Reference Number: UHB 318 **Version Number:** 1	**Date of Next Review:** 10 Jun 2019 **Previous Trust Reference Number:** T133

Information Technology Security
Access Control Guidance

Introduction and Aim

This document is written in support of the Information Technology (IT) Security Policy and supporting procedures. It provides a mechanism to achieve and maintain appropriate security arrangements in respect of Cardiff and Vale University Health Board's (the UHB) IT systems that hold confidential and sensitive patient and business information.

The UHB must ensure the safety and security of all its UHB IT systems, software and in particular the UHB's Network so as to produce a safe and secure environment in line with NHS and statutory policies and procedures. This document provides further information on access control to support the IT Security Policy and its related control documentation.

Objectives

- Successful implementation of this procedure will address business and performance standards for example the requirement to meet Caldicott standards, Health and Care Standards (2015)
- Aspire to meeting BS7799/ISO27001 standards and the Information Governance Toolkit Standards as far as possible in the Welsh context.

Scope

This guidance applies to all of our staff in all locations including those with honorary contracts

Equality Impact Assessment	An Equality Impact Assessment has been completed for the overarching IG and IT Policies. The assessment found that there was some impact on the equality groups mentioned in relation to communication. An action plan has been developed to address those areas.
Documents to read alongside this Procedure	Information Governance Policy Information Technology Security Policy Information Technology Security Procedure Information Risk Management Procedure A Guide to Incident Reporting
Approved by	Information Governance Sub Committee

Accountable Executive or Clinical Board Director	
Author(s)	Richard Williams (IT Security) Ann Morgan (Information Governance)

Disclaimer

If the review date of this document has passed please ensure that the version you are using is the most up to date either by contacting the document author or the Governance Directorate.

Summary of reviews/amendments

Version Number	Date of Review Approved	Date Published	Summary of Amendments
V1	10/06/2016	05/08/2016	New UHB document supersedes Cardiff and Vale NHS Trust IT Security Policy (ref 133) – Appendix 2 Access Control.
03.01 ISOSP03		04/2008	Original Document

Contents Page

1 Introduction

1.1 The objective of Access Control is to prevent unauthorised computer access.

1.2 Access to computer services and data should be controlled on the basis of business requirements that take account of policies and procedures for information dissemination and entitlement.

1.3 There should be formal procedures to control allocation of access rights to the UHB's computer services. Special attention should be given to the control of privileged access rights which allow users to over-ride system controls.

1.4 Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of equipment.

2 Documented Access Control

2.1 The business requirements for access control are to be clearly defined in the system security policy for the system. Service providers are to be given a clear statement of the business requirements for system access, in order to maintain an effective level of control of access to the UHB's computer services and data.

2.2 Each System Administrator/Manager are to maintain a clearly defined access policy statement, which defines the rights of each user or group of users. The policy should take account of the following:

- The security requirements of individual business applications;

- Policies for information dissemination and entitlement, e.g. the 'need to know' principle.

2.3 Standard user access profiles should be established for common categories of job

3 User Registration

The formal user registration procedure for access to all UHB computer services:

- Ensures service providers do not provide access until the authorisation procedures have been completed.
- Checks that the user has authorisation from the System Manager/Data Owner for the use of the service.
- Checks the level of access is appropriate for the business purpose and is consistent with the UHB's IT Security Policy.
- Maintains a formal record of all persons registered to use the service.

The formal user de-registration procedure for access to all UHB computer services:

- Where appropriate remove the access rights of users who have changed jobs
- Remove access rights of users who have left the UHB.
- Ensures that redundant user IDs are not re-issued to another user.

3.1 Access to computer services and data are controlled on the basis of business requirements and are the responsibility of the Departmental Manager.

3.2 "Special privileges" are those, such as are allowed to recognised users of the application that require this higher level of authority, that require "sign off" by the Head of Service. Typically they allow access to sensitive areas within a system or allow the user to amend the software itself (rather than simply the data).

3.3 Special privilege access is controlled through a formal authorisation process similar to normal user registration with, in addition:

- Authorisation from the IM&T Security Manager.

- Identification of the special privileges associated with each system and the staff to which they need to be allocated.

4 Password Control

4.1 All new staff are briefed by the line manager on the importance of passwords and instructed in the manner in which they are to be used and protected, and is part of the staff induction process.

4.2 Each member of staff have their individual user identification and password. Passwords should not relate to the user or to the system being accessed.

4.3 The allocation of passwords, is controlled by a formal management process, the requirements of which are as follows:

- All passwords are conveyed to users in a secure manner. Temporary passwords must be deleted after a pre-defined time period.

- Enforce the use of individual passwords to maintain accountability.

- Allow users to select and change their own passwords and include a confirmation procedure to allow for typing errors.

- Passwords must have a minimum length of 8 characters and must contain three of four character types: lowercase (e.g. abc) uppercase letters (e.g. ABC) numbers (e.g. 123) symbols (e.g. ?!%).

- Enforce a password change at 90-day intervals (users will be automatically prompted when password renewal is due).

- Maintain a record of previously used passwords and prevent users from re-using them.

- Systems **cannot** display passwords on the screen when being entered.

- Limit the number of unsuccessful log-on attempts to 5 within a 10 minute period, after which the unsuccessful attempt is recorded and the account is locked for 30 minutes. If unable

to wait and immediate access is required, the user must contact their relevant IT Help Desk.

4.4 Where temporary passwords are known to the system Administrator/Manager or network manager (e.g. on granting access to new users or when a user forgets their password), the users must change the password immediately.

4.5 In addition, users accessing systems containing patient-identifiable data, or users with system supervisory privileges, must use a mixture of alphabetic and non-alphabetic characters in their passwords and the password 'time-out' facility within Windows to avoid unauthorised access when staff members are temporarily absent from their workstation.

5 Privilege Management

The use of special privileges must be restricted and controlled. For multi-user systems that require protection against unauthorised access, the allocation of privileges should be controlled through a formal authorisation process that should:

5.1 Identify the privileges associated with each system product (e.g. operating system, database management system) and the staff to which they need to be allocated.

5.2 Allocate special privileges to individuals on a 'need to use' basis and on an 'event by event' basis i.e. the minimum requirement for their functional role only when needed.

5.3 Ensure that any user assigned high privileges for a special purpose uses a different user identity from that used for normal system access and is allocated a 'one-off' password that is deleted after use.

6 Network Access Control

6.1 Connections to networked services are controlled. This is necessary in order to ensure that connected users, or computer services, do not compromise the security of any other networked services.

6.2. Access to the network is restricted to authorised equipment and personnel.

6.3. Only approved access is possible to network management facilities or controls or other privileged commands on the network, where those commands could be used to bypass security control.

7 Application Access Control

Logical access controls are used to control access to application systems and data and are restricted to authorised users. Users of application systems are provided with access to data and application system functions with the following controls:

- Provide menus to control access to application system functions.
- Restrict user's knowledge of data or application system functions, which they are not, authorised to access.
- Control the access capabilities of users (e.g. read, delete, and execute).
- Ensure that outputs from application systems handling sensitive data contain only the data that are relevant to the use of the output**.**

8 Monitoring System Access and Use

8.1 Systems are to be monitored by System Administrator/Manager to ensure conformity to UHB policies and standards. This is necessary in order to determine the effectiveness of measures adopted and to ensure UHB conformity

8.2 Any system monitoring that is undertaken complies with the guidelines issued by the Information Commissioners Office and will comply with the Regulatory of Investigative Powers Act (2000) and the Human Rights Act (2000).

9 Clock Synchronisation

9.1 Computer clocks are automatically synchronised with NTP and Windows Time Services