| | |
|---|---|
| **Reference Number:** UHB 431<br>**Version Number:** 1.1 | **Date of Next Review:** 8th Aug 2020<br>**Previous Trust/LHB Reference Number:** T133 |

**INFORMATION TECHNOLOGY SECURITY**
**IM&T CODE OF CONNECTION 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 disposal of IT equipment 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<br>Information Technology Security Policy<br>Information Technology Security Procedure<br>Information Risk Management Procedure<br>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)<br>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 | 30/07/18 | 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

There are a variety of reasons for wishing to connect information systems together, but they usually involve a requirement to exchange data and information.

A Code of Connection (CoCo) is used when the UHB wishes to connect to another “unknown” information system, whereby the UHB stipulating a baseline set of controls to be implemented by the connecting organisation.

The controls are broadly be broken down into the following types:

- ***Technical*** such as implementing an assured barrier between the two organisations
- ***Procedural*** such as ensuring that all security incidents are reported to the partner organisation
- ***Physical*** such as ensuring that the physical security of assets is adequate
- ***People*** such as ensuring that all staff involved have appropriate background and identity checks or appropriate education, training and awareness

When a CoCo is requested or proposed, the UHB IT Services Department will be consulted and will assess the threat the connecting organisation poses. If the IT Security Manager believes that the risks are acceptable, they will authorise the connection

How stringent a code of connection is depends on the level of assurance required between the participant organisations

N3 is the integrated network for the NHS, a combination of broadband connections and network services which are intended to link all NHS sites in England and Wales. The NHS Wales Information Service (NWIS) ensure the UHB comply with Welsh Assembly Government (WAG) NHS security policies in Wales.

# 2 NHS Network Code of Connection Summary

The NHS Network Code of Connection can be summarised as follows:

- The UHB will abide by the NWIS N3 and Non-N3 CoCo through completion of NWIS CoCo issued toolkits

- Access to NHS-wide networking is via NWIS and is protected by authentication controls e.g. NADEX network access code and password
- Links to other systems/networks must be connected through, and comply with, the NWIS CoCo
- Department Managers or corporate management, are responsible for the security of any systems used or network connecting to the NHS-wide infrastructure
- All relevant staff are made aware of their responsibilities in relation to the security of the NHS-wide infrastructure
- Physical access to all NHS-wide network equipment is controlled
- All incidents which constitute a threat to NHS-wide networking services must be reported to the UHB's IT Helpdesk and also inform the IM&T Security Manager as and when they occur
- Advertising or any other form of promotional activity for non-NHS purposes is restricted
- Where direct on-line access to NHS systems is unavoidable, managers must provide the IM&T Security Manager with a written justification statement as to why access is required and not proceed until written approval has been given
- All program files obtained through connection to external services are checked by a virus checking facility and approved by the IM&T Security Manager before being used on any system connected to the UHB's networking infrastructure
- Departments are required to undertake regular access audits to systems and include results in their Business Continuity Department plans. As part of the access audits departments must check with the Information Governance Department that a valid Data Processor Agreement is in place

---

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**

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