Reference Number: UHB 427 **Version Number:** 1.1	**Date of Next Review:** 20th Sep 2019 **Previous Trust/LHB Reference Number:** Trust 133

INFORMATION TECHNOLOGY SECURITY
IM&T EQUIPMENT PROCUREMENT 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	Executive Director of Therapies and Health Science
Author(s)	Richard Williams (IT Security) Ann Morgan (Information Governance)

Summary of reviews/amendments

Version Number	Date of Review Approved	Date Published	Summary of Amendments
03.01 ISOSP10		04/2008	Original Document
1	20/09/16	28/08/18	Review and updated to new guidance document in line with the Schedule of Revision approved by IGSC.
1.1	20/09/16	28/08/18	Admin changes to reflect current contact details

Contents Page

1 Introduction

This guidance document applies to hardware or software procured from external suppliers and is to ensure that appropriate IM&T hardware and software is purchased to match the needs of the Cardiff and Value University Health Board (the UHB) and that installation is carried out in an efficient and effective manner.

2 Procurement

A well-drafted specification of requirement not only sets the quality and performance standards, but also provides the greatest scope for maximising value for money. A good specification should be functional and concise, but with sufficiently detailed.

The system specification must:

- include a statement of the service levels
- continuity of service required by the users
- the data security and confidentiality levels needed for the types of data being handled

Each identified point above must be met explicitly in the system solution chosen.

The specification of service levels **must be** complete before the Business Options are considered. It could be that the data is so sensitive that some of it is not held on the computer.

The acquisition of all computer assets (hardware, operating software and proprietary software) **should be** authorised centrally from the UHB, with the aim to ensure:

- PC hardware and software is, as far as possible, compatible throughout the UHB
- facilitate mutual contingency arrangements
- allows for more cost effective purchasing of hardware and software

The above points facilitates the implementation of a basic level of security across all PCs and laptops in the organisation by allowing more cost effective purchase of, for example, virus-checking software for access control mechanisms.

Where, for organisational or budgetary reasons, central purchasing is not possible, then an up to date centralised asset register of all PC hardware and software **must be** maintained.

The procurement procedures must provide for an acceptable level of hardware redundancy (i.e. spare capacity), appropriate to the required user service levels. Spare capacity should be measured in terms of sufficient additional equipment to back up failed equipment in an emergency or sufficient equipment to allow a system adequate spare time to recover from processing delays.

All procurements **must ensure** that:

- hardware or software changes, which may affect network management, are agreed by all parties affected.
- any new IM&T facilities provide an adequate level of security and will not adversely affect existing security.
- mandatory and desirable security requirements are included in procurement specifications.
- the IM&T Security Manager and Information Governance Manager are consulted to ensure that the selected hardware or software will meet the agreed security and data protection requirement.

Hardware or software changes that may affect the network management or other operational sites must be agreed by all parties affected. The aim is to avoid a situation whereby processing between linked areas may be prevented by the installation of incompatible hardware or software.

On-going maintenance arrangements (defining level of maintenance and minimum levels of performance) must be the subject of contractual agreement where hardware or software is covered by a maintenance agreement. If it is decided that any equipment need not be maintained (as it may be cheaper to replace it) the decision process should include an impact analysis of the loss of availability.

3 Installation

The installation of any hardware or software by the IM&T Department **can only be actioned** by completing the UHB's IT Installation request forms.

Installation of hardware or software must be the subject of a contractual agreement that specifies the timetable for installation.

The installation criteria for accepting the installed product **must be** clearly defines. For example, detailing the post-installation trials.

Hardware or software under trial **must not** be linked to a configuration that is engaged in live running.

Application systems must fulfil any relevant legislative requirements together with detailed supporting documentation. This includes the Data Protection

Act, Software Copyright Act, Computer Misuse Act, and any other relevant legislation.

Application systems must be designed such that the extraction, collation and reporting of all data pertaining to an individual can be performed in a timely manner in accordance with the requirements of the Data Protection Act.

4 Implementation

Test plans must include:

- attempts to cause security failures.
- deliberate crashes and restarts of the system to check whether data integrity is compromised.
- All password controls and any other security measures should be tested.

Testing must not:

- take place on live databases.

There must be formal documented hand over procedures for the migration of systems from system testing to user acceptance. All systems must be documented according to site standards. Documentation must be kept up-to-date so that it matches the state of the system at all times.

System documentation must be duplicated and one copy stored in a location that will remain secure, even if the computer system and all other copies are destroyed.

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 Manager/Clinical Coding
James Webb james.webb@wales.nhs.uk
Tel 02920 743747

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