University Hospitals of Leicester NHS

NHS Trust

IM&T Department

Privilege Access Management UHL Policy

Approved By:	Policy and Guideline Committee
Date Approved:	17 July 2020
Trust Reference:	**B28/2020**
Version:	1.0
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 2023 **6 Months Review Date Extension Approved by Director of CLA as Document Remains Fit for Purpose & Legislative Requirements.**

CONTENTS

REVIEW DATES AND DETAILS OF CHANGES MADE DURING THE REVIEW

Revision History

May 2020	V1.0	Original prepared by IM&T Head of Design Authority

KEY WORDS

Authentication
Enhanced Rights
Privilege access
CYBER ESSENTIALS

1. INTRODUCTION And Overview

This policy sets out the standards to be employed in the management Privilege Access for users at UHL,

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

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

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.

This document sets out the University Hospitals of Leicester (UHL) NHS Trusts Policy and Procedures for the management of users who are to be, or have already been given Privileged access to trust IT assets.

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

This policy covers the following areas:-

- Ongoing management of Privileged Access
- Change control of Privileged Access
- Audit of Privileged Access

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 3rdparties 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

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 computers, voice and data 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 requirements will be applied to new and existing users with Privileged Access.

Principle of Least Privilege
Privileged users must only be provided with the absolute minimum access rights, permissions to systems, services, information and resources that they need to fulfil their business role.

Authorisation Process
There must be a formal authorisation process to grant, assign and approve the allocation of a privileged user role.

Security Clearance
All privileged users must have the appropriate level of background checks and clearance for the role they are assigned.

User Identification and Access Control
Each privileged user must be uniquely identifiable.

All privileged users must be managed using identity and access management policies.

Account Management
Privileged access is only used and granted when it is needed and revoked when it is no longer required.

Joiners, leavers and movers’ processes and procedures must register and include processes for the management of privileged users.

Privileged user access rights must be monitored and reviewed and revalidated on a 6 monthly basis to confirm that the levels of access are still required for the role.

A record of all privileged user roles assigned and their level of access must be recorded, maintained and made available on request.

Monitoring and Auditing
Logging and monitoring tools and techniques must be used to monitor and manage privileged users' behaviour and actions.

The activities of a privileged user must leave a log or audit records that are outside the read, write and/or delete capability of their role.
Privileged user accounts and their usage must be monitored and reviewed. Accounts that are dormant or accounts that cannot be associated with a business process and owner, must be disabled.

Education, Training and Awareness
All privileged users must have security and awareness training in relation to the role in addition to the standard security and awareness training.

Business Continuity and Disaster Recovery
Business continuity and disaster recovery plans must have clearly defined processes and procedures for allocation and management of privileged users.

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

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.

Data Network is the technology used to transmit data which connects electronic system (computers) together and comprises switches, cables, firewalls etc. this is the mechanism which allows computers to communicate.

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.

Privileged User Definition

A privileged user is a user who has an elevated level of access to a network, computer system or application and is authorised to perform functions that standard users are not authorised to perform. This includes a standard user with escalated privileges which gives access on a par with a privileged user

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

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.

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.

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.

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

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

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

ITHC is an IT health check carried out periodically by a certified IT security professional, a report is produced highlighting areas of concern for remediation

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.

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

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.

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

Responsibilities within the Organisation

The Chief Information Officer is the executive lead for this policy.

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

Privilege Access is under the control of the UHL IM&T department.

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

Privileged user access must be requested electronically, detailing the access required, and authorised by the CIO).

A record of all privileges allocated must be maintained by the Managed Business Partner.

Suppliers

Privileged user access must be requested electronically detailing the access required, and authorised by the applicable Authority (equivalent to the CIO role) for that Supplier.

A record of all privileges allocated must be maintained by the Supplier Security Manager.

Suppliers must inform the Authority if any access has had to be revoked as a consequence of a security incident.

Suppliers must be able to provide the Authority with audit logs or records that show when the privileged accounts have been used upon request.

Policy Exceptions

If the requirements in the Privileged User Security Policy cannot be met then the reasons for this must be documented, risk assessed and explained to the CIO for their approval.

Such exception requests may invoke the Risk Management process in order to clarify the potential impact of any deviation to the configuration detailed in this policy.

Exceptions to this standard must be maintained on the Trust risk register for accountability, traceability and security governance reporting to senior management.

Documentation

The MBP must maintain records of any request for Privileged Access whether granted or denied. These records are to be kept, securely, within IM&T data storage systems and not on external storage. These records remain the property of UHL and must be made available for inspection as and when required.

Security Control Assurance

Controls presented in this policy, or referred to via this policy, will be subjected to a formalised IT Health Check penetration test to provide evidence of adequacy and effectiveness

Technical Security Control Requirements

In this document the term must, in upper case, is used to indicate an absolute requirement. Failure to meet these requirements will require a formal exemption (see '**Exceptions**' above).

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

User Identification, Authentication and Authorisation

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

Password are to be changed every 12 months maximum

Access Termination, Modification or Revocation

The MBP is responsible for producing detailed processes for terminating, modifying or revoking Privilege Access granted to users.

Accounts must only remain active whilst they are required and must be disabled or removed when not 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)

Event logging

Event logging will be provided by IM&T using technology specifically for that purpose

Event logging shall be enabled for all users

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. 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/

6. 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 access control processes to detect non-compliance with this Access Control Policy and to record evidence in case of security incidents.	Privacy Manager / IM&T Security Officer	Change in policy or processes if deemed necessary

7. Equality Impact Assessment

Name of Policy / guidance Document: UHL Privileged Access Management Policy

8.1 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.

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

.

8. 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 Data Network Policy

9. 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 IM&T Head of Design Authority on 5216
- The Head of Privacy on 6053