Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

HSE OoCIO

Technical Standards

Version 3.00

October 2017 – December 2017

Contents

Version	Date	Reason	Author
Original release: V1.1	Mar 2009	Need for ref doc	Mike McCrohan
Draft 1.2	Jan 2010	Remove product specific references	Mike McCrohan
Version 1.2	June 2010	Publish	Mike McCrohan
Version 1.2.1	July 2010	Update date details P3	Mike McCrohan/B Flynn
Version 1.2.2draft	Mar 2011	Mod 2.4.7 spec bps ideal	Mike McCrohan
Version 1.3	Apr 2011	Draft € Version	MMcC
Draft 1.4a	June 2011	Circulation for comment Various inputs	Pat Thornton John Lehane Aidan Plunkett Tadgh Buckley Mike McCrohan
Updated to full Version 2	July 2011		Pat Thornton
Version 2.01	Dec 2011	Minor tidy up edits – remove "draft"; Renumber; Edit User ID	MMcC
Version 2.02	Jan 2012	Correct anomaly User ID section	Chris Plunkett Mike McCrohan
Version 2.03	Feb 2012	Correct error User ID section	Mike McCrohan
Version 2.04	Apr 2012	Make Browser statement 5.1.8 explicitly unambiguous	Mike McCrohan Chris Plunkett
Version 3.00	Oct 2017	Initial 2017 Version	John Lehane Darren Finn Nicholas Power Richard Keating

2 Infrastructure Standards for Application installs in the HSE

This document indicates the Technical Standards governing the deployment of Business and Clinical computer applications within the HSE. It is designed to form part of the "brief" for vendors at the RFP/RFQ stage of any software project or system deployment, whether nationally or regionally.

The standards will form an integral part of the procurement process and vendors / potential vendors will be provided with copies of the standards as part of that process

HSE OoCIO will be represented on all significant National and Regional project teams to assist in implementing the standards. Any proposed deviation from the standards will be addressed through that representative.

Local projects will also involve relevant Operations and Infrastructure representatives on their project teams/sub groups (as required) and address any issues through that forum

The Head of Technology, or his/her designate, must sign off on technology component of the project prior to contract award.

2.1 Scope

These technical standards are valid up to Dec 2017 at which time they will be reviewed to update certain specifics as Operating system version(s) etc.

3 Servers

The standards cover Business/Clinical Information System Applications and are not intended to cover specific-purpose Medical Devices / Clinical Equipment.

Note: Medical devices or Clinical Equipment refers to equipment directly involved in patient care or treatment. Such devices or equipment are governed by specialist configuration and maintenance regimes. ICT will deliver network ports for connectivity of such equipment, but will have no responsibility beyond that.

3.1.1 Any proposed ICT solution should operate from the National HSE Data Centre. Where this is not the case OoCIO sanction will be required before final approval is given for any solution.

3.1.2 Restricted management and administrative remote access to centrally hosted servers should be via the use of the existing KVM technology only. Virtual Servers may be accessed using VMWARE or Microsoft Management Tools provided by the HSE.

3.1.3 Currently Windows Server 2012 R2 is the preferred 64bit server operating system. All other operating systems will be considered on their own merits with special emphasis placed on how easily they will integrate with the rest of the HSE infrastructure.

3.1.4 Server operating systems must be currently supported by the operating system vendor.

3.1.5 Operating systems are routinely upgraded to take account of the latest OS patches or emergency fixes and any proposed solutions should support these updates and also allow for minimal interruption to service during this update period; Vendors should commit, at no cost to the HSE, to keeping their application qualified against the operating system's vendor's current service pack and monthly/emergency patch levels.

3.1.6 All servers must be capable of being housed/racked in an industry standard 42u cabinet

3.1.7 The HSE reserves the right to procure from existing supplier agreements the hardware infrastructure requirements to support any new proposed solution.

3.1.8 Any proposed solution should be certified to operate on a virtual server environment.

3.1.9 The proposed solution should support at a minimum 32 bit architecture running on a 64bit Operating System

3.1.10 Servers should avail of, and integrate with, SAN-based storage where available.

3.1.11 Servers should integrate with enterprise SAN-based backup structures where available. Failing that, they shall be equipped with an adequate backup mechanism. Backup procedure, schedules and retention requirements must be clearly defined by the vendor in conjunction with the OoCIO

3.1.12 Servers should be capable of integrating with fibre fabric high speed SAN switches.

3.1.13 Physical Servers should be equipped with a minimum of four 1Gb NIC's complying with IEEE 802.3 standards to run Ethernet networking in a TCP/IP based environment. Support for 10 GB networking is avaialble in the major HSE Data Centres via Converged Network Adapters with connections via Twinax cabling.

3.1.14 Servers must be allocated IP addresses as specified by HSE OoCIO.

3.1.15 Servers should comply with relevant HSE naming conventions.

3.1.16 Servers must integrate into the HSE's network domain/Directory Service structure and single national domain

3.1.17 Servers should integrate with and run the HSE's current Antimalware software (McAfee). Where any proposed solution requires exemption from some aspects of the AV process then these must be clearly identified.

3.1.18 For applications implemented on Windows Servers, all application services should run as a Windows services and should not require continuous logon to the console to operate. Similar principles should operate on other operating systems.

3.1.19 The application vendor shall state brand neutral minimum hardware requirements for a server to run the application in terms of:
RAM, Disk Space, Processor, Other. (This should be specific to the HSE's needs and not based on a recent deployment elsewhere).

4 Database

4.1.1 The preferred Database Management Systems shall be ANSI standard SQL or other industry standard RDBMS. Other DBMS systems require explicit signoff by relevant OoCIO staff.

4.1.2 The vendor will be required to provide a full database schematic as part of the solution delivery.

4.1.3 Any database backup routines should not involve system down time.

4.1.4 Database recovery should be available at various levels i.e. up to a certain point in time or transaction.

4.1.5 The number of users requiring elevated/administrative levels of access to the database must be kept to a very minimum. On-going System Administration access by non Database Administrators or Superusers should not be a requirement on an on-going basis.

4.1.6 Access to database should be granted via the set-up and central management of agreed database roles and any local/integrated users required must use passwords that comply with the HSE Password Policy.

5 Clients

5.1.1 Any proposed solutions should support system failovers and should automatically recover from such a failover. There should be no loss of data during this failover, users logons should be preserved and they should not be required to log back into the system.

5.1.2 The proposed solution should operate within a DHCP served environment.

5.1.3 The proposed solution should use DNS and FQDN for name resolution and not rely on IP address based application access.

5.1.4 The client interface or application of any new proposed solution should be certified to operate on a virtualised server environment.

5.1.5 Browser based application deployment is preferable and should not require client side storage.

5.1.6 Where the proposed solution operates with thin-clients, those clients should run on Citrix Xen App 6.5 Enterprise and above without requiring special client-side modifications.

5.1.7 Where the proposed solution operates via web-browser it should not use version-dependant Java applets, and should require no special device drivers or configurations.

5.1.8 For web based solutions there should be a minimum workstation footprint and information should be ascertained on the quantity and level of Java or Active-X applets downloaded at session initiation and thereafter. A client load of less than 25Kbit/second per user is considered best.

5.1.9 The application, if web-enabled, should operate properly with standard configurations of all of the following network Browsers:
Microsoft IE 11 and above,
Firefox ESR 52 and above,
and should also conform with W3C DFA (Designed for all) Standards. Any peripherals required should also support these browsers.

5.1.10 Industry standard desktop workstations will be procured through the current HSE/OGP Framework/Competition process.

5.1.11 The proposed application must be cognicant of the fact that Windows 7 32bit is the HSE's predominant desktop workstation operating system currently deployed. Windows 10 64 bit build 1703 [15063.632] must also be supported.

5.1.12 The desktop workstation should integrate with and run the HSE's current Antimalware software (McAfee).

5.1.13 Any special client-side software required must be specified in detail in any proposed solution and subsequently approved by the HSE OoCIO.

5.1.14 The supplier of any proposed solution should state the minimum hardware requirements for a workstation to run the application.

5.1.15 Client specification should include areas as RAM, Disk Space, Processor.

5.1.16 Client software should support a pull/push patching environment

5.1.17 Computer applications should authenticate against an Active Directory, allowing for single sign-on.

5.1.18 Any proposed solution should not require any specific drive mappings to function or use file shares with access rights and folder structures not managed by the application.

5.1.19 On end user workstations, users should not require local or domain administrator access or require any significant alteration to registry key permissions.

5.1.20 The HSE reserves the right to install remote monitoring clients on any machine on the network for monitoring by a central monitoring service. Examples of such software include SCOM, SCCM, Lansweeper, Landesk, Altiris and Nagios.

5.1.21 Suppliers must agree to comply with the HSE remote access mechanisms and policies.

6 Printing

6.1.1 Application printing should be via network attached printers using standard TCP/IP networking attachment and protocols.

6.1.2 Printing should be via dedicated print servers where such servers are in place.

6.1.3 Standard manufacturer or Universal Printer Drivers should be supported.

6.1.4 Monochrome laser printers should be the default specification for any printer requirements. Where this is not the case then detailed information will be required to justify alternate detailed output – specific printing requirements should be detailed.

7 Interfacing / Messaging

7.1.1 Applications in the medical imaging areas shall be DICOM compliant and enabled and definition of required DICOM Classes should be sought.

7.1.2 Inter application communications shall be based on HL-7 (currently version 2.4 with XML encoding), XML and CDA release 2.

7.1.3 Where applicable, applications should be compliant with the Web Services Interoperability Group (WS-I) Basic Profile, version 1.1, that establishes core Web services specifications (SOAP, WSDL, UDDI, XML Schema, HTTPS) that should be used together to develop interoperable Web services.

8 Local Area Networks (LAN's)

8.1.1 Client PC's or local applications servers must connect to the local site LAN without creating "islands of networking".

8.1.2 Where a new application is to be deployed in a reconfigured department or newly fitted out location the following general guidelines must be followed:

8.1.3 ICT Operations and Infrastructure together with Project Managers shall advise regarding locations and disposition of users within a new or existing location in order to determine resulting costs of fit-up or re-layout.

8.1.4 Client offices shall be equipped with a minimum of one 2-gang RJ45 Cat-6 outlet per workstation. A spare 2-gang outlet shall be available per each one- or two workstations.

8.1.5 Data & Voice will be delivered on a structured cabling solution in line with the HSE's Standard Cabling Document.

8.1.6 Horizontal cabling shall be Cat-6, installed by a properly accredited installer.

8.1.7 Horizontal cabling shall be terminated in a dedicated hub in a secure location. For larger sites this shall be a locked room with restricted access, and equipped with HVAC and UPS as appropriate.

8.1.8 A separate document defines, in more detail, the telecommunications cabling standards for new installations.

9 Networks – Wide Area

9.1.1 The network access to all systems in the data centre will be over the HSE's own virtual private network (VPN) called the 'National Health Network' (NHN). Where agencies do not have direct connectivity to the NHN they will be able to connect to NHN in consultation with HSE ICT.

9.1.2 Local and wide area network bandwidth requirements should be clearly documented before any proposed solution is considered for implementation. This includes a profile of client-related network traffic during typical work sessions.

9.1.3 The supplier of any proposed solution should agree to work with the HSE OoCIO to create baseline bandwidth usage measurements for their application on the WAN (NHN) prior to deployment.

9.1.4 Most national applications will have to operate over sub 5Mb connections. Exceptionally bandwidth-intensive applications such as Radiology imaging or certain Cardiology applications will require special consideration.

10 Security

System security and related issues are governed by the following policies.

ICT Strategy

Information Security Policy

I.T. Acceptable Use Policy

Electronic Communications

Policy Mobile Phone

Device Policy Password

Standards Policy

Encryption Policy

Access Control Policy

Remote Access Policy

Third Party Network Access Agreement

Service Provider Confidentiality Agreement

Data Protection Breach Management Policy

Internet Content Filter Standard

While consideration should be given to the above security related policies the following section re-iterates some of the key requirements in relation to security which any proposed solution should adhere to:-

10.1.1 Support authentication of individual users and not just groups

10.1.2 Have controls in place to ensure that individuals can be held responsible for their actions

10.1.3 Not store passwords in clear text or in any easily reversible form

10.1.4 Provide for some sort of role management, such that one user can take control of the functions of another without having to know the other users password

10.1.5 Provide a logging facility that should be capable of recording all failed and successful login attempts

10.1.6 Allow for passwords to contain a combination of letters (both upper & lower case), numbers (0-9) and at least one special character (for example: “, £, $, %, ^, &, *, @, #, ?, !, €)

10.1.7 Not allow passwords to be left blank

10.1.8 Support the requirements for passwords to be changed at least every 90 days

10.1.9 Transmission of confidential and personal information through a public network (for example the internet) to external third parties must be encrypted or be transmitted through an encrypted tunnel (for example a secure Virtual Private Network (VPN))

10.1.10 All confidential and personal information transmitted around existing wireless networks must be encrypted using WEP (Wired Equivalent Privacy) or better. All new wireless network installations must be encrypted using WPA (Wi-Fi Protected Access) or better

10.1.11 Where encryption is required, then

10.1.11.1 The minimum encryption key length must be 128 bits or better

10.1.11.2 If using Symmetric Key Encryption Algorithms, which is a class of encryption algorithm in which the same key is used for both encryption and decryption of the information, it should support the Advanced Encryption Standard (AES) and Triple Data Encryption Standard (Triple DES)

10.1.11.3 If using Asymmetric key algorithm, which is a class of encryption algorithm in which two different keys are used: one for encrypting the information, and one for decrypting the information (Public-key encryption), the Digital Signature Standard (DSS), Rivest, Shamir & Adelman (RSA) or Elliptic Curve Digital Signature Algorithm (ECDSA) should be supported.

10.1.11.4 Encryption protocol standards which define the rules governing the use of encryption should support any of the following: IPSec (IP Security), SSL (Secure Socket Layer), SSH (Secure Shell), TLS (Transport Layer Security) or S/MIME (Secure Multipurpose Internet Extension)

10.1.11.5 Encryption key management should ensure that key management be fully automated, private keys must be kept confidential and keys in transit and storage must be encrypted

11 Licensing

11.1.1 Special consideration needs to be given to all software license requirements for any existing or proposed solutions and suppliers will be required to provide a full account of all software license requirements in any submissions made. Such submission must detail servers, any middleware or supporting subsystems, any client side licenses and any other collateral requirements resulting from deployment of the system**.** Questions on same can be addressed to samadmin@hse.ie

11.1.2 The HSE licenses its data centres on a per CPU/Core basis and any proposal should identify any costs of deploying systems on different processor models based on number of cores or sockets present in servers if any such criteria exist

12 Standardising User ID

A new ID convention has been adopted by the HSE for all computer applications other than email. This new ICT standard is called the Unique User Identifier (UUID) an is in the format of

FirstnameLastname[n] (examples: JohnSmith, MaryMurphy, etc.)

The new UUID is limited to a maximum of 20 alphanumeric characters, without spaces, dots, underscores, etc. It is not case sensitive.

In order to differentiate between people who may share common names such as the examples above, a numeric [n] may be used: JohnSmith5, MaryMurphy3 etc.

The UUID provides a viable single unique ICT user identification for HSE use while allowing for a degree of backward compatibility with systems developed on some legacy systems.

The UUID is already in use on some national applications, most notably iPMS and NIMIS.

12.1.1 Email Identifier or UPN

One variant to the standard is that which applies for E-mail.

In this case a dot (period/full stop) is used as a separator between first and last names. Otherwise the UUID standard applies. Thus, taking the examples above the email addresses become:

John.Smith5@hse.ie, Mary.Murphy3@hse.ie etc.

12.1.2 How to get a Unique User ID (UUID)

Anyone already assigned and using a National HSE email identifier will automatically have had a UUID generated for them in the process.

Generation of a new UUID for use when accessing an application is achieved by contacting the local ICT department who will manage the process on their behalf. In the case of new applications the project manager may arrange for this to be done on behalf of the new application users.