County Durham and Darlington NHS
NHS Foundation Trust

Health Informatics

County Durham and Darlington NHS Foundation Trust

Warranted Environment Specification

(WES)

with you all the way

Version Control:

Version	Date	Changes from Previous Version	Changes made by
V1.0	10/03/2020	SER for remote access and non-trust devices	Peter McGuire
V1.1	19/08/2020	Add third party machines & defined W10 version	Peter McGuire
V1.2	25/08/2020	Added supplier acceptance boxes	Peter McGuire
V1.3	23/09/2020	Added notes box to each element, and updated standards link (e14)	Peter McGuire

1. Overview

The purpose of this document is to provide clear guidance on the Trust's computer, infrastructure, security and systems to all potential suppliers who will provide hardware, software, applications, systems and services to the Trust. The Trust's preferred position is to provide standard hardware and base software which the supplier can then build their system on, wherever possible.

Compliance with this Warranted Environment Specification (WES) is the responsibility of the supplier, and as such, forms part of the contract of engagement.

The supplier must confirm for each of the sections listed that the product they want to introduce to the Trust is Fully Compliant, Partially Compliant, Not compliant or not applicable. Explanations to partial or non-compliant must be provided.

Each element of the WES document contains a section for the supplier to express their confirmation of compliance to that element. If the supplier can't conform to a particular element then this should be explained in the notes section. If any section does not apply to the supplier's system or software than this should be indicated and an explanation given.

2. Minimum Endpoint Client Hardware Specification

The minimum computer, laptop and tablet specification is:

Windows devices:

- Intel Dual Core 2.0GHz
- 8GB RAM
- 100GB HDD
- On-Board Intel Graphics

Non-Windows devices

Android – all software intended for use on Android devices must be compatible with Android v6 (Marshmallow) and newer, and must be deployable using the MAAS360 MDM solution.

Apple – all software intended for use on Apple devices must be compatible with IOs v9, and must be deployable using the MAAS360 MDM solution.

SUPPLIER CONFIRMATION (element 1):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

3. Core Client Software

The following software are core and any new software must be optimised and compatible with:

- Windows 10 Enterprise – Latest "fall" release of Windows 10.
- Automatic deployment of Critical, Security and Important Microsoft Updates on a monthly schedule with automated restarts where required.
- Microsoft Internet Explorer 11 and above
- Microsoft Office Professional 2013 and above
- .NET – Latest Version
- Java – Version 8 update 202.
- McAfee Endpoint Security – Latest Version, with device encryption.
- Imprivata client agent to deliver user password self-service; fast user switching with smartcard authentication and Single Sign on.

SUPPLIER CONFIRMATION (element 2):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

4. Device management

The Trust utilises Microsoft System Centre Configuration Manager (SCCM) current branch to deploy all software to Windows computers. Along with the use of Group Policy within Active Directory to control user setting and configuration. Any software deployment must be performed as a package through SCCM, and the supplier will provide guidance on how to achieve this. The Trust does not support software which is only available through the Windows Store.

Every device connected to the Domain or network infrastructure must have a unique identifier, following the Trust naming convention, and where possible, text in the description field which identifies the location of the device.

For non-Windows devices, the Trust utilises two Mobile Device Management (MDM) solutions. Android devices are configured using a restricted Knox profile, and Apple device are managed through IBM MAAS 360. Any applications to be deployed on these environments will need to be supported by these two MDM systems.

SUPPLIER CONFIRMATION (element 3):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

5. End user Desktop Infrastructure

The Trust has a combination of traditional laptop, desktop and tablet computers along with a Citrix Virtual Desktop Infrastructure (VDi).

Physical computers are installed with Microsoft Windows 10, deployed using an SCCM task sequence

Citrix XenApp (latest version) delivers a 64-Bit Microsoft Windows Server 2012 R2 streamed desktop (RDS) to Dell Wyse Thin Clients running ThinOS Linux operating system. A hybrid of AppSense and Group Policy manage user and computer, profiles and policies.

XenDesktop is also available to deliver full VDI Windows 10 Enterprise using Windows server 2016 as the VDi server OS platform to deliver Windows 10 1909 experience.

All third-party computers Devices that are not supplied by the Trust must have a Security Exception raised by an internal sponsor and must have the Trust base image applied before any systems or applications are installed or configured. This is to ensure the correct version of the Windows operating system is applied to ensure the Trust remains in an effective license position; and to also ensure that the Trust has control over the deployment of security updates and patches.

SUPPLIER CONFIRMATION (element 4):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

6. Server and Datacentre

The system architecture is a combined infrastructure using a Cisco and DellEMC platform with Cisco UCS B200 based blade solutions providing the servers for the compute power and DellEMC Unity providing block storage and Isilon providing file storage.

The primary system site will be at the Trusts Tier 3 Data Centre connected with 10Gb links, with any need for replicated system components hosted at the Trusts secondary data centre. In the architecture, all components will be deployed in the primary locations (with space allocated in the secondary site for recoverability), physically separated to ensure data recovery in a disaster situation.

SUPPLIER CONFIRMATION (element 5):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

7. SAN Component

The shared storage will use the Trust's preferred array, which is currently DellEMC Unity All Flash. This is to provide the block storage for the virtual environments and shared across the production workloads for the Trust. This includes tiered storage for performance and RecoverPoint for replication.

For each datacentre, there are redundant Fibre Channel SAN switches and Cisco 6248 Fabric interconnects that provide connectivity between the SAN storage and the VMware Servers hosted on the computer platform.

File Storage is on EMC Isilon, replicated between datacentres and managed by the Trust.

SUPPLIER CONFIRMATION (element 6):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

8. Server Hardware Component

The server infrastructure provided by the Trust is Cisco UCS Chassis 5108 and B200 blade servers, combined with VMware ESXi 6.5.0 and vSphere software to enable a virtual server cluster.

The minimum virtual machine version supported by the Trust is eight (8), along with VMWare Tools Version 9.0.5 and VMXNET3 network adaptor profiles.

SUPPLIER CONFIRMATION (element 7):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

9. Minimum Server Specification

The minimum server specification is:

- Dual CPU Intel Dual Core 2.0GHz
- 8GB RAM
- 100GB HDD

SUPPLIER CONFIRMATION (element 8):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

10. Core Server Software

The following software is core and any new software must be optimised and compatible with:

- Windows Server 2012 R2 or later
- Microsoft SQL 2012 R2 or later

- Automatic deployment of Critical, Security and Important Microsoft Updates
- .NET – Latest Version and above
- Java – Latest Version and above
- McAfee Endpoint Security 10.6

SUPPLIER CONFIRMATION (element 9):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

11. Datacentre and Server Resilience

The Trust uses VMWare High Availability (HA) and Distributed Resource Scheduler (DRS) to protect virtual machines and manage resources, ensuring that in the event of a host failure they are recovered quickly and the relevant resource is correctly assigned. RecoverPoint for Virtual Machines protects the virtual servers to the secondary datacentre as required during failover instances.

EMC Avamar DataDomain is the backup solution within the datacentres with cross-site replication.

SUPPLIER CONFIRMATION (element 10):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

12. Networks

The Trust is responsible for providing the network capabilities between the Trust sites and all connected clients within using Cisco equipment.

The Trust provides 10Gbps redundant links between the Trust primary site and secondary site for successful synchronous replication.

The trust is responsible for the operation and maintenance of the wired and wireless network. Any connection to the network, wired or wireless, should be approved by the trust network team in advance and be compatible with existing protocols and security configured on the network. In the case of any network devices not managed by the trust no equipment should be connected without a full risk assessment by the trust network team. Insecure protocols such as Telnet and http must be disabled along with unused services and a SNMP V3 read username and password should be provided to the network team for monitoring purposes.

Any equipment configured for call-home or remote monitoring must use secure communications methods and utilise the trust proxy servers for internet connectivity.

SUPPLIER CONFIRMATION (element 11):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

13. Firewall and Internet Proxy

The trust infrastructure prevents devices from connecting directly to the Internet. All firewall requirements for servers to connect to entities outside of the Trust control should be clearly documented and as restrictive as possible while still allowing expected functionality.

All client software should be able to work through an explicit proxy as client machines are not allowed out directly through the trust firewall.

Any system making use of an internally or externally hosted web portal must only use the HTTPS protocol.

SUPPLIER CONFIRMATION (element 12):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

14. Security

Where possible all Desktop, Laptop and Tablet devices must be CDDFT issued, configured and maintained to the current Trust standards.

When this is not possible or when the device has embedded computer hardware or software then the following specification must be adhered too, unless agreed with the CDDFT Health Informatics Change Advisory Board.

Any agreement should be obtained, not only before the procurement process is completed, but also before any trial equipment is used within the CDDFT campus or with any CDDFT Data.

All supplied operating systems included embedded operating systems must be compatible with and allow the installation of the Trusts IT security protection software. Currently McAfee Endpoint 10.

All devices that are to be connected to the Trust Data or Telephony network and any devices that may contain any Trust sensitive data must only run software and operating systems for which security patches are made available. All currently available security patches must be applied on a schedule appropriate to the severity of the risk that they mitigate. This will include the ability to automatically receive and install all critical operating system updates at point of operating system vendor release.

The supplier should be able to guarantee that when the expected life cycle of the device hardware is greater than the expected life cycle of the operating system or supplied software then there will be an upgrade option which will be presented to CDDFT at the start of the procurement exercise.

All unnecessary software and operating system services should be disabled and prevented from auto running, and only CDDFT approved client software that is essential to the specified purpose of the device should and will be installed.

All devices must where appropriate support Encryption both at disk level and when transporting data, this is for wired and wireless connections and is with particular reference to insecure services such as Telnet, FTP, SNMP, POP, and IMAP which must be replaced by their encrypted equivalents. When disk encryption is performed by the supplier then all encryption/decryption keys must be made available to CDDFT.

All devices must have a local CDDFT login with administrative rights.

All devices not managed by CDDFT IT must be patched with the latest security and critical updates on a monthly basis unless specifically agreed with the IT Security Manager at CDDFT.

When authentication to the device is not managed by CDDFT then Password/Passphrase complexity must meet Trust Standards. For high privileged accounts then these passwords should include 15 characters of upper and lower case as well as special characters and numbers. CDDFT ICT and Systems support services must be made aware of all locally created user and system accounts.

Suppliers should also be aware that CDDFT do not allow the use of local administrator accounts on any client device and suppliers should provide a list of all services with the relevant privilege requirement so that CDDFT can adhere to its least privilege policy.

Remote access to systems is provided on an on-demand basis, with planned work by remote being achieved by the supplier asking for access to be granted in advance of the activity. Arrangements can be made for remote support through a shared desktop service - such as LogMeIn; or via a dedicated remote access link over the HSCN network. A Security Exception needs to be submitted by an internal sponsor for any remote access arrangements.

All suppliers must either demonstrate regular vulnerability testing of any managed and supplier maintained equipment or allow CDDFT to test as part of our vulnerability management plans. These tests would take place with support from the supplier and at a time convenient with the service utilising the devices.

CDDFT do not allow any media fixed or removable that does or may have contained any CDDFT sensitive data to leave its control without that media being encrypted or wiped and certified using a UKAS accredited method. When maintenance or repair of devices is required to take place outside of CDDFT premises then assurance must be given by the supplier that this has been completed before the device is removed from site.

SUPPLIER CONFIRMATION (element 13):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

15. Standards

Overview

1. The Prime Contractor shall, and ensure any subcontract(s) with its subcontractor(s) observe and keep track of NHS and industry standards as such standards evolve and emerge and are issued by NHS England or any of its authorised bodies including but not limited to NHS Digital and Standardisation Committee for Care Information. The Contractor shall include and ensure in all appropriate subcontracts with its subcontractor(s) that the subcontractor will use these standards in the development of future releases of the Services.

The standards are listed:
https://digital.nhs.uk/about-nhs-digital/our-work/nhs-digital-data-and-technology-standards/framework

and

https://theprsb.org/

2. The Contractor acknowledges that the definitive source for NHS and social care standards and amendments to them is the Standardisation Committee for Care Information (SCCI). The definitive source for British (BS), European (CEN) or International (ISO) standards and amendments to them is the British Standards Institution (www.bsigroup.co.uk).

3. Unless otherwise agreed by the Authority, the Contractor shall and include in any subcontract(s) with its subcontractor(s) that the solution comply with latest approved versions of the standards in this Section without further charge to the Authority.

4. If the Authority requires the Contractor to implement additional standards, then this shall be requested using the Change Control Procedure.

Release Management

5. The Contractor shall include and in any appropriate subcontract(s) with its subcontractor(s) that it assesses new and amended Authority standards as part of the requirements definition for a new release. The release definition shall detail the standards the new release will comply with and indicate where it will not.

6. The Contractor shall and include in any appropriate subcontract(s) with its subcontractor(s) that it is stated the compliance of the new release with the **relevant** Compliance Requirements given below.

7. Should the Contractor reasonably believe that adoption of any standard conflicts with any other obligation under this Agreement, then the Contractor shall request direction from the Authority.

8. Any other variation from the standards must be agreed by the Authority as part of the design and development of an update to the Services. The variation must be explicitly stated and agreed by the Authority.

Audit

9. The Contractor shall on reasonable request provide the Authority with documents showing how standards have been implemented in the provision of the Services.

10. If the Authority finds that the Services do not comply with a standard where compliance has been agreed as part of the release then this will be raised as a defect.

Approved Standards

11. The Contractor shall and include in any subcontract(s) with its subcontractor(s) that the solution complies with the **relevant** standards from those stated below for the provision of the Services.

12. The Contractor shall include and in any appropriate subcontract(s) with its subcontractor(s) that the solution complies with the GovTalk Technical Standards Catalogue, available from the Cabinet Office website (http://www.cabinetoffice.gov.uk/govtalk.aspx). In the case of conflict, the standards approved by the ISB take precedence over those in the Technical Standards Catalogue.

Draft Standards

13. The Contractor acknowledges that a number of standards are in development. The Contractor shall and include in any subcontract(s) with its subcontractor(s) that the solution complies with the **relevant** standards once they are approved and comply with the timescales for inclusion of such standards

SUPPLIER CONFIRMATION (element 14):

Fully Compliant	☐
Partially Compliant	☐ (complete the notes section for this element)
Non-Compliant	☐ (complete the notes section for this element)
Not Applicable	☐

Supplier notes:

16. SUPPLIER COMMITMENT

The supplier considers this Warranted environment specification as a component in their contract with the Trust and has stated their compliance or otherwise with each of the 14 elements.

Signed (on behalf of the supplier) Signed (on behalf of the Trust)

_____ _____

Name _____ Name _____

Job Title_____ Job Title_____

Date _____ Date _____