Protection Officer handles all such agreements.

Common Network Services

HEILSUNET offers a wide range of common network services to be used on equipment, modalities, and applications: DNS, DHCP, NTP, SMTP, SYSLOG and SNMP v2c.

Service windows

Pre-agreed service windows are assigned to every Tuesday at 20:00 to 01:00 and every equal-week Thursday from 20:00 to 06:00.

The IT Security function has mandate to request emergency updates / patches for zero-day security risks. These will be handled ad-hoc.

Monitoring

SolarWinds Orion is used to monitor all servers and network equipment on HEILSUNET. Sensors such as Ping, CPU, RAM and diskspace are always monitored. Depending on the system, a wide range of possible sensors and alarms are available, these include SQL, Exchange, services, processes, logs, and others. The most common method of monitoring on Windows and Linux servers is via Agents, while SNMP and SYSLOG is used with network equipment.

HEILSUNET client endpoints

All endpoint clients are built around Microsoft Windows 10 and Remote Desktop Services. There is full central management, software deployment and patching. The clients are available in two variants depending on the work and placement of the client: “kiosk” -setup and Single-user setup (typically laptops belonging to specific employees). In compliance with IT security policies and common sense, the following applies for all endpoint clients:

- Endpoint clients receive IP addresses and network configurations via centralised DHCP servers.
- No users have local administrators. Selected people have a separated user that is used to elevate to administrator rights.
- All computers and servers are domain joined and part of HEILSUNET Active Directory.
- Applications are primarily run via Remote Desktop Services; however, some applications are installed locally.
- All applications are centrally deployed via a centralised management software called EasyInstall.
- Google Chrome and Internet Explorer 11 are being replaced with Microsoft Edge. Microsoft Edge will be the only accepted / allowed browser in the future.

Mobile devices and clients

Mobile devices and iPads are conceptually established at the same level as HEILSUNET PC clients, and therefore, follow the same principles for management, procurement, maintenance, and support.

Enterprise Mobile Management (EMM)

Mobiles and iPads are centrally managed by the EMM product VMware AirWatch. No access is given to internal resources via mobile devices unless these are managed by the AirWatch. Consequently, all enterprise APPs, e.g., e-mail clients, emergency and EPJ are deployed and managed using AirWatch.

/> IT Department