Reference Number: UHB 358 **Version Number:** 1	**Date of Next Review:** 20 Sep 2019 **Previous Trust/LHB Reference Number:** Trust 133

INFORMATION TECHNOLOGY SECURITY PROCEDURE

Introduction and Aim

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

The IT Security procedure of the UHB is to ensure the safety and security of all 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 as to the detail of the policy and its supporting information.

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 procedure 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.
Health Impact Assessment	A Health Impact Assessment (HIA) has not been completed. Not Required.
Documents to read alongside this Procedure	Information Governance Policy Information Technology Security Policy 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	20/09/2016	27/07/2017	New Procedure

Contents Page

1 Introduction

1.1. Purpose of Security Procedure

It is essential that all information systems in the Cardiff and Vale University Health Board (the UHB) are protected to an adequate level from events that may jeopardise health care activities. These events may include accidents as well as behaviour deliberately designed to cause difficulties. The purpose of an IT security procedure is to preserve:

Confidentiality access is confined to those with authority to view the data.

Integrity all systems are working in the way they were intended to work.

Availability information is delivered to the right person, when it is needed.

1.2. The Need for a Security Policy and Procedure

Data stored in UHB information systems represent an extremely valuable asset. The increasing reliance of the UHB on information technology for the delivery of health care makes it necessary to ensure that these systems are developed, operated, used and maintained in a safe and secure fashion.

The IT Security procedure supports the IT Security Policy which sets out the broader implications of statutory and NHS policies in related security area. Currently the most notable UK acts are:

- Copyright, Designs and Patents Act (1988)
- Access To Medical Records Act (1990)
- Computer Misuse Act (1990)
- Computer Crimes Act (1997)
- Data Protection Act (1998)
- Human Rights Act (1998)
- Regulation of Investigatory Powers Act (2000)
- Anti-Terrorism, Crime and Security Act (2001)

This procedure sets out how the UHB will address the requirements in operational terms.

1.3 Scope of the Procedure

This procedure fully addresses the IM&T security requirements of the Welsh Assembly Government DGM (96)43 ‘The Protection and Use of Patient Information’, WHC (98)80 ‘The Caldicott Report’ and WHC (99)92 ‘Protecting

Patient Identifiable Information: Caldicott Guardians In The NHS', WHC (2001)47, Code of Connection and WHC(2002)36

The procedure builds on the general requirements published by the National Assembly for Wales Welsh Assembly Government and these are detailed below:

- The NHS In Wales Security Policy
- Baseline IT Security Standards
- NHS-wide networking Code Of Connection For NHS Organisations

The EU directive "For the Protection of Individuals With Regard To the Processing of Personal Data and the Free Movement of Such Data" was adopted on 24 July 1995. A new Data Protection Act came into force during 1998, which included manual as well as automatically processed personal data. Staff are under a common law obligation to preserve the confidentiality of this information at all times both during and after their employment with the UHB has terminated.

2 Responsibilities

Chief Executive

The Chief Executive has overall responsibility for ensuring the UHB has processes in place to fully comply with the IT security requirements placed upon the organisation.

Executive Director Therapies and Health Science

The Executive Director of Therapies and Health Sciences has been given the delegated responsibility for all aspects of Information Technology within the UHB which includes IT security.

Head of Information Technology

The Head of IT has overall responsibility for all aspects of information Technology within the UHB. This includes ensuring process are in place for monitoring of the IT Security procedure

IM&T Security Manager

The IM&T Security Manager is responsible for

- Implementing, monitoring, documenting and communicating the UHB's IT Security Policy and IT Security Procedures within the organisation.
- Ensuring compliance to the NHS Network Code of Connection and with relevant legislation including the Data Protection Act (1998), Computer Misuse Act (1990) and Human Rights Act (1998), Privacy and Electronic

Communications Regulations (2003), Regulations of Investigatory Powers Act (RIPPA) (2000).

- Monitoring for signs of illegal or unauthorised software being loaded
- Monitoring for signs of misuse of internet services

The IM&T Security Manager has the authority in the event of a security incident to affect the disconnection of any user from the network.

The IM&T Security Manager will periodically report to the Head of IM&T the state of IT security within the organisation

IT Department

It Department is responsible for providing service and operational support for corporate systems and for devolved departmental systems the IT department provide functionality for systems but no service and support.

Managers

Managers are responsible for ensuring all of their staff comply with IT Security requirements for all IT systems used within their department, albeit departmental specific or corporate systems.

Managers are required to report any IT Security infringement, such as inappropriate usage or access, immediately to the IM&T Security Manager.

All managers must have processes in place to ensure that all staff are trained and are aware of their responsibilities. Managers should also ensure that their staff capabilities are reviewed at regular intervals.

Managers must ensure that any authorisations they approve for special privileged access rights are reviewed on a regular basis.

Managers must make the IM&T Department and the appropriate system managers aware of all new staff, leaving staff and temporary staff, so that log-in domain rights and access privileges can be set as appropriate, at the earliest possible opportunity.

Managers will be responsible for ensuring that their staff are aware of the IT Security Policy, IT Security Procedures and all related documents and that staff are trained as appropriate. They will also ensure that their staff abide by the UHB policies.

Managers must ensure that all staff have sufficient knowledge and training to be able to use systems efficiently and securely before access can be given to UHB systems.

Managers must also take responsibility to ensure that all staff are made aware of their responsibilities under the Data Protection Act (1998), Computer Misuse Act (1990) and Human Rights Act (1998), Privacy and Electronic Communications Regulations (2003), Regulations of Investigatory Powers Act (RIPPA) (2000).

Systems Managers

Managers who are responsible for the administration and management of IT systems as systems managers must comply with all UHB IM&T security policies, guidelines and procedures as set out and agreed.

All Staff

All staff have a responsibility to comply with UHB policies.

All users of any UHB IT facilities and systems must report any IT Security infringements to their manager.

Each individual must ensure that as far as is possible no unauthorised person has access to any data held by the UHB. Also each person must ensure that any physical security measures are properly used.

Staff, who are provided with passwords to access computer systems, must not disclose any passwords to other members of staff.

Staff must not

- Load software packages onto their PC's or laptop's without authorisation from the IM&T Security Office. On no account must 'games software' be loaded on staff PC's or laptops.
- Logon to any computer system using another member of staff's log in details and password.

Staff must

- Ensure that all data is saved to network servers and not to the local device hard drive.
- Ensure that when leaving computers unattended for any length of time they either switch them off, lock the screen or log themselves off. Computers must not be left unattended or accessible to others.
- Staff must ensure that they use the information they have access to in an appropriate manner at all times.

Staff have a responsibility for ensuring the strict confidentiality of the information to which they will have access to as per the codes of conduct.

Failure by any UHB staff to abide by the IT Security Policy and related procedures will be viewed as a serious matter and may result in investigation and possibly lead to disciplinary action which could include dismissal.

Staff will be made aware of information security threats and concerns through explicit reference in job descriptions and contracts of employment.

Contractors/Third Party Agents

Legal contracts will be in place with the relevant agencies and companies such as Data Processor Agreements.

Users not already covered by an existing contract will either require an honorary contract (users carrying out work for the UHB, e.g. Social Workers, non NHS contracted Clinicians) or complete a confidentiality agreement (Third Party contractors employed by the UHB, Agency Staff, Students, and IT Contractors) prior to connection to UHB IM&T facilities.

3. SECURITY OF ASSETS

The UHB will maintain an inventory of the major assets associated with its information systems. Assets will include:

- Physical assets
- Software applications
- Data
- Back-ups

3.1 Physical Assets

Protection of IT equipment (including that used off site) is necessary both to reduce the risk of unauthorised access to data and to safeguard against loss or damage.
Data Centre’s both local and national servers must be protected from power failures through use of uninterruptible power supplies (UPS), with backup generator power.

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

Details of all faults on “maintained” equipment will be recorded by the UHB’s IM&T Help Desks.

3.2 Software Applications

The IM&T Department will monitor all systems and PCs to ensure that all proprietary software products on the Local Area Network are used legally, licenced, and use SNOW as a Software Assett Management (SAM) solution.

In general the number of software installations of a given application e.g. Microsoft Office version xx cannot exceed the number of licences for that application held by the organisation. The UHB has purchased software specifically to monitor levels of usage of all software applications on the network. Regular reviews will be undertaken to ensure adequate licensing.

Copying of proprietary or organisational software, for use on computers that do not belong to the UHB, for any purpose other than authorised business, may infringe copyright and may be in breach of organisational policy. Copying of software in these circumstances may lead to disciplinary action.

Only software licensed to the UHB may be used on UHB equipment. Although it is not strictly illegal to use software legitimately belonging to an individual the installation and use of such software will not be permitted on any UHB equipment.

In the event of a dispute on the authorised validity of software the IM&T Security Manager has the authority to order the removal of any software from UHB equipment.

Software procured from academia cannot be loaded onto an NHS device i.e. students are not able to load university software onto the UHB device due to licencing restrictions.

Free software is not to be downloaded onto UHB computers due to the risk of malware, viruses and trojan’s being introduced and affecting the network.

Staff need to remember that the same restrictions and requirements apply when utilising UHB IT equipment and working at home.

3.3 Data

Equipment (e.g. PCs, Laptops), data and software can be taken off-site but requires authorisation by the appropriate line manager.

Data must be saved to network servers and not to the local devices hard drive.

All laptops must be encrypted.
The destruction of data can only be authorised by the manager of the relevant system that the data is stored on, and “routed” via procurement.

Any storage media (e.g. hard disk, CD-ROM, diskette, magnetic or DAT tape) can only be disposed of after reliable precautions to destroy the data have been taken, and routed via procurement.

3.4 Back-ups

It is the responsibility of individual users to back up any systems that do not store their data centrally.

The IM&T Department undertakes to back up on a daily basis the Network Servers and all centrally held data and will maintain detailed data housekeeping procedures for all systems they are responsible for.

Back-up and archive data will be accorded the same security as live data. All back-ups and archived data will be held off-site at CRI. Back-up data should be able to provide an adequate level of service and recovery time in the event of an emergency.

The IM&T Security Manager and all relevant managers and staff must be informed prior to any recovery from back-up data.

4 SECURITY INCIDENTS

An IM&T security incident is defined as any event that has resulted or could result in:

- The disclosure of confidential information to any unauthorised individual
- The integrity of the system or data being put at risk
- The availability of the system or information being put at risk
- An adverse impact, for example
- Threat to personal safety or privacy
- Legal obligation or penalty
- Financial loss
- Disruption of UHB business
- An embarrassment to the UHB

.

All incidents or information indicating a suspected or actual security breach should initially be reported to the immediate Line Manager and logged on the incident reporting system (e-Datix). In addition, the IT Security Manager or Information Governance Department should be informed for them to determine whether an actual security breach has taken place. Further comprehensive guidance will be developed to support this.

5 SYSTEM PLANNING, PROCUREMENT AND ACCEPTANCE

Procurement procedures must ensure that they encompass security aspects further information can be found in the IM&T Equipment document.

Before any work commences with any non-NHS organisation there must be a Privacy Impact Assessment completed and also UHB’s Data Processing Agreement (DPA) these must be returned to the Information Governance Department.

6 BUSINESS CONTINUITY PLANNING AND RISK ASSESSMENT

Business continuity planning is an organisational issue.

All Clinical Board areas will ensure that they have developed, maintained and tested adequate business continuity plans which will cover the following:

- A documented assessment of how long their users could manage without the relevant UHB system they depend on
- A documented assessment of the criticality of the loss of their system, including the impact of the short, medium and long term on UHB business activities
- Identification and agreement of all responsibilities and emergency arrangements
- Documentation of agreed procedures and processes
- An assessment of how resilience and continuity will be achieved.

The IM&T Department will ensure that it has an up-to-date Business Contingency/Disaster Recovery Plan in place that assesses the criticality of the loss of all systems managed and maintained by the IM&T Department.