IT Technical Requirements

IT Overview

Background

Taunton and Somerset Foundation Trust (TSFT) currently has its own department dedicated to the management of IM&T within the organisation. IT Services department make sure the Trust's IM&T requirements are met. Procurement of new IT systems, whether by other departments or by IT services must be in line with both the IT Strategy and the overarching Trust Strategy.

In line with the NHS procurement guidelines, IT Services must be involved at all stages of IM&T procurement, installations, developments and projects. All changes must follow the IT Services change procedure.

TSFT expects suppliers to maintain and develop systems in line with advances in technology within reasonable timeframes.

We will consider environmental, social and economic issues when making new purchases.

Infrastructure

Currently IT services manage a mixture of systems, networks, servers, software and other IM&T products for the Trust. In brief, the following outlines a few key aspects of this infrastructure. This information is provided so that suppliers can fully understand the environment where the solution will deployed.

Suppliers should read and understand this and highlight any areas where there may be concerns that would affect the proposed solution.

Physical Network

Within TSFT there are currently over 7000 network devices, including but not limited to switches, routers, PCs, servers, printers, and IoT devices. These devices are all connected at minimum to a 100Mbps Ethernet port via Cat 5E cabling, the standard however 1Gbps over Cat6a. The Trust currently has approximately 35 communications rooms, which all have at minimum a 1Gbps link back to the core, but the standard is 1 x 10Gbps. The core network comprises of two large fully redundant core switches. These core switches are capable of managing network traffic at OSI layers 1, 2, 3, 4. The current preferred manufacturer for network equipment is Aruba/HP, but other manufacturers are used.

In order to provide resilience the core switches are hosted in separate parts of the Trust and there is an 80Gbps aggregated link between them. All areas of the network have been implemented to meet future requirements and we maintain capacity for future technical and physical upgrades. The core server network operates at 10GB.
Wireless Network

TSfT has an enterprise grade wireless network that covers the clinical areas and the majority of the rest of the site. The wireless network supports 802.11a/b/g/n covered areas, with 802.11ac currently being rolled out. 802.11ac wave 2 is currently under investigation and in early trials.

Servers

There are currently around 400 servers in operation within the Trust, which are located across two server rooms. These 400 servers currently host in excess of 350 applications systems, some of which are used throughout the county.

To maximise the efficiency of the infrastructure, in 2006 TSfT adopted a virtual server approach. TSfT utilises VMWare clusters, consisting of several Dell servers and Dell Compellent SANs. All new severs/systems will be expected to be compatible inside a virtual environment.

Only in special circumstances will a non-virtual server be considered. In this situation, a full explanation must be provided to the nominated IT lead. This explanation must be backed by performance data and evidence that reinforces any statement made.

Desktop Devices

Please note when referring to desktop devices we include PCs and Laptops. Currently the preferred supplier for desktop devices is Dell, with the current preferred models being the Optiplex 5000 series, and Dell E5000 series for laptops. There is however, a mixture of other manufacturers and models used. There are currently in the region of 3500 desktop devices within TSfT, that are managed by IT Services. All of these desktop devices are on a 7 year refresh program, in order to maintain system performance, reliability and hardware compatibility.

Mobile

TSFT supports both Android and iOS mobile devices. We currently support both company owned devices and BYOD devices, although BYOD is restricted currently to iOS. Both company and BYOD devices are managed by use of a Mobile Device Management (MDM) solution. The current MDM is Mobile Iron. This although to manage security policies, track devices, software configurations and deploy software to mobile devices.

Security

TSfT has an array of technologies used to protect the organisation from security threats. These include but are not limited to network monitoring, IDS/IPS systems, firewalls, Email
filters, Web filters and virus scanners. TSfT expects 3\textsuperscript{rd} parties to take all reasonable steps to make sure their products remain free from vulnerabilities and protected. This includes keeping up-to-date with 3\textsuperscript{rd} party dependencies used with the product e.g. web browser and operating systems.
Technical Requirements

Overview

TSfT must fully understand the solution and components.

Suppliers must provide any overview documents or architecture diagrams that will help TSfT understand the proposed solution.

Server Infrastructure

Hardware
As stated above it is expected that the system will run within a virtual operating system environment (OSE), however it is also recognised that occasionally this may not be supported.

Suppliers must provide hardware specifications for all parts of the system requiring physical servers. Specifications must include but not be limited to CPU Speeds, Memory Capacity, Storage Capacity, and Storage Performance.

Suppliers must provide information as to why Virtual OSE cannot be used.

Software

Operating System
Server components required to run on a Microsoft server operating system must be compatible with at least Microsoft Windows 2012 R2.

Other operating systems are acceptable as long as they are current and actively maintained by the operating system manufacturer.

All systems should be compatible with the latest major release of the chosen operating system within 2 years of its official release.

Regarding specific distributions of Linux the long-term supported release will be considered the latest major release.

All systems installed must be compatible of running within a virtualized operating system. The virtual operating system will be hosted on a VMWare cluster, to which all server-hosted software must be compatible.

Only in special circumstances will a non-virtual server be considered. In this situation, a full explanation must be provided to the nominated IT lead. This explanation must be backed by performance data and evidence that reinforces any statement made.

Suppliers must provide full details of the server operating systems the system is intending to utilise, compliance with the statements above and any other relevant information.
**Database Engine**

Any database engine that is required for the system to run must be compatible with the above operating system environments. The database engine must be capable of providing a backup file as part of a routine that does not require the system to be taken offline.

All database software must be compatible with the latest major release within 2 years of its official release and any product update of the same version within 3 months. The term update includes, but is not limited to Critical product updates, Critical security updates and Service Packs.

Suppliers must provide full details of the database engines the system is intending to utilise, compliance with the statements above and any other relevant information.

**Desktop Infrastructure**

**Hardware**

TSfT must understand fully any requirement for desktop infrastructure (PCs and Laptops) required to enable the system to function fully.

Suppliers must provide hardware specifications for any software component expected to run on desktop devices. Specifications must include but not be limited to CPU Speeds, Memory Capacity, and Storage Capacity.

**Software**

**Operating System**

Any desktop client software must be compatible with running on Windows 7 and Windows 10. Any desktop client should be operating system agnostic and be compatible with Mac OS X and Linux.

Supplier must confirm compliance to this requirement.

**Client Software Compatibility**

The proposed system/software must be compatible to run alongside the following software:

- Microsoft Office 2010 and Later
- Adobe Acrobat X and Later
- Microsoft Internet Explorer 11 or Later

**Mobile Devices**

TSfT is actively trying to mobilise IT use to better-fit workflows. Suppliers should have support for the system in part or fully on mobile platforms such as Tablets, Phones, PDA etc. Operation on mobile device should be agnostic and be fully maintained. Mobile software solutions should be ergonomic and be designed specifically design for which they were design. For example, a piece of desktop software made available on a mobile tablet that inherently was designed for mouse and keyboard inputs would not be considered ergonomic.
Suppliers must fully state any part of their system that is available on a mobile platform. Suppliers must fully state any compatibility requirements in able to deploy to a mobile platform.

**Other hardware**

TSfT needs to be informed of any hardware that is required to make the solution work. This may include but not be limited to Barcode Scanners, Printers, and Patient Monitors. TSfT need to understand fully the requirements for any such hardware.

Suppliers must provide full details of any other hardware required to make the solution operational. This should include support and purchasing responsibilities.

**Network Requirements**

In order to maintain system performance for the proposed solution over a term of 5 years. Requirements must take into consideration the following:

- Local Area Networks
- Wide Area Networks
- Wireless Networks
- Mobile technologies such as GPRS, 3G, and 4G

Suppliers must state in full any network requirements.

**Licencing**

**System Components**

TSfT must fully understand all licencing requirements for the solution. This includes but not limited to server operating systems, database engines, desktop software and 3rd party dependencies.

Suppliers must state in fully each component dependency, which requires licencing. Suppliers must state whether TSfT or the supplier is responsible for the procurement and management of each licence.

**Solution Licencing**

TSfT must fully understand how the solution is licenced and of the deployment and usage of the solution may affect licencing requirements.

Suppliers must fully describe the licensing structure for whole system to ensure all aspects of the system can be utilised, including details of all costs and any future liabilities for the Trust, for example, additional licences or system upgrades.

**Disaster Recovery**

**General**

Any solution must be robustly designed to avoid system failure. System should be designed using modular and scale out technologies so that components of the system may be implemented so that there is redundancy within the component. Systems should be designed to operate 24x7x365 and planned downtimes minimised. Systems should be
designed so that operating systems used can be patched without downtime. Systems should not require downtime for common occurring events such as Daylight Saving changes.

**Suppliers must state how the solution architecture meets this requirement.**

**Recovery**
Solutions must be design and implemented to meet the recovery needs of TSfT. The system must be capable of satisfying a Recovery Point Objective (RPO) of 0.5 hours as a minimum. The system design and implementation must be capable of meeting a Recovery Time Objective of 4 hours. It is expected that the supplier will work in conjunction with the local IT services department to meet these objectives.

**Supplier must state how the solution and the support of the supplier will help meet these objectives.**

**Business Continuity**
TSfT regard business continuity as a responsibility of the departments and/or business and not a specific responsibility of the IT services department. Departments must be able to operate during times of downtime, which may be planned or unplanned. System outages can be for any length of time but the expectation is no downtime planned or unplanned should exceed 8 hours.

**Supplier must state any process of components of the system that will assist the organisation during both planned and unplanned downtime.**

**Security**

**General**
The system security must be inherently robust and incorporate all features appropriate to safe-guarding data. The proposed system must not store any data that may be considered as sensitive and/or confidential on desktop devices, mobile or other devices unless encrypted. Data that is considered as sensitive and/or confidential must not travel across unsecured networks unencrypted. If there is any circumstance where the above might occur you are required to inform the IT lead.

The system must comply with all national security and confidentiality policies, which include, but are not limited to, Caldecott, Data Protection Act, and Health & Safety Act etc.

All data stored external to the system must be stored within the UK. All data will remain the property of TSfT and must not be transferred or made accessible to any organisation without prior consent.

Any system support must be carried out by individuals, which the supplier takes full responsibility for and is liable for.

**Suppliers must confirm compliance and detail any assurance process they undertake to meet these requirements**

**Access Controls**
System should invoke access control mechanism appropriate to protect the information stored within a system. Access controls must be able to accommodate different user roles and responsibilities. Access controls systems should be able to integrate with the Trust’s
Microsoft Active Directory. Ideally, the system should be able to support multiple user directory systems and/or support Microsoft Forrest and Domain Trusts to allow users to authenticate across domains.

**Suppliers must state the access control methods for all parts of the system and compatibility with integrating to the Trust’s Active Directory.**

**Antivirus**
All desktop devices, servers, and devices attached to the network must run the antivirus software chosen and managed by IT Services. Antivirus updates rolled out as soon as they are released.

The proposed system shall be fully compatible with enterprise grade antivirus software and in particular Kaspersky Antivirus.

Reasonable exclusions of directories of files and folders will be excluded as long as they are specific to the system.

**Suppliers must confirm compliance to this requirement.**

**Software Updates**
The system must be actively checked and patch against vulnerabilities. The system must be maintained in line with any 3rd party dependencies updates. 3rd party dependencies may include but not be limited to Operating Systems, Web Browsers, Java, .Net, redistributables.

**Suppliers must confirm compliance to this requirement.**

**Connectivity**
Connections between system components must be robust and secure. All components of the system that exchange information, where the information contains patient identifiable, or any form of sensitive data must be done using encrypted communication protocols. Connections between system components and other systems must be fully documented. This documentation must include a data flow diagram. Documentation must include but not be limited to descriptions of the system(s) and/or component(s), protocols, TCP/IP ports and the data that is exchanged. Details of the data must include full details of each data item/field that is exchanged.

**Suppliers must provide details of connectivity between solution components and intended linked systems.**

**Support**
**User support**
TSfT must fully understand the requirements for supporting the users or the system. TSfT has a dedicated IT service desk team, which is a single point of contact for users for IT incident and problem management.

**Suppliers must fully state requirements and or expectations regarding IT incident and problem management in relation to supporting end users. Please include details of how support calls/tickets will be managed in conjunction with the local service desk operated by IT services.**
Technical support
TSfT must fully understand the provision of technical support by the supplier. This includes the proposed service level agreements, assumptions in regards to roles and responsibilities and a support matrix.

Suppliers must provide full details of technical support available including on-line, helpdesk, telephone and on-site.

System Administration
TSfT must fully understand any system administration processes required on an ongoing basis so that the supplied solution remains working optimally and accessible to all those who need to use it.

Suppliers must provide full details of the methodology and process required for system administration and maintenance including all assumptions about roles and responsibilities.