Reference Number: UHB 424 **Version Number:** 1.1	**Date of Next Review:** 8th Aug 2020 **Previous Trust/LHB Reference Number:** Trust 133

INFORMATION TECHNOLOGY SECURITY
IM&T BUSINESS CONTINUITY 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 IT business continuity 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	28/08/18	List title and reference number of any documents that may be superseded
1.1	08/08/17	28/08/18	Admin changes to reflect current contact details

Contents Page

1 Introduction

The UHB will face business risks should a disaster occur within its IT facilities. It is essential to understand that disaster recovery is a whole business issue and not solely the domain of IT.

With the pace of implementation of new technology the UHB has become increasingly reliant on systems being continually available and with data remaining secure and confidential.

The reliance of the UHB on IT systems to support the UHB services which it provides means that it is crucially important to plan to protect against disruption and have arrangements in place to recover from a business disruption.

The impact of a short term or a long-term disruption will potentially be wide reaching. Both the UHB as a whole and the individual Departments, including IT, will need to understand and undertake their responsibilities in the event of the need to recover from an interruption in services.

The reliance on IT systems will only increase as technology advances as the UHB introduces ever more sophisticated and Business Critical systems which are fully integrated into working practices.

IM&T have identified to the UHB's Risk Management Group the associated risk to continued business if individual departments do not have a Business Continuity plan to support each of their Business and Clinical Systems when system downtime occurs.

2 Responsibilities

Senior Management

It is the responsibility of appropriate Senior Managers, throughout the UHB, to ensure that they have back up manual contingency arrangements in place to support their services ready to implement once notified of disruption to IT systems.

All Departments

It is the User Departments own Business Continuity Plans that allow continued clinical and administrative services in the event of failure. As such it is only when the IT Department plan is combined with those User Department's manual contingency and recovery arrangements, that they form an effective UHB Business Continuity Plan and Disaster Recovery Plan.

It is the department’s responsibility to ensure their Business Continuity plan, Risk Registry and Audit documentation entries are kept up to date.

IM&T Department

The UHB has a significant number of Critical Business and Clinical Systems which are either managed specifically by the IM&T Department, in association with the NHS Wales Informatics Services (NWIS), or where the system access is supported through the Network inter-connectivity, a combination of the IM&T Department and NWIS.

In addition most UHB Services and Departmental servers are managed by the IT Department.

The IT Department have arrangements in place to prevent, and if required to recover from, disruptions in service for all services that are hosted by the IT Department.

The IM&T Department has put into place many precautions to ensure that systems are protected and consistently scores highly in internal and external IT security reviews.

The UHB IT Disaster Recovery Plan is a vital component of IT Security and is a key feature of maintaining Services throughout the UHB.

3 Business Continuity Planning

The following is not an exhaustive list of all possible inclusions for a Business Continuity process, but should be considered during planning:

- A formal documented assessment of how long the service can provide effective Clinical and/or Business services without access to computer applications hosted on the Network

- A formal, documented assessment of the criticality of each application used, including the impact of the short, medium and long term loss of the system

- Identification and agreement of all responsibilities and emergency arrangements within the service

- Documentation of agreed procedures and processes, and reviewed on a regular basis

- A formal assessment of how resilience and continuity will be achieved

- A test schedule should be drawn up for each contingency plan

- There should be a formal review process of each contingency plan.

- Any change to a contingency plan should be done under formal change control procedures

There should be multiple copies of all continuity plans held both on-site and offsite. Consideration should be given to the possibility of some copies being held by responsible managers at home, to allow immediate reference in off-duty hours.

All continuity plans are subject to review by internal and external audit.

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

Appendix 1

Useful Contacts

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

IG Manager/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