University Hospitals of Leicester NHS
NHS Trust

IM&T Directorate

Data Network Security UHL Policy

Approved By:	IM&T Security Board
Date Approved:	21 December 2009
Trust Reference:	**B48/2009**
Version:	2
Previous version:	1.5 June 2016 Policy and Guideline Committee
Author / Originator(s):	IM&T Head of Design Authority
Name of Responsible Committee/Individual:	Chief Information Officer
Latest Review Date	17 July 2020 Policy and Guideline Committee
Next Review Date:	March 2024

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

Revision History

March 2005	V1.0	Original prepared by IM&T Security Manager
Nov 2009	V1.1	Prepared document using original unapproved version 1
Jan 2009	V1.2	Used standard document template
Jan 2014	V1.3	Reviewed, references to EMIAS removed, titles changed etc. Extra rules added for account revocation responsibilities.
July 2014	V1.4	Modified to comply with PGC formatting
March 2015	V1.5	Modified and re-published due to technical content
July 2020	V1.6	Updated password length

KEY WORDS

Access to electronic systems

Access to computer systems

Login to computer

Authentication

1. INTRODUCTION And Overview

This policy sets out the standards to be employed in the management of data network components used at UHL, these components are used to transfer digital data and voice communications in a secure manner.

References to the MBP (Managed Business Partner) include IBM and its sub-contractors e.g. NTT Data Services

The management of data is summarised in the following statement from the UHL privacy board:

Confidentiality – ensuring that sensitive and/or business critical information is appropriately protected from unauthorised 3rd parties and can only be accessed by those with an approved need to access that information

Integrity – ensuring that information has not been corrupted, falsely altered or otherwise changed such that it can no longer be relied upon

Availability – ensuring that information is available at point of need to those authorised to access that information

2. Policy Scope

The data network consists of the hardware and software connected together to allow communications between computer systems both internal and external to UHL. The many components of the data network include network switches, hubs, routers, cables, firewalls etc. the complex configuration of these components is achieved using software tools.

This document sets out the University Hospitals of Leicester (UHL) NHS Trusts Policy and Procedures for the management of electronic data networks used within its premises to connect data and voice systems, these networks connect internally and externally using a variety of technologies.

The intended audience for this policy are primarily those responsible for establishing and maintaining electronic data and voice networks for, or on behalf of UHL and its partner organisations

This policy covers the following areas:-

Access to the Data Network:

- Physical security of Data Network components
- Electronic security of Data Network components
- Resilience and capacity management

The Data Network consists of:

- The Metropolitan Area Network (MAN), fibre cabling connecting the three hospital sites, routed separately for resilience by the supplier.
- Three Local Area Networks (LAN's), a mixture of fibre and copper cabling within the hospital campuses.
- A large number of network hardware devices including cores, switches and firewalls on each site.
- External networks connected to UHL i.e. HSCN, Virgin Media providing connectivity to the Internet, the MBP, NHS etc.

This Policy applies to all users of electronic information to include:

- Trust employees
- Honorary trust members
- Employees of temporary employment agencies
- Vendors, business partners, contractor personnel and functional units regardless of geographic location.

- This policy applies to all electronic networks used by UHL that are used to transfer data and voice electronically, owned by the Trust or entrusted to the Trust by internal and/or external customers.

The standards detailed in this policy are mandatory and are derived from mandatory NHS security standards.

Compliance with this policy is submitted as evidence to the NHS Information reporting via DS&P (Data Security & Protection) toolkit and that will feed into CE+ (Cyber Essentials Plus), a mechanism used by the NHS to ensure best practice is being used to securely manage information

This policy provides assurance to the following requirements laid out by NHS Digital to comply with the Cyber Essentials Plus requirements –

Compliance with this policy is submitted as evidence to the NHS Information reporting via DS&P (Data Security & Protection) toolkit and that will feed into CE+ (Cyber Essentials Plus), a mechanism used by the NHS to ensure best practice is being used to securely manage information

The IT Data Network is a vital component for the smooth running of most IT systems within the UHL, allowing users to access both clinical systems (e.g. HISS and PACS) and non-clinical systems (e.g. email and finance) It is therefore essential that a robust framework is developed to ensure a secure network infrastructure throughout the UHL.

2 DEFINITIONS AND ABBREVIATIONS

A.C.L. (Access Control list) is a list of users which is presented as a group, authorised to access specific electronic data. This is a common technique used in

systems management to handle large numbers of people accessing data, group membership grants access to data which would otherwise be denied to unauthorised users.

Access control system is a method of securing access to electronic data stored on a computer system, a system user is authorised to access data using the rules specified in the Access Control System.

Active Directory is directory based architecture provided by Microsoft to manage the components of a diverse network such as the one used at UHL, this allows the granular management of access control to thousands of personal computers and servers.

Administrator / supervisor are terms used to describe a 'super user' on a computer system; this role is normally used to manage the system users and access to data stored on the system

Authentication is the correct verification of an end user by virtue of a login name and password or a smart card and pin number.

Authorisation is the allocation of access to electronic data dependant on successful authentication, usually by group membership after login is successful to the relevant computer system.

The Change Approval Board (CAB) is a process group within IM&T which monitors and approves or declines change requests for the IT Infrastructure at UHL, this is a formal procedure to prevent unstructured changes which may result in instability.

Electronic Systems are essentially computer based technology which can be as diverse as database servers, personal computers, analysers or tablet devices.

Generic User. is a term used to describe an anonymous person who shares a login identity to access a system; these are frequently used in areas where login times are excessive and may adversely affect patient care. The use of Generic logins are no longer supported as they represent a threat to secure access of data, access is anonymous therefore the user cannot be verified

IM&T Design Authority is a collective group of decision makers whose members are made up from the MBP and UHL IM&T, this group makes decisions regarding the technical direction and standards used in IT at UHL

Information Asset Administrator (IAA) is someone within the organisation who manages a computer system containing data, both hardware & software can be considered an information asset. At UHL the Information Asset Administrator would normally be the System Manager of one or more systems.

Information Asset Owner (IAO) is someone within the organisation who is responsible for the overall management of the information assets used by their part of the business, in UHL this would typically be the head of a division or department.

Managed Business Partner (MBP) is the company contracted to work with UHL IM&T to deliver the IT services to the organisation

NHS Digital is an organisation which regulates Informatics on behalf of the NHS

Root Access describes the ability to access all services and data on a file server, the 'root' user is normally found on servers using the UNIX operating system. Access to the 'root' username should be strictly controlled as it presents a threat if not used correctly.

Senior Information Risk Owner (SIRO) is someone designated to:

- Be responsible to Lead and foster a culture that values, protects and uses information
- Be responsible for the success of the organisation and benefit of its patients
- Own the organisation's overall information risk policy and risk assessment process, test its outcome, and ensure it is used.
-

(The Chief Information Officer is currently the SIRO at UHL)

Service Account is a pseudo-user account designed to be used to authenticate between systems in an automated way, this type of account normally has elevated privileges.

S.I.E.M. (**S**ecurity, **I**nformation & **E**vent **M**anagement) is a system for recording and archiving event information for recall at a later date, it can also be part of a Unified Threat Management system to alert when threats are detected to the Network Infrastructure.

Single-factor authentication is the traditional security process that requires a user name and password before granting access to the user, this can also be a smart card as used for single sign-on

System Manager is a person whose job role includes the management of any number of computer systems: this could include the management of system users and perhaps a specific application such as PACS.

Two factor authentication, requires the user to provide dual means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security code

802.1x is an IEEE standard for network access control. Used predominantly in Wi-Fi wireless networks, 802.1X keeps the network port disconnected until authentication is completed. Depending on the results, the port is either made available to the user, or the user is denied access to the network

3 ROLES – WHO DOES WHAT

3.1 Responsibilities within the Organisation

The Chief Information Officer (CIO) is ultimately responsible for the Data Network

The Chief Information Officer (CIO) is the Executive lead for this policy

Network Engineers employed by the MBP are responsible for the day to day management and support of the Data Network

All components of the Data Network are under the control of the UHL IM&T department.

The management and support of the Data Network is the responsibility of the Managed Business Partner.

Managed business Partner (MBP) is responsible for implementing the policies and guidelines created by UHL and to report any identified breach using the formal procedures set out in the MBP contract to UHL IM&T management

All UHL employees are responsible for compliance with this policy wherever the policy is applicable to them.

3.2 Responsibilities of and communication with stakeholders

No changes will be made to the UHL data network without UHL IM&T approval via the formal change management process (CAB).

The IM&T Design Authority will define Security standards to be implemented for all operating system, networks, applications and remote access based on the sensitivity of the data being accessed

3.3 Network Documentation

The MBP must maintain current network diagrams detailing the configuration of the Data Network itself and all the major network components on it. These diagrams are to be kept, securely, within IM&T and copies must be lodged with the company supplying external support for the Data Network.

5. POLICY Implementation And Associated Documents –What To Do And How To Do It

5.1. User Identification, Authentication and Authorisation

Access to network hardware and its configuration must be restricted to authorised users and must be protected by appropriate physical and logical authentication and authorisation controls, it may be necessary to use multi factor authentication in certain circumstances to achieve this aim.

Network access to Data Network components must be restricted to specifically authorised personnel, such as members of the MBP and other designated persons.

Administrator login credentials for Data Network components must be changed from the manufacturer's defaults on installation and access must be controlled using the Authentication, Authorization, and Accounting (AAA) system rather than direct generic access

Wherever possible the use of ACL's (Access Control Lists) will be used to control and manage access to network hardware and its configuration.

5.2 Account Access to the Data Network

Access is split into three distinct modes:

- **Administrator access** – this is the access granted to the MBP and to any external supplier contracted to provide support for the network. Individual officers having this level of access are granted the rights to configure network devices and monitor network traffic. A register of users having this level of access is maintained by the MBP.

- **User access** – this is the access granted to UHL staff and affiliates to allow them to perform their duties. Individuals who access the Data Network are granted the minimum rights necessary to data processing facilities which are appropriate to their role. UHL employees granted user access level are responsible for keeping their account details secure and must report, to IM&T, any incidence, whether actual or suspected, where this security may have been compromised. The sharing of user credentials such as username & password or NHS smart card & pin number is strictly prohibited

- **Third Party access** – this is the access granted to organisations outside the UHL who require access to the Data Network in order to support applications or other systems. A register of organisations having this level of access will be maintained by the MBP. Companies offering third party support for systems within the UHL will only be granted sufficient access to the Data Network to allow them to fulfil their support function.

5.3 Authorisation

User access to the UHL Data Network will only be granted to individuals upon receipt of a correctly completed on-line application form sponsored by a line manager.

Access will only be granted on the understanding that the user granted access will comply with the relevant policies on use of the data network, including applications such as email and the internet etc.

5.4 Physical security of Data Network components

All components of the Data Network shall be housed in secure accommodation i.e. equipment rooms, data centres etc. except where provision of such accommodation is not feasible e.g. Glenfield hospital where shared accommodation is available with facilities equipment in basement areas.

Where only shared accommodation is available then locked cabinets shall be provided and used to house Data Network equipment, this shall apply in other areas where cabinets are installed in open areas e.g. Rogers Ward, to prevent unauthorised access to Data Network components

Access to Data Network equipment shall be restricted at all times using physical locks and the centralised door locking system to prevent unauthorised access to Data Network components.

Entry to secure areas housing critical or sensitive network equipment will be restricted to those whose job requires it. The physical security team will maintain and periodically review a list of those with unsupervised access to core Trust network/computer rooms. Detailed lists of those with approved access will be displayed at the entrances to such areas.

Only authorised persons are to change the physical and / or logical components of the Data Network, this includes the patching of all devices connected directly to the Data Network.

Data Network components must be sited so as to avoid interference from other potential sources of electromagnetic interference such as electrical power cables, high powered medical scanners etc.

All visitors to areas housing core critical or sensitive network equipment must be authorised by the physical security team and must be made aware of network security requirements. All visitors to these areas must be logged in and out. The log will contain name, organisation, purpose of visit, date, and time in and out. Visitors to rooms/areas that contain switches and hubs are to be controlled by the network team. Responsible staff are to ensure that all relevant are made aware of procedures for visitors and that visitors are escorted, when necessary.

5.3 Service Accounts

Service accounts: are defined as being those accounts used by computer systems to authenticate to other computer systems, they are not to be used by users to authenticate to those systems.

Passwords are to be a minimum of 15 characters consisting of complex characters.

Service accounts must have a non-expiring password.

These accounts must not have the right to logon interactively (i.e. on to a desktop/server)

5.5 User Access Privilege and Entitlement

This policy assumes that anyone who is granted access to systems has been through the appropriate personnel checks before employment / access is granted (Registration Authority as used for Smart Cards is acceptable).

Access to systems should be authorised on a need to use basis that is an individual should not be granted access in excess of that which is required to fulfil their role within the Trust.

Annual checks should be performed to prevent users gaining excessive rights when they move roles within the Trust.

Users who use their access for purposes which are not required by the Trust (e.g. looking up medical or demographic details of friends or family) are acting against Trust policy and (where personal information is concerned) are in breach of the Data Protection Act (1998).

Access privileges must be authorised & revoked by the appropriate Information Owner or manager

Where account holders are transferred to private companies e.g. when a service transfers under T.U.P.E. then access to UHL systems can continue, however transfer of data to third parties must be approved by UHL.

Where access to UHL systems is required by third parties then the relevant Information Owner from UHL should authorise access.

5.6 Account Security

Users must never share their personal login credentials (including Smart cards & tokens) with anyone else for whatever reason. If a user inadvertently discloses their password then they should change it as soon as possible.

5.7 Administrator / supervisor / root access

The techniques of minimum elevated user privileges should be used on all systems i.e. only privilege levels necessary to accomplish tasks should be employed and not full administrator rights.

Logins which have administrator access require greater security and should:

- Have a minimum of 15 characters consisting of complex characters.
- Have a lifetime of 365 days, and must be changed when staff who know the passwords leave, whichever is the shorter.
- Where possible administrators should use administrator level privilege to run application in 'run as' mode with lower level privilege overall, this is recommended by Microsoft to reduce the spread of malicious software between systems.
- Administrator accounts should not be used for server applications (services in Microsoft language) Windows service accounts should be used where necessary to achieve these aims.

5.8 Generic logins

Is a term used to describe an anonymous person who shares a login identity to access a system; these are frequently used in areas where login times are excessive and may adversely affect patient care. The use of Generic logins are no longer supported as they represent a threat to secure access of data, access is anonymous therefore the user cannot be verified.

5.9 Access Termination, Modification or Revocation

Systems owners are responsible for producing detailed processes for terminating, modifying or revoking user access.

It is the responsibility of the person using an information system (or their Manager) to inform IM&T and the systems Information Owner that the person no longer requires access to that system for whatever reason.

It is the responsibility of the person using an information system (or their Manager) to inform IM&T and the systems Information Owner that the person will not require access to a system due to extended absence e.g. maternity leave, sabbatical etc..

- Accounts must only remain active whilst they are required.
- Accounts must be disabled as soon as a person leaves employment with the Trust.
- Under no circumstances must an account be used by another person, either temporarily or permanently.
- IM&T will monitor accounts for usage; any account not used for 90 days will be disabled for a further 180 days after which it will be scheduled for deletion.

Audit activity of account management is required to be maintained for 6 years after the individual has left the employment of the Trust (in line with the retention requirements for smartcards administration)

5.10 Operating System, Network, Application and Remote Access Control

Security standards stated in this policy will implemented for all operating system, networks, applications and remote access irrespective of the sensitivity of the data being accessed.

A restricted access policy must be observed on all network devices (Hubs, Routers, Switches) using suitable passwords (see the UHL Policy For The Control Of Access To Electronic Systems)

The configuration of network devices will be automatically recorded by the Network Monitoring System (Solar Winds) so that the configuration can be restored in the event of an inadvertent change or disaster occurring.

All communications with Network devices will be encrypted using either SSH or SSL to prevent credential snooping using packet sniffing techniques. Access to Network Devices using the TELNET protocol is prohibited due to its lack of security.

Access Control Lists (ACL's) shall be used to control and monitor access to all network devices via 802.1x authentication servers linked to active directory (e.g. Radius Servers)

5.11 Remote Access to internal UHL Systems

Access to UHL systems from third party suppliers or UHL employees will be via the Virtual Desktop solution provided for that purpose which can be accessed via the

Internet. This solution provides restricted secure access to Network devices on the UHL network using two factor authentication techniques.

Authorized users shall protect their login and password, even from family members.

While using a UHL owned computer to remotely connect to UHL's corporate network that computer must use the AO-VPN (Anywhere on VPN) provided for connectivity over public networks.

Use of external resources to conduct UHL business must be approved in advance by the appropriate business unit manager.

Personal equipment used to connect to Internal UHL networks must meet the requirements of UHL owned equipment and be approved by IM&T.

All hosts that are connected to UHL internal networks via remote access technologies must use the most up-to-date anti-virus software.

Any changes made to the configuration of the remote access service must be approved by the TDA (Technical Design authority), Change Approval Board together with independent penetration testing of the service to verify security.

Requests for third party remote access must be made via the Service Desk and approval gained from UHL IM&T management.

5.12 Third Party Access

All third party access (contractors, business partners, consultants, vendors) must be appropriately authorised and monitored for compliance.

Third party access to electronic information will be granted for the minimum period necessary with a termination date set on the relevant account (this would normally be the end of contract date).

In cases where third party access is needed for long periods to satisfy service level agreements under support arrangements, the business owners must specify access timeframes and justification for such access. Where possible restrictions should apply to service accounts by disabling access until requested, this will prevent unauthorised changes being made to live systems.

Remote access for external suppliers shall also incorporate the following features:

Any account provided for external support shall be disabled until access is formally requested via service desk protocols

All requests for remote access shall be recorded by the service desk

The account will be disabled as soon as the external support session is completed.

The account shall not be left enabled for extended periods of time.

5.13 Event logging

Event logging shall be enabled on all computer systems, irrespective of roll or function.

Event logs shall be held for a minimum of 24 hours on the local system producing them.

Event logging shall be enabled in Active Directory to log events for all systems including Servers, Domain Controllers, Personal computers and Laptops that are members of the domain.

The Active Directory events to be logged are: user logon success, user logon failure and user logoff.

All user logon events shall be logged along with date, time, IP address of originating machine, machine name, and user ID.

All event logs shall be forwarded to the UHL S.I.E.M. (Security, Information & Event Management) system to be archived for future analysis.

The S.I.E.M. should retain all logs for a minimum period of 5 years so that retrospective analysis can take place.

5.14 Risk Assessments

UHL will carry out security risk assessment(s) in relation to all the business processes covered by this policy. These risk assessments will cover all aspects of the network that are used to support those business processes. The risk assessment will identify the appropriate security countermeasures necessary to protect against possible breaches in confidentiality, integrity and availability.

Risk assessment will be conducted to determine the assured levels required for security measures that protect the network.

Formal risk assessments will be conducted using an appropriate methodology and will conform to the ISO27001 standards.

Risk assessments will be carried out on behalf of the IM&T by the Security Manager and / or an external Security consultancy

6. EDUCATION AND TRAINING REQUIREMENTS

Information governance training is mandatory for all UHL employees, training materials can be found on the UHL training website at https://uhlhelm.com/

More specific and detailed training will be required by those people who manage the data network, this will usually be specific to the products being managed

7. PROCESS FOR MONITORING COMPLIANCE

POLICY MONITORING TABLE

Element to be monitored	Lead	Tool	Frequency	Reporting arrangements	Lead(s) for acting on recommendations	Change in practice and lessons to be shared
Compliance with this policy	IM&T	External Audit of implemented controls	Annually	UHL Audit Committee	UHL Chief Information Officer	Change in policy if necessary
Access control processes to be monitored to detect non-compliance	Privacy Manager	Information security risk assessment	Monitoring results must be reviewed on a regular basis as determined by the information asset risk classification	Information asset owners are responsible for monitoring their control processes to detect non-compliance with this Access Control Policy and to record evidence in case of security incidents.	IM&T Security Officer / IM&T Security Board	Change in policy or processes if deemed necessary

8. EQUALITY IMPACT ASSESSMENT

Name of Policy / guidance Document: DATA NETWORK SECURITY POLICY

The Trust recognises the diversity of the local community it serves. Our aim therefore is to provide a safe environment free from discrimination and treat all individuals fairly with dignity and appropriately according to their needs.

As part of its development, this policy and its impact on equality have been reviewed and no detriment was identified.

9. SUPPORTING REFERENCES, EVIDENCE BASE AND RELATED POLICIES

Principles of information security, https://digital.nhs.uk/services/data-security-centre

- Related Policies
  - UHL Information Security Policy Trust Ref A10/2003
  - UHL Access to Electronic Systems policy
  - UHL Firewall policy

10. PROCESS FOR VERSION CONTROL, DOCUMENT ARCHIVING AND REVIEW

- Once this Policy has been approved by the UHL P&G Committee, Trust Administration will allocate the appropriate Trust Reference number for version control purposes.
- The updated version of the Policy will then be uploaded and available through INsite Documents and the Trust's externally-accessible Freedom of Information publication scheme. It will be archived through the Trusts SharePoint system
- This Policy will be reviewed every three years and it is the responsibility of the Policy and Guideline Committee to commission the review

Contacts & Assistance

For information and guidance on the implementation of this policy, contact:

- The IM&T Service Desk on 8000
- The Chief Information Officer on 5391
- The Head of Privacy on 6053