Oslo University Hospital

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 1C Technical Requirements

Version 1.0, July 2019

Oslo University Hospital

Table of contents

1 General architectural principles and system description

Sykehuspartner is the Customer's service provider, and operates and manages the Customer's infrastructure and ICT platform on behalf of the Customer. The Customer's technological platform is described in more detail in the documents:

- *SSA-T Appendix 3a – "Customer's technological platform*"
- *SSA-T Appendix 3b – "Kundens tekniske plattform – Integrasjon"* (Customer's technological platform – Integration)
- *SSA-T Appendix 3c – "Kundens tekniske plattform – Identitet og tilgangsstyring"* (Customer's technological platform – Identity and access management).

When this document refers to "SSA-T Appendix 3 – Customer's technological platform", without explicit saying 3a, 3b or 3c, it refers to Appendix 3a, 3b and 3c together.

The Customer's service provider also manages large portions of the Customer's system portfolio under a service contract established between the Customer and the Customer's service provider.

The Customer and the Customer's service provider commit to comply with guidelines established in National ICT's general Architectural Principles in the specialist health services, cf. *SSA-T Appendix 1 - Attachment 1 – "NIKT Arkitekturprinsipper i Spesialisthelsetjenesten" (Architectural Principles in the specialist health services).*

The offered system shall be established in the Customer's established infrastructure and on the Customer's existing ICT platform. The offered system shall be integrated with and interact with existing and future technical equipment. The system shall additionally integrate and interact with both existing and future administrative and clinical specialist systems, and the Customer's PAS/EPJ (DIPS).

It is therefore important that the offered solution can be established in accordance with the requirements and guidelines described by the general guidelines and limitations described in SSA-T Appendix 3 – "Customer's technological platform" and the requirements in this requirement specification.

No.	Requirement	Importance (O/H/M/L)	Describe
T 1	The Contractor shall confirm that it has familiarised itself with and has understood the architectural principles described in the document *SSA-T Appendix 1 - Attachment 1 – "NIKT Arkitekturprinsipper i Spesialisthelsetjenesten" (Architectural Principles in the specialist health services).* **Note:**	O	

No.	Requirement	Importance (O/H/M/L)	Describe
	The Southern and Eastern Norway Regional Health Authority is committed to complying with National ICT's general Architectural Principles in the specialist health services, cf. *SSA-T Appendix 1 - Attachment 1 – "NIKT Arkitekturprinsipper i Spesialisthelsetjenesten" (Architectural Principles in the specialist health services).* The Architectural Principles are brief and concise rules intended to develop the specialist health services in line with the specialist health service's visions and goals, statutes and regulations, and technological opportunities.		
T 2	The Contractor must confirm that it has familiarised itself with and has understood the description of the Customer's infrastructure and ICT platform described in the document SSA-T Appendix 3 – "Customer's technological platform." **Note:** The Customer has an established infrastructure and ICT platform described in SSA-T Appendix 3 – "Customer's technological platform," which includes a number of guidelines and restrictions on new systems that are to be established at the Customer. The Customer's infrastructure and ICT platform is established in accordance with the principles in National ICT's general Architectural principles in the specialist health services, in addition to other guidelines, principles and objectives defined by the Southern and Eastern Norway Regional Health Authority, the Customer and the Customer's service provider.	O	
T 3	The system shall be established as an internal system in the Customer's existing infrastructure and ICT platform. **Note:** The Customer will not permit that the system is established externally, for example in an external cloud service or a data centre under the control of the Contractor, Manufacturer or other third party.	O	
T 4	The system should support *internally* established cloud services (Private Managed Cloud). The Contractor is asked to clarify the system's support for establishment on internally established cloud services, and on any platforms that are supported. **Note:** An internal cloud service is not currently established in the Customer's technical platform, but it is expected that this will be established and applied in the future.	L	D
T 5	The system should be established without dependencies on external services, for example cloud services, web portals or interfaces (APIs) outside the Customer's network, for example at the Contractor or Manufacturer. **Note:** The Customer requires control and traceability for all external communication to and from the system.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
	If the system relies on external communication, the Contractor is asked to clarify the response and document for which purpose such communication is required, and the Contractor of and name of all external services.		
T 6	If the system is dependent on *external* service, for example cloud services, web portals or interfaces (APIs), the offer must also include the relevant solution design and risk assessment for the Contractor's infrastructure that the system depends on. The description must also include which data that are intended to be transferred.	H	D
T 7	The Contractor must present a general solution design and concise system documentation for the solution established internally in the Customer's existing infrastructure and ICT platform.	O	
T 8	Solution design and concise system documentation in requirement item T 7 should in a clear and concise manner show the system's relevant key components, general data flow and communication interfaces internally and externally. **Note:** It is of utmost importance that the documentation reflects the system, with an accompanying illustration, as it is intended to be established in the Customer's technical platform, cf. *Appendix 3 Customer's technological platform* The documentation should include all individual components, for example technical equipment, client PCs, servers, storage, network, converters, etc., included in the system. Any individual components that are not in compliance with the Customer's technical platform should be described, including how these deviate, viewed in connection with requirement T 1.	H	D
T 9	The Contractor must present a detailed overview based prepared documentation from requirement item T 8 of all relevant network-related data flows as the system is planned to be established at the Client. The documentation should in a transparent manner show the detailed data flow between the system's individual components, with existing components and other services in the Customer's network, and from which component the traffic is initiated (traffic direction). **Note:** By "relevant" it is meant data flows that use or traverse the Customer's data network and thus can require that firewall rules must be adjusted for the offered system to function in the Customer's infrastructure and ICT platform.	H	D
T 10	The system should use a three layer architecture to limit exposure of the underlying database to the client application. The Contractor is asked to clarify such support, and to describe which components in the system where this is not supported.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
T 11	The system should be modular in order to ensure that modules may be easily added, replaced or removed in the system in accordance with future change requirements. The Contractor is asked to clarify the system's support in terms of module-based architecture, which modules that are included in the system or that may be purchased as options, and in general which functionality that is covered in which module.	H	D
T 12	Duplication of data across systems should only occur if enterprise needs indicate that this is the best solution. **Note:** If the Contractor deviates from the requirement, describe why this may be an appropriate method. The Customer prefers that lookup towards source or other systems are used when the system itself doesn't own the data elements.	M	D
T 13	The system should support the use of container services, for example Docker or Kubernetes. The Contractor is asked to clarify which container services that are supported, if any. **Note:** Container services are currently not extensively used in the Customer's technical platform, but it is expected that these will be used more widely in the future.	M	D
T 14	The system should be developed using a modern development language and framework, uniform for all the components of the system. **Note:** The Contractor is asked to clarify: • which development language and framework that is used for the development of the system • which version of framework that is used • any deviant development languages/frameworks and versions used in different components in the system The Contractor is particularly asked to clarify whether there are differences in development languages, frameworks or versions of frameworks that are due to certain components in the system not being modernised, or where the Contractor has an ongoing process to modernise the system. Any ongoing processes for modernisation should be reflected in a roadmap.	M	D
T 15	The system must ensure data integrity in those cases where several users are working on the same dataset at the same time.	O	
T 16	The Customer wished to promote sustainable use of ICT throughout the system's life cycle. The Contractor is asked to clarify how it works in accordance with principles established in connection with Grønn IT (www.ikt-norge.no/bransjenormer-guider/gronn-it/)	M	D

2 Scalability and performance

Scalability is defined in this context as the system's ability to handle changes, for example in number of users, simultaneous users, number of integrated technical devices or data volume, without impacting the performance of the system or other components and services in the infrastructure and ICT platform in general.

Performance is defined as the system's ability to work and respond quickly, to ensure efficient use and a good user experience.

The requirements to scalability and performance concern all components and features in the system, for example client application, application services, integration interfaces and databases.

No.	Requirement	Importance (O/H/M/L)	Describe
T 17	The system should scale with regard to *simultaneous* users without this impacting the system's performance. **Note**: The Customer estimates between 30 and 60 *simultaneous* users on the system when the system is in full use. The Contractor is asked to clarify any limitations in *simultaneous users*, how this is impacted by the licence model and how the system should be technically facilitated to ensure scalability with regard to *simultaneous* users, e.g. in intervals of 30-40, 40-60, 60+ users.	H	D
T 18	The system should be designed to scale with regard to *total number* of users without this impacting the system's performance. **Note**: The Customer estimates between 50-100 users on the system when in full use. The Contractor is asked to clarify any limitations in *total number*, how this is impacted by the licence model and how the system should be technically facilitated to ensure scalability with regard to the *total number* of users, e.g. in intervals of 50-60, 60-80, 80+ users.	H	D
T 19	The system should support scaling up or down as needed, for example due to changes in: • number of daily treatment plans created • number of users • treatment techniques for different patient groups, typically more advanced treatment techniques for more and more patient groups The Contractor is asked to describe any limitations in the systems scalability. **Note:** For example, this includes how the system's scalability is impacted by licence model,	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
	application management and equipment, and how the system is adapted for scaling in the event of changes in future needs. See also requirement item T 11.		
T 20	There should be no limitations with regard to the *total number* of client PCs or users/work spaces the system may be distributed to, in accordance with the Customer's scalability requirements. The Contractor is asked to clarify any limitations.	H	D
T 21	The system should be without known errors, defects or issues with regard to scalability and performance, for example with regards to increasing number of users, locations, operations, orders, instruments or data processed by the system. The Contractor is asked to clarify any known challenges related to scalability, and recommendations to avoid future scaling challenges.	H	D
T 22	The Contractor should describe the normal start-up time of the client application from the application starting and until the user may work in the system. The Contractor is asked to clarify with regard to normal start-up time for the client application and factors that may impact this.	M	D
T 23	The system should prevent users with ordinary user permissions from starting processes or features that result in degraded performance for other users or processes in the system. The Contractor is asked to clarify any processes and features users may start that can lead to degraded performance.	L	D
T 24	The system should not start processes, e.g. report extraction, logging, monitoring agents, backup, archiving, analysis, indexing, and clean-up jobs, regular automatically or manually that will have a negative impacting of the users' experience of the system's performance. The Contractor is asked to clarify any processes and features that lead to reduced performance, and recommendations to reduce the possibility that this impacts use of the system.	H	D
T 25	The Contractor should describe typical data volumes in the data flow during normal use of the system, for example on start-up, login or specific user operations in the system. **Note:** The customer wants to clarify whether there are specific incidents or user operations in normal use of the system that entail the transfer of large data volumes, which thus may degrade the system's performance.	M	D
T 26	The Contractor should describe the system's bandwidth requirements.	M	D

3 Infrastructure and platform

Sykehuspartner is the Customer's service provider, and operates the Customer's infrastructure and ICT platform described in *SSA-T Appendix 3 – "Customer's Technological Platform*."

Through the Service Provider's contracts, the goal is that all system components included in a system support a so-called "N/(N-1)" life cycle. This means that the latest or second latest versions of all hardware and software components are supported.

3.1 General requirements to infrastructure and platform

No.	Requirement	Importance (O/H/M/L)	Describe
T 27	The Contractor should describe all relevant components (operating system, client applications, database platform, web servers, server software, third party components, etc.) that are not provided as a part of the system, or that deviate from the Customer's standards. **Note:** This may include web browser, browser extensions, web server, database platform, Java, Flash, Silverlight, Microsoft Office, .NET Framework, C++ Redistributable, MDAC, etc. The Contractor is asked to clarify the component's purpose, in addition to Contractor, component name and version of the components for all parts of the system.	H	D
T 28	The system should be established without dependencies on specific versions of Microsoft Office on the Customer's client platform. The Contractor is asked to clarify any dependencies, the purpose of the dependency, product in the Office package and version required. **Note:** Dependencies to products in the Office package are not desirable, as it poses challenges to maintenance and upgrades of the Office package on the Customer's client platform.	H	D
T 29	The client applications should run without the use of Java runtime, ActiveX controls, Flash, Silverlight or browser extensions installed on the Client PC. In the event of needs, this must be described and justified. **Note:** Due to security reasons, the Customer does not permit local installations of Java runtime on client PCs. Java runtime may be enabled for applications distributed through App-V (virtualised), but it is preferable to avoid this. It is preferable to avoid dependencies on ActiveX controls, Flash and Silverlight, as these have already lost or are in the process of losing support in modern web browsers.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
T 30	The system should maintain support for N and N-1 life cycle for all of the system's components. The Contractor is asked to clarify such support, and describe methodology to ensure that the system is updated to support new versions. **Note:** For example, this applies to components and services: • provided by the Customer's service provider, and not part of the delivery of the system • provided by the Contractor as part of the system • provided by a third party	H	D
T 31	All components included in the system shall synchronise time with a central NTP server in the Customer's technical platform.	H	
T 32	The system must have support for Norwegian characters, for example UTF-8 or ISO/IEC 10646.	H	

3.2 Licensing technology

For the Customer and the Customer's service provider it is important to be aware of which technical solutions that are used for license management, and how this impacts operation and management of the system.

It is not desirable to use physical license dongles due to challenges related to this in a virtualised operating environment, or distributed license files due to the maintenance requirement this leads to on the Customer's workspaces.

No.	Requirement	Importance (O/H/M/L)	Describe
T 33	Any licensing mechanisms should be based on a central license and centralised license management.	H	
T 34	The Contractor should describe the system's licensing mechanisms, including the Contractor's technical requirements to this. **Note:** This includes, for example:	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
	• the use of license dongles or other physically attached devices for licensing, including connection interfaces (USB or similar) • the use of client licenses that require installation on the Customer's workspace • the use of a license server, including the Contractor's requirement to this		
T 35	The system should in the event of temporary loss of the licensing mechanism, function without this affecting use of the system. The Contractor is asked to describe any consequences for use of the system in the event of failure of the licensing mechanism.	H	D

3.3 Criticality

The Customer's ability to sustain effective and proper patient care may quickly be affected if the system fails.

The system is planned to be established as a "Criticality 2 – Critical" system. The criticality level imposes restrictions on how the system must be established to secure the highest possible level of availability, fastest possible re-establishment and limit data loss in the event of failure of the service.

Final configuration of the solution for establishing the system will be clarified in the further process for preparing a solution design for the selected system.

No.	Requirement	Importance (O/H/M/L)	Describe
T 36	The Contractor should clarify how the system can and should be established for a high criticality level, with limited downtime and data loss in the event of failure of the system. **Note:** It is particularly important that the Contractor clarifies how the system in technical terms can be enabled to support the criticality level, for example through the use of redundancy, load balancing and clustering of all critical components of the service. It is also important that the Contractor clarifies the consequences in the event of failure of nodes or where individual nodes are taken down for maintenance of the system or underlying infrastructure.	H	D
T 37	The Contractor should describe the system's support for redundant establishment, and describe any individual components in the system that cannot be established redundantly.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
T 38	The Contractor should describe the system's support for load balancing, and describe any individual components in the system that cannot be established with load balancing.	H	D
T 39	The Contractor should describe its recommendation with regard various scenarios for re-establishing the service when service disruption or loss of data occur.	H	D

3.4 Network

The Customer's service provider is responsible for and operates the Customer's network infrastructure with associated network components such as switches, routers, firewalls, etc.

The Customer's network is ready for IPv6, but this has not currently been implemented. The current protocol is IPv4.

The Customer's network uses Network Access Control (NAC, IEEE 802.1x) that closes LAN access for unknown or inactive network connected devices on both wired and wireless infrastructure. The Customer also has standardized firewall control between network zones where inactive TCP sessions are terminated after 60 minutes for security reasons. This places requirements on any equipment that is to be connected to the Customer's network, and the Contractor must take this into account in its tender.

No.	Requirement	Importance (O/H/M/L)	Describe
T 40	The system must support IPv4.	O	
T 41	The system should support IPv6.	L	
T 42	Any wireless equipment accompanying the delivery should use the Customer's existing wireless network infrastructure. Describe any support or deviations from this.	H	D
T 43	The system should be configured with the Customer's own IP address series. **Note:** If the system does not support use of the Customer's own IP address series, such a deviation must be documented and justified. The documentation must contain the necessary IP addresses/IP ranges and TCP/UDP port numbers for services that are made available.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
T 44	The system should support fixed TCP and UDP ports. The Contractor is asked to describe whether fixed or dynamic ports/port ranges are used, and specify the ports to be opened in the Customer's firewall, including traffic direction.	H	D
T 45	The system should use the Client's network without imposing vendor-specific limitations or technical requirements to this. The Contractor is asked to clarify any limitations and requirements to the client's network.	H	D
T 46	The Contractor should describe the system's requirements to latency in the network.	H	D
T 47	The system should handle network communication failures between the different components of the system such that functionality is maintained to the greatest possible extent while the system re-establishes its network communication without a need for manual user operations. **Note:** Security mechanisms in the Client's network closes inactive network connections on layer2 & layer3 (MAC and IP), and packet loss may occur that leads to network communication failures. Any requirements and consequences on the part of the Vendor following from these mechanisms must be documented with regard to design and associated security approval.	H	D
T 48	In case of break in communication between components in the system, the system should restart automatically when network communication is restored. The Contractor is asked to describe any deviation from this. Any components that don't support automatic restoration must be described and reasons explained.	H	D
T 49	All communication should withstand packet loss with subsequent retransmission. The Contractor is asked to describe any limitations and possible error situations in the system in the event of package loss.	H	D
T 50	The system should support DNS name lookups (FQDN) rather than IP addresses.	H	
T 51	The system should not be dependent on WINS or Windows hosts file.	H	

3.5 Servers

The Customer's service provider operates the Customer's server platform, and is based on use of Windows Server and Linux RHEL servers in a VMware virtualisation environment. The use of

physical servers must be avoided where possible. Supported operating systems are Windows Server 2019 and Linux RHEL 7.5, in addition to previous version (N and N-1).

Services may be provided in the Customer's locale data centre (SHKR).

No.	Requirement	Importance (O/H/M/L)	Describe
T 52	The system should be implemented on a virtual server platform operated by the Customer's service provider. The Contractor is asked to clarify such support, and document any certifications the system has with regard to virtualisation technology.	H	D
T 53	The system should be implemented without the use of physical servers. **Note**: Any physical servers will be operated by the Customer's service provider. The Contractor is asked to justify any use of physical servers.	M	D
T 54	The Contractor is asked to clarify minimum requirements to all servers that will be included in the service. **Note:** Example: RAM, CPU, operating system (HOST/GUEST), disk capacity, RAID configuration, etc.	M	D
T 55	The system should work om Windows Server 2019 or Linux Redhat RHEL 7.5 The Contractor is asked to clarify which operating system that is supported, in addition to vendor-specific requirements to version of operating system, patches and deviating configuration. **Note:** If the system supports several operating systems on servers, the Contractor should clarify and provide recommendations with regard to choice of server platform, and document any pros and cons in terms of solution choice.	H	D
T 56	The system should at all times support the latest patches of the operating system on the Customer's servers. The Contractor is asked to clarify any limitations and justify these. **Note:** Deviating patch levels are not desirable in server environments	H	D
T 57	Use and maintenance of software and services installed on servers should take place without the use of local administrator privileges on the operating system. The Contractor is asked to clarify any deviations and justify these needs.	M	D
T 58	All applications and system services on servers should be started as services.	H	

No.	Requirement	Importance (O/H/M/L)	Describe
	Note: It is not desirable that applications and service on servers require that a user is logged on to a session on the server's desktop during normal use.		
T 59	All system services should start automatically upon restart of server. **Note:** There should be no requirement for manual procedures related to starting services after a server restart.	H	
T 60	All applications running as system services on servers should use users defined by the Customer's service provider. The Contractor is asked to clarify any deviations and justify these. **Note:** Global users defined by or hard coded by the Contractor or where passwords may be retrieved from available documentation, are not permitted.	M	D

3.6 Web server

The Customer's service provider operates and manages the Customer's web servers. The requirements are answered if the system is delivered as a web application or with web services, for example APIs based on use of web services.

No.	Requirement	Importance (O/H/M/L)	Describe
T 61	The Contractor should clarify which web server platforms the system supports, for example Microsoft IIS or Apache.	H	D
T 62	If the system supports several web server platforms, the Contractor should clarify and provide recommendations with regard to web server platform, and document any pros and cons in terms of solution choice.	H	D
T 63	The Contractor should clarify any additional components, for example .NET runtime, PHP or similar frameworks and third party components that are required to be installed on the system's web server.	H	D
T 64	The Contractor is asked to clarify mechanisms that secure the web server and contents from unauthorised access.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
	Note: This includes which security mechanisms that are activated, and which mechanisms that additionally may be activated.		

3.7 Database

The Customer's service provider normally operates and manages the Customer's database platforms.

The database platforms are based on Microsoft SQL-Server 2016 and Oracle 12c (N and N-1). Microsoft SQL Server Always-On cluster and Oracle Maximum Availability Architecture (MAA) are supported.

No.	Requirement	Importance (O/H/M/L)	Describe
T 65	The Contractor should clarify which database platforms the system supports, including product name and version. If the system supports several database platforms, clarification should provide recommendations with regard to database platform, and any pros and cons between the solution choices.	H	D
T 66	The Contractor should describe any special requirements to configuration of the database platform for use with the system.	H	D
T 67	The system should have support for establishment in a technical environment with High Availability-design (HA), which includes clustering of services (database), mirroring of data and any other HA mechanisms. The Contractor is asked to clarify such support.	M	D
T 68	Database connections for all of the systems components should be configurable. The Contractor is asked to clarify any individual components that fail to meet this requirement.	H	D
T 69	Database connections should be encrypted in configuration files. The Contractor is asked to clarify such support and any individual components where this is not supported.	H	D
T 70	The system should be established without the need for local setup of ODBC drivers for database connection on the workspace.	H	

No.	Requirement	Importance (O/H/M/L)	Describe
T 71	The database must handle Norwegian characters, date format and time for registration, display and sorting of data.	O	
T 72	If the Contractor must operate the database platform, it must be described reasons for this.	M	D

3.8 Workspace and client application

The Customer's standard operating system is currently Windows 7 64-bit on PC clients, and a process is ongoing for transfer from Windows 7 to Windows 10 with planned completion in Q1 2020.

The Windows 7 platform uses RES One Suite from Ivanti (www.ivanti.com, for Windows 10 the product has changed name to Ivanti Workspace Control) for administration of client workspaces, including provisioning of client applications with all associated plugins/third party components. The distribution of applications is preferably done via App-V, where the application is distributed to a user, alternatively via SCCM, where the application is distributed to a specific PC client.

In connection with the Windows 10 transfer, establishing Windows 10-based tablets is planned.

In this context, the term application is used for the component or components in the system that either will be distributed to the user's workspace, or made available as a web application.

The term workspaces used as a collective term for Windows-based desktop PCs, laptops, tablets and Citrix.

A process has been initiated for establishing a mobile platform for the secure use of clinical and administrative applications on smartphones and tablets with Android and iOS operating systems.

No.	Requirement	Importance (O/H/M/L)	Describe
T 73	The application must support both Windows 7 and Windows 10.	H	D
T 74	The Contractor is asked to clarify any vendor-specific minimum requirements to client PC, for example: RAM, CPU, OS, disk, RAID, connection boards, etc.	M	D
T 75	The Contractor is asked to clarify any vendor-specific requirements to version of	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
	operating system, patches and deviating configuration.		
T 76	The application should work in the Customer's Citrix environment. Clarify any vendor-specific requirements to version of operating system, patches and deviating configuration.	H	D
T 77	The application must at all times support the latest patches of the operating system on the Customer's workspaces. **Note:** Deviating patch levels are not permitted on operating systems on the customer's standard workspaces.	H	
T 78	The application should be made available as a web application. Describe how such support is facilitated, or which features/modules in the system that have such support and which that must be made available as applications installed on the Customer's workspace.	H	D
T 79	Applications that require installation to be accessible on the Customer's workspace must support the use of RES One Suite/Ivanti Workspace Manager for facilitation of the application on the Customer's workspace.	M	
T 80	Applications that require installation to be accessible on the Customer's workspace should be delivered as MSI packages.	H	D
T 81	Applications that require installation to be accessible on the Customer's workspace must be possible to pack by the Customer's service provider before being distributed to the Customer's workspaces.	O	
T 82	Applications should support distribution via App-V. The Contractor should clarify which distribution methods that are supported for making distributed applications accessible, and any consequences of distribution such as App-V package vs. SCCM. **Note:** The Customer's service provider prefers distribution of application packages via App-V. If required, applications may be installed using SCCM.	M	D
T 83	In normal use the application must be run with standard user privileges, for example without the use of local administrator privileges or other customisations.	H	
T 84	The Contractor is asked to clarify any deviations or required customisations of user privileges for normal use of the application.	H	D
T 85	The application should work without limitations due to logging on to the operating system with a common user (Functional user).	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
	The Contractor is asked to clarify any support and which limitations the use of a common user (Functional user) on the operating system has for the application.		
T 86	Web applications must support Internet Explorer 11 on Windows 7 and Edge on Windows 10. **Note:** Internet Explorer 11 is the default browser on Windows 7. Through the planned deployment of Windows 10, Microsoft Edge will be introduced as the default browser. Google Chrome has been introduced as secondary browser on Windows 7, and continues as secondary browser on Windows 10.	H	
T 87	The Contractor is asked to clarify any functionality or parts of the system that are not supported or are limited in Internet Explorer 11, Microsoft Edge and Google Chrome. **Note:** The Contractor is also asked to clarify how functionality that is not supported or that is limited is otherwise facilitated.	H	D
T 88	The Contractor is asked to describe which browsers and versions that are supported.	H	D
T 89	Web applications should be developed according to the HTML5 standard.	H	
T 90	Web applications should work without the use of third party components or browser extensions/add-ons. The Contractor is asked to clarify any need for any third-party components (extensions) that are required in the user's browser, and justify the need.	H	D
T 91	The application should support the use of different screen resolutions and aspect ratios (e.g. 4:3, 16:9). **Note:** The Contractor must describe any limitations that exist in the application with regard to screen resolution and aspect ratios.	H	D
T 92	The application should support the display of different information in the user interface when the application is used in a multi-display setup. The Contractor is asked to clarify such support, and which modules/features in the system that may/may not be shared on several screens.	M	D
T 93	The application should be configurable on a system level. The Contractor is asked to describe and give reasons for, functions, components or peripheral devices that will require manual setup locally on the workspace. **Note:** It is not desirable to have to make local settings on the individual workspace the	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
	application is installed on because this will increase complexity related to change and management of the application.		
T 94	The system should have a built-in help feature with search functionality.	H	
T 95	Where relevant in the system, the system must have a search feature to perform lookups, for example of history and latest patient lookup.	H	

3.9 Storage, backup and archiving

The Customer wishes to comply with the principles of Data Lifecycle Management, where Backup/Restore is a key component to ensure data security and integrity. The goal is to use centralized storage and backup/restore to the greatest possible extent.

Services for storage, backup and archiving of data are operated by the Customer's service provider.

No.	Requirement	Importance (O/H/M/L)	Describe
T 96	The system should use storage solutions that can be delivered by the Customer's service provider. Clarify any vendor-specific requirements to storage solution. **Note:** This may for example be storage principles, file system, disk volume, read/write speed, etc.	H	D
T 97	Backup of disk, including software, configuration, calibration, etc., on server must run towards existing centralized and automated backup services at the Customer.	O	
T 98	The Contractor is asked to clarify any vendor-specific requirements and recommendations for backup, for examples limitations related to the use of backup agent installed on servers belonging to the system.	H	D
T 99	Backup of databases should run against existing centralized and automated backup services operated by the Customer's service provider.	H	
T 100	The Contractor is asked to clarify any vendor-specific requirements and recommendations for database backup.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
T 101	Databases included in the system should support both full and incremental backups (through e.g. log backup/log shipping) of databases.	O	
T 102	Servers included in the system must permit the use of snapshots for backup of virtual machines.	H	
T 103	The system should support automatic archiving of data based on configurable policies to different levels in the Customer's storage solutions, and manual archiving as needed.	M	D

3.10 Printing

The Customer has established a solution for pull print (Follow-me print/secure print) based on Canon uniFLOW, with centralised print servers and networked printers/multifunction printers. For special needs and applications, for example related to workflows or for label printers, local printers without pull print may be established subject to approval. It is preferred that these are connected to the network and do not use local connections, for example via USB.

The Customer's service provider will ordinarily provide label printers for systems that require label printing.

No.	Requirement	Importance (O/H/M/L)	Describe
T 104	The system should use the Customer's pull print service with networked printers provided by the Customer's service provider. Clarify any vendor-specific requirements to printers and any need for locally established/connected printers.	H	D

4 Hardware and peripheral devices

The Customer's service provider is the Customer's main provider of all hardware, including client PCs, servers (virtual and physical), and standardised peripheral equipment, such as printers, label printers, barcode readers, mice, keyboards and displays.

For operational reasons, it is not desirable that the Contractor provides hardware, peripherals or consumables for such equipment as part of the delivery.

The Customer's service provider's product catalogue is revised annually, and which specific products that are available in the product catalogue will depend on the agreements that have been concluded with different Contractors at the time of establishment of the system in the Customer's technical platform.

No.	Requirement	Importance (O/H/M/L)	Describe
T 105	The system should use hardware, for example PC clients, tablets and servers, that may be provided by the Customer's service provider. The Contractor is asked to clarify any hardware that is a part of the delivery, and justify the reason that this must or should be included.	H	D
T 106	The system should use peripherals, for example electronic delineation tablets, keyboards, mice and printers that can be provided by the Customer's service provider. The Contractor is asked to clarify any peripherals that are a part of the delivery, brand, model, connectivity (wireless, network, Bluetooth, USB), and justify the reason for including this. For equipment that can be supplied by the Customer's service provider, the Contractor is asked to clarify any requirements the Contractor of the system has to such peripherals, such as supported brands, models, standards, barcode formats and printing format.	H	D

5 Information security

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 and management 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 (the "Code of Conduct") from the Norwegian Directorate of eHealth, see:

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

To support the Customer's commitments and statutory requirements related to information security, the Southern and Eastern Norway Regional Health Authority has defined a set of information security requirements in the *Regional information security management system*. The set of requirements includes requirements for infrastructure, systems and service, as well as for Contractors 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 or *T Appendix 1 - Attachment 5c "*Sikkerhetsprinsipper og – krav for IKT-infrastruktur *og applikasjoner" (Security principles and requirements for ICT infrastructure and applications).*

The Contractor is expected to have incorporated these requirements and principles and that they are complied with. The requirements in this chapter are particularly drawn from *Regional information security management system*, and will be given emphasis in the tender.

Before the system may be established, a risk assessment must be conducted and approved of the systems final solution design, with all associated components, services and configuration, as the system is planned to be established at the Customer. This will normally be prepared by the Customer's service provider, in cooperation with the Customer and Contractor.

5.1 General requirements to authentication and authorization

Based on internal requirements and requirements in statutes and regulations, the Customer has strong focus on the identification of users and access control to applications.

The desire is centralised and externalised access control with automated creation, change and blocking of users. The benefit is simpler administration of accesses and higher security through timely controlled access to resources. The ultimate goal is to have a policy based (Attribute Based Access Control, ABAC) control of privileges that provides a thorough and automated control of accesses that adapt to the user's work situation and thus give the user the accesses necessary to perform the work in the given situation.

On the way to the goal, the customer and the customer's service provider has several components that may be used for authentication and authorisation.

No.	Requirement	Importance (O/H/M/L)	Describe
T 107	Authentication of users must be done towards the central authentication solution. **Note:** By central authentication solution, it is meant either the regional IAM solution established by the Customer's service provider, or towards the Customer's directory service (Active Directory).	O	
T 108	The system should have support for attribute based access control (ABAC). **Note:** The Contractor should clarify how the system is enabled or may be enabled for attribute based access control, and which attributes that may be used for access control, such as organisation, employment relationship, shifts, delegated responsibility and login location, etc.	H	D
T 109	If the system doesn't support attribute based access control, the system should support role based access control (RBAC). **Note:** The Contractor should clarify how the system is enabled for role based access control, and whether roles and functionality/accesses belonging to the role are pre-defined or may be customised in the system.	H	D
T 110	The system should be established without a need for a local user database that must be manually maintained. **Note:** If the system has a user database that must be maintained manually, the Contractor is asked to justify such a need and describe the purpose of this.	M	D
T 111	The duration of the user's active session in the system must be time-limited.	H	
T 112	The system should support configurable time-limiting for the user's active session.	H	D
T 113	The system should support that there is more than one authenticated user on the system from the same workspace. Clarify any support, and how the system handles the logged in user if a new user logs in, for example by terminating the previous user's session or keeping sessions inactive, but with the option of reactivation through fast user switching. **Note:** It will be relevant for certain applications to configure the customer's workspace with "functional user" (c.f., *SSA-T Appendix 3 – "Customer's Technological Platform"*), that will allow that several users to use the same logged in workspace with fast user switching in the system. SSO will not be possible to use on workspaces with "functional user".	M	D

No.	Requirement	Importance (O/H/M/L)	Describe
T 114	Only personal, identified users may be used in the system. **Note:** Common users or other forms of sharing of user accounts must not occur in the system.	O	
T 115	Global users, such as administrator, SA, root or similar defined by the Contractor or hard coded in the system should be avoided. **Note:** The Customer does not want predefined or hard coded users that may be used for untraceable access to the system. This also applies to third-party components that are used in the system. Any deviations from this must be clarified and justified, as well as whether such users may be deactivated or deleted.	H	D
T 116	In the event of support for integration with the Customer's directory service, this should be done with real-time lookup to the directory service for authentication of users. The Contractor is asked to clarify and justify any deviations from this. **Note:** It is not desirable that integration with the Customer's directory service is used for the synchronisation of users for any local user database in the system.	M	D
T 117	Any local administrator accesses to administration modules should enforce the Southern and Eastern Norway Regional Health Authority's requirements to password complexity and length. **Note:** The requirements are currently: • All user accounts must have a password • The password must have at least 8 characters • The password must have at least 3 of the following 5 properties (cf. Microsoft complex password policy) ○ Uppercase letters (A-Z) ○ Lowercase letters (a-z) ○ Numbers (0-9) ○ Special characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/) ○ Unicode The Contractor is asked to clarify support and any deviations from this, and whether password complexity is configurable in the system. The Southern and Eastern Norway Regional Health Authority's password policy is described in more detail in *SSA-T Appendix 1 – Attachment 5b "*Fellesregional passordpolicy" (Common regional password policy for the health enterprises in the Southern and Eastern Norway Regional Health Authority).	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
T 118	The system should support Single Sign-On (SSO). The Contractor is asked to clarify how SSO is supported. **Note:** SSO will not be possible to use on workspaces where “functional user” is used.	M	D
T 119	The system should support identification of health personnel through the use of smartcards, RFID or similar technology. **Note:** The Contractor is asked to clarify such support and any standards that are supported. Such support should be integrated with the customer’s central authentication mechanism. Also see *requirement item T8.14* with regard to the use of GS1 for the identification of health personnel.	L	D
T 120	In the event of denied access to the system the application should present the reason in an understandable manner to the end user.	M	
T 121	For role based access control (RBAC) the system should support privileges being assigned to roles, and not to individual users.	H	

5.2 Requirement to use of solution for Identity and Access Management

The Customer's service provider has established a common, regional solution for Identity and Access Management (IAM) for federation and provisioning of users. The purpose is to ensure uniform and centralised access control for systems established in the Customer's technical platform and across the health enterprises in the Southern and Eastern Norway Regional Health Authority. There is therefore a preference for systems that may integrate with the IAM solution through federation and provisioning of users, and that supports international standards such as SAML or OpenID Connect for the purpose.

It is required that the system supports authentication towards the centralised solution for access control, and support for attribute based access control (ABAC) will be preferred. If the ABAC requirement cannot be supported by the system, role based access control (RBAC) with provisioned roles may be an appropriate alternative. It is not desirable with role based access control that requires manual maintenance of users and accesses in a local user database in the system.

If the system cannot be integrated with the Customer's IAM solution, it is required that the system may be integrated with the Customer's directory service (Active Directory) via LDAP, preferably LDAP over SSL.

The system should have access control that ensures that employees' role and tasks provide access to functionality, and that the organisational affiliation is governing for which data the user may access.

The IAM solution established by the Customer's service provider is described in more detail in *SSA-T Appendix 3c – "Kundens tekniske plattform – Identitet og tilgangsstyring" (Identity and access control).*

No.	Requirement	Importance (O/H/M/L)	Describe
T 122	The system should support federation as authentication mechanism.	H	
T 123	The system should support recognised standards for federation as authentication mechanism, such as SAML 2.0 or OpenID Connect.	H	
T 124	When using SAML, the system should support the "Service Provider initiated" federation process.	H	
T 125	Upon login to the system, as a minimum the attributes user id, organisational affiliation and role should be retrieved from the central authentication solution to provide the user with access to information and functionality in the system when establishing the user's session.	H	
T 126	The system should enforce the security session. **Note:** This includes, but is not limited to, inactivity, start and end time of the token.	H	
T 127	The system should use federation if a user must be authenticated in another user's security session. **Note:** If the system supports control and approval (peer control) with need for authentication of another user than the currently logged in user, this should be achieved with a centralised authentication mechanism. The Contractor is asked to describe security functionality in the event of peer control.	H	D
T 128	The system should have the possibility to fall back to an alternative authentication mechanism if the federation solution is deactivated or unavailable. **Note:** This entails that in the event of failure of the central federation solution, it must still be possible to log on to the system to ensure operation. An alternative authentication mechanism can in this context be the use of automatically provisioned, locally stored user identities.	H	

No.	Requirement	Importance (O/H/M/L)	Describe
T 129	Upon successful *authentication* of a user who is not *authorised* to use the system, the system must not fall back to an alternative authentication mechanism, and the user should be notified that access is denied.	H	
T 130	The system should query the external authorisation system whether there is an active patient-carer relation if the internal access control mechanism us unable to determine access. **Note:** If the solution is a treatment oriented health register, there is a requirement that access to patient data is regulated through whether there is a patient-therapist relation.	H	
T 131	If an external authorisation service is used, calls to this should be in accordance with international authorisation standards, for example XACML and OAuth.	H	
T 132	In the event of support for integration with the Customer's directory service, this should take place via LDAP over SSL.	M	
T 133	The application should support provisioning of users, i.e. creation, reading, alteration and deletion via a standardised API.	H	
T 134	API for provisioning should support encrypted communication. **Note:** The Contractor is asked to clarify such support, and how communication is encrypted and in accordance with which standard(s).	H	D
T 135	API for provisioning should support the SCIM standard.	H	
T 136	API for provisioning should be REST-based, with communication over HTTPS.	H	
T 137	The API should make it possible to automate provisioning of users in the system, such that privileges don't need to be configured manually.	H	
T 138	The API should enable the granting of individual privileges in addition to standard accesses.	H	
T 139	The system should provide a user interface for user administration, in addition to the API for provisioning.	H	
T 140	The API should provide data on the users in the system so that the API may be used to audit user access.	H	

5.3 Logging

There are strict requirements to logging of use of the system and security events in the system.

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.

No.	Requirement	Importance (O/H/M/L)	Describe
T 141	All relevant actions should be logged. Relevant actions should be measured against the information system, but as a minimum, the following must be logged: • logins • attempted logins • creation, modification and deletion of data • creation, modification and deletion of users • accessing or modification of any health records stored in the system modifications, or attempted modifications, to the system configuration **Note:** For further information, refer to the Standard's fact sheet 15 – "Logging and follow-up of logs," see https://ehelse.no/normen/faktaark/faktaark-15-logging-og-oppfolging-av-logger	H	D
T 142	The following must at least be stored upon access and activity in a treatment-oriented health register: • User, and which of the user's roles that was active, that has attempted to perform or has performed access/any form of activity • The data element that has been created, read, modified or deleted • If the data element modified has been created, read, modified, printed, deleted or any other activity that is possible for authorised users to perform • Date and time for execution/event • Indication of device where activity/unauthorised access has been attempted or completed **Note:** For further information, refer to the Standard's fact sheet 15 – "Logging and follow-up of logs," see https://ehelse.no/normen/faktaark/faktaark-15-logging-og-oppfolging-av-logger	H	D

5.4 Network and communication

The Client's network uses NAC (802.1x), which shuts down LAN access for unknown or inactive devices. Devices that cannot be authenticated in the network will be placed in a quarantine network without access to other components and services in the infrastructure.

No.	Requirement	Importance (O/H/M/L)	Describe
T 143	Any Contractor-provided components that are to be connected to the Customer's network, such as electronic pencil and other technical equipment, should be compatible with use of IEEE 802.1x (Network Access Control). **Note**: For all equipment that is to be connected and given access to the Customer's network, as a main rule the equipment is registered with an approved MAC address for access control. The Contractor is asked to clarify any deviations in such support.	H	D

5.5 Integration interface

No.	Requirement	Importance (O/H/M/L)	Describe
T 144	All integration interfaces (APIs) must be secured against unauthorised use.	O	
T 145	All access requests to the integration interface (API) should be authenticated using an international standard equivalent to SAML. The Contractor is asked to clarify how the API is secured.	H	D

5.6 Encryption

In the Southern and Eastern Norway Regional Health Authority common regional encryption instructions have been established, described in *SSA-T Appendix 1 Attachment 5a – "Fellesregional kryptopolicy"* (Common regional encryption policy).

No.	Requirement	Importance (O/H/M/L)	Describe

No.	Requirement	Importance (O/H/M/L)	Describe
T 146	All data traffic between the endpoints should be encrypted on the application layer in compliance with the Southern and Eastern Norway Regional Health Authority encryption instructions.	H	
T 147	Encryption of any traffic over https should use TLS v1.2, for example when using a web server for web applications or web services for integration purposes. **Note:** For security reasons, the Customer does not want to permit the use of older protocols, and blocking these is desirable. The Contractor is asked to justify any deviations.	H	D
T 148	In the event of using certificates, these should be issued by the Customer's service provider	H	

5.7 Anti-virus and anti-malware

Applicable standard software at the Customer for anti-malware is currently Trend on Windows servers and Microsoft System Center Endpoint Protection (SCEP) on Windows-based workspaces.

No.	Requirement	Importance (O/H/M/L)	Describe
T 149	Applications installed on the Customer's workspace must support the Customer's standard software for antivirus/anti-malware.	O	
T 150	Antivirus/anti-malware scanning on the Customer's workspaces should take place without the need to exclude files or folders. The Contractor is asked to clarify any deviations.	H	D
T 151	Applications installed on the Customer's servers should support the Customer's standard software for antivirus/anti-malware. The Contractor is asked to clarify any deviations.	H	D
T 152	Antivirus/anti-malware scanning on the Customer's servers should take place without the need to exclude files or folders. The Contractor is asked to clarify any deviations.	H	D

6 ICT related operations and administration

The Customer's service provider is responsible for the operation and management of the Customer's technical platform. The Customer's service provider will also have the main responsibility for technical operation of the system to be established on the platform, but will perform this work in close cooperation with the Customer and Contractor.

It is therefore important that the Contractor relates to both technical solutions and procedures that are included in the service provider's operation and management of the system.

6.1 General requirements to ICT related operations and administration

No.	Requirement	Importance (O/H/M/L)	Describe
T 153	The system should only use third-party components that not already are End of Life/End of Support or that become so in the course of the system introduction period. **Note:** Any components that already are beyond End Of Life/End Of Support, or that will become so in the course of the system introduction period, should be specified and justified, and planned upgrades should be highlighted in the system's roadmap.	H	D
T 154	The Contractor is asked to clarify which possibilities and limitations lie in the system's administrative functions and modules that may be used by the Customer and the Customer's service provider through operation and management of the system	H	D
T 155	The Contractor is asked to clarify any included or third party tools and support systems that must or should be used to support technical operation and application management.	H	D
T 156	For installation, troubleshooting, fault rectification, maintenance, updates, upgrades and user support that take place through use of remote access, a Data processor agreement must be concluded and a confidentiality agreement must be signed between the Contractor and the Customer's service provider.	O	
T 157	All use of subcontractors that directly or indirectly gain access to the system installed in the Customer's technical platform shall be informed of and approved by the Customer and the Customer's service provider. **Note:** The Contractor is asked to clarify: • any use of subcontractors	O	D

No.	Requirement	Importance (O/H/M/L)	Describe
	• for which purpose subcontractors are used • the subcontractor's name and where it is located		
T 158	The Contractor must relate to and comply with the Customer's and the Customer's service provider's change regime[1] for deployed solutions. **Note:** The Contractor may not plan and/or implement changes that conflict with planned changes in the Customer's infrastructure. This requires mutual notification of planned changes between the parties' service personnel. In the event of any conflict, it is the Customer's and the Customer's service provider's change regime that takes priority.	O	

6.2 Remote access and external accesses

The Southern and Eastern Norway Regional Health Authority has established a standardised portal for remote access for Contractors through the use of solutions from F5 BigIP and Citrix, and it is currently offered by the Customer's service provider for all external Contractors. This is known as the "Fjernaksess for leverandører" and must be used for all Contractor-specific operations and management where personal attendance on Customer premises is not expected.

In order to use this solution, the Contractor must be able to use the F5 BigIP Web plugin for SSL VPN and the Citrix Receiver web client on its PCs. The Contractor may then access an access server at the Customer's service provider where the necessary software and/or remote control application for the server is made available. All use of the remote access solution must be linked to personal, identified users at the Vendor. Users must be identified with either:

- For Norwegian citizens:
  - Personal identification number F-number (Fødselsnummer)

[1] By change regime it is meant the rules that apply for planning, notification and execution of changes to infrastructure at the Customer, including central data centres at the South-Eastern Norway Regional Health Authority. This includes all physical infrastructures such as power/cooling, physical cables, network, network services and server platforms (physical and virtual) that the offered system depends on to produce the agreed services. All changes that the Vendor wishes to perform must be agreed and aligned with the Client's service provider, as work by this always takes precedence in the event of time slot conflicts. This is to prevent planned maintenance from failing during implementation with associated operational disruptions and risk of patient safety.

- For foreign citizens residing in and working for the Contractor in Norway:
  - D-number
- For foreign citizens who shall use the remote access solution, one of the following:
  - National ID in own country for EU citizens
  - Passport number
  - Social security number
  - Tax identification number

Furthermore, the Customer has established a standardised one- or two-way "file lock" for the controlled and secure transmission of authorised data between the Customer and the Contractor.

A regional VPN Gateway has been established for the termination of VPN connections between Contractors and the Customer. This is the preferred method for *outbound* data transport over VPN from the Customer's network. All planned use of *outbound* data transmission over VPN must first be risk assessed and approved before being established. All changes to configuration and data that is transmitted must be approved by the Customer before changes may be implemented.

No.	Requirement	Importance (O/H/M/L)	Describe
T 159	The Contractor must use the Customer's standard remote access solution for user support, troubleshooting, error correction, maintenance and updates of the system. **Note:** Currently Vendor access provides access to an access server with installed management/operation tools such as UltraVNC, WinSCP, RDP and SSH. Use of custom internal vendor access using solution such as 3G/4G/5G or ADSL modem, as well as software such as TeamViewer, LogMeIn, etc. is not permitted.	O	
T 160	The Contractor must use personal, identified users when using the remote access solution. Only personal user account can be used. Prior to using the remote access solution, the user must provide an official identification, see below. **Note:** Official identification; • For Norwegian citizens: – Norwegian F-number (Fødselsnummer) • For foreign citizens who lives in Norway and are employed by Norwegian Contractor: – D-number • For foreign citizens whom will use the Costumers remote access solution one of the following: – EU citizens, national ID in home country	O	

No.	Requirement	Importance (O/H/M/L)	Describe
	– Passport number – Social security number –Tax identification number – Or other national identification that will uniquely identify the user		
T 161	If access to software beyond standard installed management/operation tools such as UltraVNC, WinSCP, RDP and SSH is required, the Contractor should clarify and justify such requirements.	H	D
T 162	The system should have clear division between content in technical logs and other logs that may contain personal data, including encrypted logs. The Contractor is asked to clarify whether vendor access to production logs includes only technical data, and whether there is a risk of access to personal data, including encrypted data, in the event of such access.	H	D
T 163	The Contractor should perform technical support without a need to *automatically* obtain/transfer technical logs and example material via transfer of logs to the Contractor, for example via VPN. The Contractor must describe any needs and justify these.	H	D
T 164	The system should support the use of "*service access" or "service mode"*, where any personal data on patients is hidden/anonymised in connection with Contractor assistance.	L	D

6.3 Updates, upgrades and maintenance

For security and operational reasons it is important for Customer and the Customer's service provider that the system may be maintained and updated continuously, and that the system does not restrict how maintenance of underlying components and services in the Customer's technical platform may be carried out.

No.	Requirement	Importance (O/H/M/L)	Describe
T 165	The system should have mechanisms to reduce downtime in the event of updates, upgrades and maintenance. The Contractor is asked to describe such mechanisms, and describe which forms of changes to the system that typically entail downtime, and estimate normal downtime for the individual changes.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
T 166	The system should handle automatic rollout of security patches, service packs and other updates from the Contractor of the *operating system* on PC clients and servers. The Contractor is asked to clarify any deviations from this, and any restrictions due to certifications or the producer's self-imposed restrictions.	H	D
T 167	The system should handle automatic rollout of security patches, service packs and other updates from the Contractor of the *database platform and other third party components* used in the system.	H	D
T 168	Correction of corrupt values in the database should ordinarily take place while the system is in use.	M	D
T 169	The Contractor should describe assistance that is provided when restoring from backup.	H	D

6.4 Operational technical monitoring and logging

The Customer's service provider has established centralised solutions for the monitoring of the underlying components and services on the Customer's technological platform.

It is central and important for both the Customer and the Customer's service provider that systems established in the Customer's technical platform can offer operational and management-related technical log functionality at several levels.

This may for example be in the event of error situations or notifications related to hardware, operating system, services in the system, error events and other alerts that may be monitored and acted upon, to help avoiding error situations. Additionally, it is necessary to have good access to technical log data in order to produce information after error situations that are relevant to uncover the cause of the error, such that measures to prevent the error from reoccurring can be implemented.

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. It is preferable that system specific parameters that are to be monitored by the Customer's service provider are stored in the operating systems event log.

No.	Requirement	Importance (O/H/M/L)	Describe
T 170	The system should offer mechanisms and/or interfaces for operational technical monitoring ad error reporting.	H	D

No.	Requirement	Importance (O/H/M/L)	Describe
	The Contractor is asked to clarify any possibilities and limitations for integration with existing monitoring systems at the Customer's service provider. **Note:** This includes any standards and protocols that may be used, and how any notification to the system administrator may be carried out, if this takes place as a function in the system.		
T 171	The Contractor should clarify which components and services in the system that can be monitored and are recommended to monitor. **Note:** This may for example include: • Processes • Services • Queues • Integrations • File areas • Logs • Ports	H	D
T 172	The system's logs should clearly distinguish general information from specific errors that require follow-up and correction in the case of events in the system, such that error situations may be followed up. The Contractor is asked to describe how the system distinguishes information and errors in the system logs, and how this is categorised with regard to type of alert/error, severity, etc.	H	D
T 173	The Contractor is asked to clarify which type of information that is logged in the case of events in the system, for example error code, error cause, event category, component/module that has caused the event, date/time and other relevant information necessary to efficiently perform troubleshooting and error correction.	H	D
T 174	The system should have functionality to change the level of detail of logging. The Contractor is asked to clarify any support for this, and whether there is support for whether this may be done by the system's operations and management administrators, for example via a user interface.	H	D
T 175	All system errors should be logged in the operating system's standard event log with an understandable error code and error message.	H	

7 Dictionary

Terms	Description
.NET	Microsoft .NET framework for development
3G/4G/5G modem	A modem used to send SMS messages across the cellular network. This is not permitted to establish at the Customer.
ABAC	Attribute Based Access Control – Authorization through the use of policies that compile attributes belonging to users, for example the user's user ID, organizational affiliation and role. Also called policy-based access control.
AD	Active Directory – Microsoft's catalogue service for authentication and authorization of users in a Windows domain
ADSL	Asymmetric Digital Subscriber Line - line for data transfer via copper wire/telephone network
API	Application Programming Interface, interface for integration
Application	In this context, used as a term for software for end-users that is either installed on the user's workspace or distributed as a web application.
App-V	Microsoft App-V, standard for virtualization and streaming of applications.
Authentication	By authentication it is meant confirmation of the identity of users in the system.
Authorization	By authorization it is meant the accesses the user is given in the system, either for functionality, data or a combination of these.
Bluetooth	Wireless communication technology
Browser extension	Extensions/plug-ins that are used to customize or extend functionality in a browser.
Central log reception	The Customer's centralized log reception, including tools for log analyses, based on Splunk

Terms	Description
Change regime	By change regime it is meant the rules that apply for planning, notification and execution of changes to the Customer's infrastructure, including central data centers at the South-Eastern Norway Regional Health Authority. This includes all physical infrastructures such as power/cooling, physical cables, network, network services and server platforms (physical and virtual) that the offered solution depends on to produce the agreed services. All changes that the Vendor wishes to perform must be agreed and aligned with the Client's service provider, as work by the Client's service provider always takes precedence in the event of time slot conflicts. This is to prevent planned maintenance from failing during implementation with associated operational disruptions and risk of patient safety.
Citrix	The Customer's terminal server solution is based on Citrix
Cluster	See High Availability (HA) cluster
Control and approval	Manual quality assurance/peer control that must be possible to carry out as a feature in the system and logged.
CPU	Central Processing Unit - processor in e.g. client PC/server
CRUD	Create Read Update Delete - operations that are used in connection with data processing through user interfaces, databases and APIs.
CSV	CSV - Comma Separated Values - text file containing data separated by a comma or other character for separating fields
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.
DIPS	The Customer's electronic medical health record system, supplied by DIPS ASA
DIPS Arena	New version of the Customer's electronic health record system which there are plans to upgrade to
DIPS Classic	Current version of the Customer's electronic health record system
Directory service	See AD.

Terms	Description
DNS	Domain Name System - System service for translating between machine name and IP address
Docker	Solution for container services, see www.docker.com
EHR	Electronic Health Records, see DIPS
Enterprise application software	Purposed-designed software that takes care of specific functions within one or more fields. For example, LIMS or HER.
ERP	Enterprise Resource Planning, the customer's system for orders, inventory management and finances.
External data exchange	By external data exchange it is meant all data traffic that uses the Customer's infrastructure. This may for example be communication with centralized services for authentication and authorization of users, file storage, database or integration with other services.
F5 BigIP VPN	Standard provider access VPN is delivered using the BigIP product from F5
Federation	Compile identities and trust across domains. In this context, federation is used as a mechanism for central authentication.
FQDN	Fully Qualified Domain Name
GDPR	General Data Protection Regulation (EU) 2016/679, the EU's privacy regulations
GSM	Global System for Mobile Communications - standard for telecommunication for cellular phones
High availability (HA) cluster	Redundant cluster solutions established to ensure a high level of uptime and availability on established services
HL7	Health Level 7 – standard for exchange of messages with clinical and administrative information between health-related information systems
HL7 CDA	HL7 Clinical Document Architecture – standard for clinical documents
HTTP/HTTPS	HyperText Transfer Protocol (unencrypted)/HyperText Transfer Protocol Secure (encrypted) - communication standards for World Wide Web

Terms	Description
IAM	Identity and Access Management – System for identity and access control, including the use of services for federation and provisioning of users.
IEEE 802.1x	Standard for authentication of hardware connected to network. Must not be confused with standards for wireless networks (WLAN).
Integration	Interaction between systems
Interoperability	Interoperability can basically be described as the system's ability to interact with other systems under a common agreement and understood standards.
IPv4	Standard addressing protocol for connectionless communication in networks
IPv6	Latest version of the IP communications protocol that eventually will replace IPv4
Ivanti Workspace Management	The Customer's solution for administration and securing of Windows 10-based workspaces, formerly RES One Suite.
Java	Development language and framework
KDVH	Clinical Data Warehouse – The Customer's data warehouse solution for analysis and research, based on Oracle.
Kubernetes	Solution for container services, see www.kubernetes.io
LAN	Local Area Network, wired network
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
Manufacturer	"By "Manufacturer" it is meant the entity that has developed and supplied the system, where the Contractor is either: • identical to the Manufacturer, or; • distributor of the Manufacturer's systems "
MSI	Microsoft's format for installation packages

Terms	Description
MSMQ	Microsoft Message Queuing – Microsoft's solution for message queues, supported in most versions of Windows
N and N-1	Used in this context to describe the Customer's service provider's support for current (N) and previous version (N-1) of components and services.
NAC	Network Access Control – See IEEE 802.1x
NAS	Network Attached Storage
NAT/PAT	Network Address Translation/Port Address Translation – a method for mapping an IP address/Port range to another
NTP	Network Time Protocol, protocol and service for synchronizing clocks.
OeBS	Oracle e-Business Suite, see ERP
OS	Operating system
OUS-DOC	The Customer's current system for sterile supplies
PAS	Patient Administrative System, see DIPS
PDF	Adobe format for documents
Personal data	Any data about an identified or an identifiable physical person ("the data subject"); an identifiable physical person is a person that directly or indirectly may be identified, particularly using an identifier, e.g. a name, an identification number, location data, an online identifier or one or more elements that are specific for the mentioned physical person's physical, physiological, genetic, mental, economic, cultural or social identity.
PKI	Public Key Infrastructure - framework for issuing, managing and use of digital certificates
Provisioning	In this context a mechanism to automatically distribute and configure privileges for users in the system.
Pull print	The Customer's solution for centralized and secure printing, based on Canon uniFlow
RAM	Internal memory

Terms	Description
RBAC	Role Based Access Control – Authorization through the use of roles.
RDP	Remote Desktop Protocol – Microsoft protocol for remote control of Windows PC/server.
RES One Suite	The Customer's solution for administration and securing of Windows 7-based workspaces. See Ivanti Workspace Management.
REST	Representational State Transfer – a method to exchange data over http/https in connection with integration.
RHEL	RedHat Enterprise Linux
Risk assessment	A risk assessment is carried out when establishing new and changing existing systems at South-Eastern Norway Regional Health Authority. The risk assessment identifies risk and vulnerability in the system, as well as eventual risk-reducing measures and the person responsible for implementing these measures.
RJ45	Modular connection used for termination of network cable (Ethernet)
RS232	Serial port – interface for serial data transfer
SAML	Security Assertion Markup Language, open standard for exchanging data for authentication and authorization of users.
SAN	Storage Area Network
SCADA	Supervisory Control And Data Acquisition, system for operational technical monitoring.
SCCM	System Center Configuration Manager, Microsoft's tool for application distribution.
SCEP	Microsoft System Center Endpoint Protection – standard antivirus solution for client PCs at South-Eastern Norway Regional Health Authority.
SCIM	System for Cross-domain Identity Management-standard for exchanging information on user identity across systems and domains.
SDS	Central Datacenter
Secure print	See Pull print

Terms	Description
Sensitive personal data	See Special categories of personal data
SHKR	Central Main Communication Room
SOAP	Simple Object Access Protocol - Protocol for exchanging structured information over web services using XML
Special categories of personal data	"By special categories of personal data (formerly called sensitive personal data) in this context it is meant: • Data regulated by the General Data Protection Regulation article 9 • Health data that includes names, personal identity numbers or other identifying characteristics so that the data may be traced back to an individual • Health data where names, personal identity numbers and other identifying characteristics are removed and replaced with a serial number, a code, fictional names or similar, that refers to a separate list with the direct personal data, for example a requisition number, sample ID or similar."
Splunk	See central log reception
SSH	Secure Shell - Application protocol with encrypted communication for access to login and command line on remotely controlled client/server
SSL	Secure Sockets Layer – Certificate-based encryption protocol often used for web
SSO	• Single Sign-on
Storage solution	Collective term for various network solutions where data may be stored externally. Examples are file server (physical/virtual), NAS/SAN
TCP	Transmission Control Protocol – Secure communication protocol for applications that communicate over an IP network
The Customer	In this document, this is used as a term for the healthcare company Oslo University Hospital
The Customer's technological platform	The established infrastructure and ICT platform established at the customer, and which is owned, operated and managed by the Customer's service provider.

Terms	Description
TLS	Transport Layer Security, protocol for encryption of http-traffic
UDP	User Datagram Protocol – Non-secure communication protocol for applications that communicate over an IP network
UltraVNC	Application for remote control of client/server via a remote access solution
USB	Universal Serial Bus – interface for connecting peripherals
Vendor	In this document this is used as a term for those submitting tenders based on a request for tender from the Customer
VLAN	Virtual LAN - a method for logical separation of a network in broadcast domains
VMware	The Customer's virtualization platform for servers
VPN	Virtual Private Network. "Fjernaksessløsning for leverandører" established for Contractor access to the customer's network, is based on VPN
VPN Gateway	Regional WAN reception, the customer's standard gateway for the exchange of data over VPN

8 Attachments

Attachment 1 NIKT Arkitekturprinsipper i Spesialisthelsetjenesten

Attachment 5a Fellesregional kryptopolicy

Attachment 5b Fellesregional passordpolicy

Attachment 5c Sikkerhetsprinsipper og -krav for IKT-infrastruktur og applikasjoner