Reference Number: UHB 430 **Version Number:** 1.1	**Date of Next Review:** 8th Aug 2020 **Previous Trust/LHB Reference Number:** **Trust 133**

INFORMATION TECHNOLOGY SECURITY
SECURITY OF ASSETS 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 security of assets 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 Guidance	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	Executive Director of Therapies and Health Science
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
1	08/08/17	29/08/2018	New Document
1.1	08/08/17	29/08/2018	Admin changes to reflect current contact details

Contents Page

1 Introduction

It is clear that assets represent an important expenditure for the NHS and any theft or loss can place a huge financial burden on the UHB, as well as having a significant impact on the delivery of healthcare and depriving the UHB of resources which would otherwise contribute to patient care.

In the current economic climate and at a time when the NHS is expected to demonstrate 'value for money', the UHB and their staff should ensure their assets are protected and secured properly.

Gaining a clear understanding of an asset can be complex. UHB assets may not stay within the UHB and be on a UHB site all of the time. They can be loaned to other Health Boards and to patients, or taken off site for maintenance and repair. Equally, the financial or operational value associated with the asset, its size and portability, can make it more susceptible to it being stolen, damaged or lost. These issues can lead to difficulties in determining how best to secure and protect the UHB assets.

2 Assets Ownership

For security purposes each physical asset and each set of data will be assigned an "owner" as follows:

- Physical Assets (computer hardware and associated peripheral equipment) - the UHB
- Data and Software Assets - Senior Management, that is those who are responsible for the system

Physical Assets Control

For practical purposes (inventory, maintenance etc.) physical assets are delegated to the Directorate Manager/Head of Department.

Maintenance arrangements are however the subject of contractual agreement and only approved system engineers are allowed access to hardware.

In general terms the following maintenance criteria applies:

- hardware critical to the effective running of the UHB business are the subject of maintenance contracts
- individual PCs upon procurement have a five years on-site maintenance
- printers are not contracted (as it is less expensive to replace failed equipment than to maintain it under contract)

Where there is uncertainty as to whether an individual hardware item should be the subject of a maintenance contract or not, the IT Security Department will undertake a risk analysis of the loss of availability.

Critical equipment (for example PMS, Security, Email, Windows servers) are protected from power failures through use of uninterruptible power supplies (UPS) that is further supported by the Hospital Generators.

Data and Software Assets Control

Data owners are Senior Management that is those that are responsible for the system, and are responsible for:

- backing-up any systems that do not deposit their data centrally (this is the exception not the norm)
- specifying how the data can be used
- agreeing who can access the data and what type of access each user is allowed
- ensuring compliance with IT security policy, procedures, and with reference to IT Security guidance documentation
- ensuring compliance where necessary with legal acts and legislation covering personal, patient or medical data

3 Responsibilities

The managing of IT assets (albeit IT equipment, software or data) is the responsibility of individual Departments and for core UHB services the IM&T Department.

Departments

Departments should hold local asset /equipment and software/data registers. Individual departments should be made responsible for ensuring their local registers are kept up to date and reviewed on a regular basis.

Departments should develop procedures to ensure that the asset is properly managed throughout its usage. Attention should be given to how the item will be stored securely when not in use, what should happen if it is relocated or loaned to another department, patient or other Health Board, and how it will be tracked and audited.

The department must always be mindful that when IT equipment or system reaches the planned *end-of-life* date, all sensitive and confidential data must be removed from all IT equipment such as laptops and mobile phones before being redeployed or decommissioned. Where the data is still required to be stored, it should be transferred in the appropriate manner to another system.

IM&T Department

The IM&T department is a department in its own right therefore all the above department responsibilities are applicable. The department consists of; the IT Helpdesk, network, server, technical development, development, project support and IT Security teams.

Within the UHB Services Accommodation Centre core systems/data and departmental system/data servers are housed in secure air conditioned computer rooms.

The IM&T department are responsible for:

- Back up on a daily basis the Network Servers and all centrally held data.
- Maintaining detailed data housekeeping procedures for corporate systems.
- Ensuring compliance with UHB security controls
- Ensuring compliance, where necessary, with the relevant acts and other relevant legislation covering personal, patient or medical data.

This document is one of several that sustain the UHB's IT Security Policy and IT Security Procedure.

Useful Contacts

Appendix 1

IM&T IT Security cv.imt.security@wales.nhs.uk

Head of IT and Strategic Planning
Nigel Lewis Nigel.Lewis@wales.nhs.uk
Tel 02920 745600

Technical Development, Network and Support Manager
Gareth Bulpin Gareth.Bulpin@wales.nhs.uk
Tel: 02920 745605

IT Helpdesks
UHW (East) IT.Helpdesk.UHW@wales.nhs.uk
Tel 02920 745073
UHL (West) Llandough.Helpdesk@wales.nhs.uk
Tel 02920 715218

Information Governance cav.ig.dept@wales.nhs.uk
Including Data Protection/Freedom of Information and E-mail monitoring

Information Governance/Clinical Coding
James Webb james.webb@wales.nhs.uk
Tel 02920 746208

Corporate Governance Senior Information and Communication Manager
Ann Morgan ann.morgan4@wales.nhs.uk
Tel 02920 744870

Information Governance Co-ordinator
Denise Gulley denise.gulley@wales.nhs.uk
02920 745625