| | |
|---|---|
| **Reference Number:** UHB 428<br>**Version Number:** 1.1 | **Date of Next Review:** 20th Sep 2019<br>**Previous Trust/LHB Reference Number:** Trust 133 |

# INFORMATION TECHNOLOGY SECURITY
# IT SECURITY INCIDENT (BREACH) 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's) IT systems that hold confidential and sensitive patient and business information.

The UHB must ensure the safety and security of all its 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 incidents 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<br>Information Technology Security Policy<br>Information Technology Security Procedure<br>Information Risk Management Procedure<br>Electronic Incident Reporting Guide<br>Data Protection Act Policy and Procedure |
| **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 |
|---|---|---|---|
| 03.01 ISOSP09 | | 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

The objective of the Cardiff and Vale University Health Board (the UHB) IT Incident Guidance is to ensure that all staff are made aware of the dangers that can be caused and the potential impact that their action can have on the whole of the IT Network, in an attempt to ensure that any possible risks can be minimised

The UHB acknowledges that the majority of IT security breaches are innocent and unintentional (e.g. user not "logging out" when leaving for the day) and would not normally result in disciplinary action being taken

However, if a breach were deliberate and intentional then the UHB's disciplinary policy would be invoked

The UHB encourages staff to report risks, incidents and 'near misses' and raise concerns about matters which affect the quality of patient care

The UHB Incident Reporting process is easy to follow and accessible by all staff across the IT network via the 'Incident Reporting' icon which is available on PC/laptop desktops.


Evidence of an IT security breach may have been captured by the PC, laptop or server that was being used when the incident took place and therefore must be set apart from the UHB network immediately.

## 2 EXAMPLES OF REPORTABLE INCIDENTS AND BREACHES

### a) Breaches of IT Security

IT Security Department - Responsible Officer IT Security Manager

Examples:

- Virus or other security attack on IT equipment, systems or networks
- Breach of Information Technology (this includes any breaches of any of the following IT Security documents
  - i. IT Security Policy,
  - ii. IT Security Procedures and all related
  - iii. IT Security Control documents

If the investigation of the incident requires access to a user's IT account e.g.in a case of suspected downloading of illegal material, this must be escalated to the Head of IT

**b) Information (Data) Security Breach (Data Protection Act Breaches).**
Information Governance Department (Responsible officer - Head of Information Governance).

Examples: loss or unauthorised disclosure of

- Medium or high risk confidential information such as patient medical records, staff personnel records
- Any personal identifiable data (PiD) such as name address date of birth etc.
- Information and records of operational, legal or evidential value to the UHB

**c) Breaches of physical security such as loss or theft of devices and /or equipment:**

IT Security Department (liaising with Site Security Manager and Information Governance Department). Where appropriate the police will be informed.

Examples:

- Loss or theft of laptop, PC's, Netbooks, Printers UHB mobile phones, personal phones / devices with UHB software loaded.
- Attempted break in to secure server, secure area or area where confidential records are stored such as medical records.

## 3 RESPONSIBILITIES

All staff members have a responsibility to report suspicious activities, incidents or suspected security weaknesses affecting the organisations systems or data.

Examples of these include compromise to an IM&T system due to a virus outbreak, inappropriate access to patient / person identifiable or business sensitive information, suspected loss of confidential data or abuse of the internet or email systems. All incidents should be reported via the UH's Incident reporting policy.

All users of the UHB's IT network have the following personal responsibilities.

**All staff must:**

- Report **immediately** any IT security incident or breach, whether suspected or detected
- If an IT security incident occurs then in order to preserve any incident evidence **immediately** isolate the PC/laptop from the UHB IT network and power supply.
- Make every possible effort to ensure that no actual or potential security breach occur as a result of their actions
- Ensure that desks and PC screens are clear of any confidential information before leaving their workstations.
- Ensure that when leaving their PC unattended they lock the screen.

- Ensure that screen cannot be read by unauthorised individuals when working in public areas
- Ensure that they do not share passwords

PCs should also be closed down in the evenings and at weekends, and desks kept as clear as possible with any confidential information being locked securely away.

**All staff must not:**

- Disclose their passwords or allow anyone else to use their passwords
- Allow another user to work on a PC/laptop whilst they are still logged on
- Disclose Patient Identifiable Information (PID) or sensitive business information to third party agents.
- Store PID or sensitive business information data on PC/laptop local drives or removable devices (CDs/DVDs, Memory Sticks, Portable Drives etc)
- Download email attachments from an unknown, suspicious or untrustworthy source.
- Open any files attached to an email if the subject line is questionable or unexpected.
- Download files from the internet unless for business purposes and if this is required advice must to be sought from the helpdesk before any download it attempted.

**Line Managers must:**

- Ensure that their staff receive the relevant training they require before they access any UHB equipment or are provided with access to the network
- Ensure staff are only given access to the systems they require which are necessary for their job role.
- Ensure that all staff read and sign agreement with the IT Security Policies, Procedures and relevant guidance documents before accessing any equipment and the network.
- Ensure that all staff read and sign the UHB confidentiality Code of Conduct

IT security and confidentiality issues **MUST** be included in general training

**The UHB is responsible for ensuring:**

- IT Incidents are investigated in a timely manner
- Outcomes of investigations to be forwarded to appropriate divisions within the UHB for further investigation or follow on actions, as appropriate

**The IT Security Manager is responsible for:**

- Continual monitoring and re-categorising the incident as the investigation progress and regularly update the Head of IT of any implications for the UHB
- Ensuring documented records of the incident(s) are retained and stored securely for audit review
- Providing updates during the investigation to:

  - ❖ The relevant Line Manager to determine whether any disciplinary action is necessary.
  - ❖ Director of Finance immediately should the classification become level 3 and above.
  - ❖ Information Governance if there is a loss of patient/personal identifiable data/information and/or UHB personal identifiable data via. CAV.IG.DEPT@WALES.NHS.UK

## 4 IT SECURITY INCIDENTS EXPLAINED

**What is an IT Security Incident?**

An IM&T security incident is an event which may result in:

- Degraded system integrity e.g. causing a virus to enter the system.
- Loss of system availability e.g. e-mail not working.
- Disclosure of confidential information e.g. password sharing.
- Disruption of activity e.g. inappropriately deleting files from a network drive.
- Financial loss e.g. theft of laptop.
- Legal action e.g. inappropriate disclosure of patient information.
- Unauthorised access to applications e.g. unauthorised access to financial or clinical systems.
- A serious untoward incident (SUI) concerning person identifiable data (PID), such as loss or breach of confidentiality, these incidents must be reported appropriately and handled effectively.

## 5 WHAT TO DO IF AN IT SECURITY INCIDENT IS SUSPECTED OR DETECTED

**Action to be taken by Staff** Report **immediately** any IT Security Incident:

1 Contact a UHB IT Helpdesk -
UHW (02920 745073) IT.Helpdesk.UHW@wales.nhs.uk
UHL (02920 715218) Llandough.Helpdesk@wales.nhs.uk

2 Complete an e-Datix Incident Report – 'Incident Reporting' icon is available on PC/laptop desktops.


3 Send a notification e-mail to the IT Security Manager - CV.IMT.SECURITY@WALES.NHS.UK

This initial e-Datix Incident Report categorisation of an IT Security Incident is based upon the user's personal evaluation of the IT security incident.

In order to preserve any incident evidence and to ensure its integrity the following should be adhered to:

1 Switch off all devices which were involved in the incident by removing the power cable from the wall socket (DO NOT log off or power down the device)

2 If possible remove the device and store in a secure area (or remove power cables, keyboard and mouse)

3 Arrange for the password of the account that was being used when the incident occurred to be reset

**IM&T Department Actions**

- Review the e-Datix Incident Report which is based upon the user's personal evaluation of the IT security incident
- Initial categorise the IT security incident within one of the classifications (from 0-5) as defined in the IM&T Incident Classification Chart below
- During the course of the investigation re-evaluate periodically the incident categorisation as the incident may need to be re-categorised as new information or impacts are discovered
- Report as appropriate at closure of the IT security incident investigation

Any staff member reporting an IT security breach/incident must have unhindered access to the Head of IT if that staff member believes the breach has been as a result of an action by the IT Security Manager, a member of senior management, or a member of the professional medical staff.

The IT Security Manager must be available to any member of staff reporting a breach in IM&T Security. The anonymity of the member of staff must be ensured during the investigation, irrespective of whether or not the event turns out to be a genuine breach or a false alarm.

It is most important that the reporting process remains as easy as possible, especially where the offence is being committed by someone in a position of trust. It

is possible that the offender may be in a position of authority over the staff member making the report. Therefore, it is essential that no adverse pressures be brought to bear on the staff member as a consequence.

## 6 IM&T INCIDENTS CLASSIFICATIONS

Risk assessment methods commonly categorise incidents according to the likely consequences, with the most serious being categorised as a 5, e.g. an incident should be categorised at the highest level that applies when considering the characteristics and risks of the incident.

| 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| No significant reflection on any individual or body Media interest very unlikely | Damage to an individual's reputation. Possible media interest, e.g. celebrity involved | Damage to a team's reputation. Some local media interest that may not go public | Damage to a services reputation/ Low key local media coverage. | Damage to an organisation's reputation/ Local media coverage. | Damage to NHS reputation/ National media coverage. |
| Minor breach of confidentiality. Only a single individual affected | Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted | Serious potential breach & risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected | Serious breach of confidentiality e.g. up to 100 people affected | Serious breach with either particular sensitivity e.g. sexual health details, or up to 1000 people affected | Serious breach with potential for ID theft or over 1000 people affected |

### High, Medium and Low Risk IT Security Incidents

**"High"** risk incidents pose a severe risk to the UHB information and will be classified as critical security incidents. These incidents include, for example, a widespread risk of compromising systems or compromising sensitive or critical data.

**"Medium"** risk incidents pose a medium risk to the UHB information and as such will be classified as medium-severity security incidents. These incidents include, for example, compromising an information system that does not contain sensitive data and will not pose a widespread risk to other organisations information systems.

**"Low"** risk incidents pose a low risk to UHB information and will be classified as low-severity security incidents. These incidents include, for example, compromise of a system that does not contain critical or sensitive data or pose the risk of compromising other systems.

Cardiff and Vale University Health Board Risk Assessment Scoring and Matrix

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 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