Reference Number: UHB 319 **Version Number:** 1	**Date of Next Review:** 10 Jun 2019 **Previous Trust Reference Number:** T133

Information Technology Security
Authorised Users 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 authorised users 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	
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	10/06/2016	05/08/2016	New UHB document supersedes Cardiff and Vale NHS Trust IT Security Policy (ref 133) – Appendix 3 Authorised Users Procedure
03.01 ISOSP04		04/2008	Original Document

Contents Page

1 Introduction

Due to the sensitive personal data that many of the UHB IT systems hold, users of UHB computers must agree to comply with the UHB's IT security policies and procedures and obtain authorisation from their Line Manager before access will be granted.

Access to UHB computer systems may require mandatory training before an account can be created.

2 Domain Accounts

2.1 All users must complete the electronic IT User Security Form. The form is completed by accessing the IT Departments Help Desk page on the UHB's Intranet site. Authorisation can only be made by a manager with budget holding responsibility.

http://helpdesk/helpdesk/main.html.

2.2 On completing the electronic form an email is generated complete with an attachment. The attachment contains authorisation from the manager and this must be emailed to the IM&T Security Office. The IT Security form should be printed and placed in the user's personal folder. On receipt of the authorisation email the IM&T Security Office will;

- Check authorisation from the system "owner" or departmental manager to use the service and that the level of access requested is consistent with the systems security policies.
- Authorise the IT Help Desk to create the domain account.
- the IT Help Desk will issue network account credentials i.e. user name and password

3 Password Management

- Each member of staff will have their own unique individual user name and password which must not be shared.
- Passwords should not relate to the user or to the system being accessed.

- Users will be issued with a temporary password, users will be forced to change the temporary password when they log on to the network for the first time.

- Users will be allowed to select and change their own passwords.

- Application access passwords to have a minimum length of 8 characters and must contain three of four character types: lowercase (e.g. abc) uppercase letters (e.g. ABC) numbers (e.g. 123) symbols (e.g. ?!%). In the case of an application that cannot comply the system manager is responsible for the security of the access to the application

- Domain password changes will be enforced at 90-day intervals (users will be automatically prompted when password renewal is due).

- Best practice requires users to be limited to 5 unsuccessful log-on attempts, after which the account is locked; users can wait 30 minutes before retrying or contact the IT Help Desk to have the password reset before system access can be re-instated. In the case of an application that cannot comply the system manager is responsible for the security of the access to the application.

3.1 In addition, users accessing systems containing patient-identifiable data, or users with system supervisory privileges should have a 'time-out facility within Windows to avoid unauthorised access when staff members are temporarily absent from their workstation.

4. Internet Users

4.1 Staff that require access to the Internet can only do so by connecting to the UHB's network.

4.2 All internet users will be provided with a copy of the UHB's Internet/Email Policy which they must adhere to.

5 Patient Management System (PMS)

PMS can only be accessed via a network account. It may be necessary therefore to request a network account at the same time that you request a PMS account.

Access to PMS will only be permitted after appropriate training has been given.

Applying for a PMS account uses the same processes as applying for a domain account (see Section 2) with the following exceptions.

- You need only complete the sections of the form relevant to your request i.e. you do not need to fill in the request for network access if you already have a network account.
- the IT Help Desk will alert the PMS Implementation Team.
- PMS account details will only be issued when training has been completed in the classroom by one of the IT Trainers.

Further information on PMS access is available from the PMS Implementation Team.

6 Clinical Portal

The Clinical Portal will give users access to inpatient/outpatient activity, Results and Reports, Clinical Letters, A&E Episodes and Radiology Images. Access to this area is restricted to authorised personnel who have a Clinical Portal account.

Clinical Portal personal accounts can only be obtained by registering user details on the Clinical Portal intranet site. Users who have registered will not be able to access patient details until they have been authorised to do so by the Department's ''Super User'', who will ensure that new users have completed the online training and agree to the acceptable use policy.

7 Access to Systems Not Directly Managed by the IM&T Department

Examples of IT Systems not managed by the IM&T Department;

Child Health
Pharmacy
Paris
PROTON (Renal System)

EuroKing to use the service and (Maternity System)
RADIS (Radiology Patient Administration/Reporting System)
TELEPATH (Pathology)

7.1 Users will need to contact the administrator of the system that they wish to connect to in order to obtain access.

7.2 The system administrator will be responsible for operating and maintaining an access control process.

7.3 All external systems must provide equivalent or greater security as that described in previous sections.

8 Current Users/Additional Services

Existing users who require access to other UHB computer systems must contact the IT Help Desk to discuss their requirements. Depending on the requirements users will be guided on the appropriate process to the additional services required.

9 Third Parties

9.1 Users employed at other NHS organisations that require access to Cardiff and Vale UHB computer systems must complete the Firewall Registration Form. Access will only be granted once the form has been authorised by their line manager and the administrator/manager of the Cardiff & Vale NHS UHB IT system that they require access to.

9.2 Non NHS users, such as local authority staff and agency staff, must obtain an honorary contract of employment.

9.3 Bank staff must complete a confidentiality agreement before access to the network will be granted.

9.4 Contractors must complete the data processor agreement before being allowed to connect to the system they maintain.

For further information on Third Parties accessing the network contact the IM&T Security Office.

10 Account Removal

It is the manager's responsibility to inform the IM&T Security Office when a member of staff changes jobs or leaves the organisation. This should

be done as soon as a termination date is known in order that archive arrangements can be made and no data is lost.

The IM&T Security Manager will immediately authorise the IT Help Desk to remove the access rights of any staff who have changed jobs or left the organisation or if it is suspected that an account is being used inappropriately.

11 I.T. Security Code of Practice

Users will:

1. Only access and use authorised applications and services as provided by their Manager.

2. Users are not permitted to access any other users password to access UHB services.

3. Always log out whenever work has been completed.

4. Take precautionary measures to avoid any unauthorised access to or modification of data under their control.
   This includes activity protecting PCs left logged-on to the system while the user is temporarily absent from their workplace (activated protected screensavers).

5. Always save data to the network server and **NOT** the hard disk of the local device and ensure that regular and effective back-up procedures are in place. It is the responsibility of all users to ensure that they comply with relevant procedures to recover lost data in the event of a system failure. System users should therefore liaise with the Manager regarding the frequency and method to be used.

6. Change their password regularly, passwords should only remain operational for a maximum of 90 days.

7. When terminating their employment with the UHB, ensure that any password associated with any system is passed on to their Manager. A further requirement is also to ensure that any archived data held on external media away from the system is surrendered to their Manager.

8. Be responsible for the security of their system passwords, passwords must not be disclosed to a third party or written down.

If you suspect that your password has been compromised you should immediately change it.

9. Ensure that they comply with the UHB's Email and Internet policy when using email and internet services.

10. take all reasonable care of allocated PC/Laptop and printer equipment to avoid as far as possible any potential security incident arising.

11. Report system faults to their appropriate user support and not attempt to rectify faults on their own as more serious damage to the system or its components may result.

12. Not import, copy or install PC software on equipment without prior authorisation of the system manager.

13. Users responsible for or whose conduct contributes towards any breach of security of the system may be liable to disciplinary action under the UHB's Disciplinary Policy, the Data Protection Act 1998, the Computer Misuse Act 1990 and/or the Computer Crimes Act 1997.

14. Also be responsible where applicable for adherence to the Data Protection Act as well as UHB's IT Security Policy, rules and security guidelines that will be publicised and may be periodically revised. These can be obtained from the UHB Intranet and/or IT Security Office.

15. Report any perceived breaches of security (actual or attempted) to the system manager and/or IT Security Manager, who will decide whether any further investigation is required.

The Data Protection Act 1998

Protection of data about individuals is now a requirement of the Law. The Data Protection Act 1998 which is in force lays down that: -

- data shall be obtained and processed fairly and lawfully
- data shall be held only for specific purposes and not used or disclosed in any way incompatible with these purposes

All persons that use information on a computer or produced from a computer have an obligation to see that it is not passed on in any unauthorised way.

This means, among other things, that printouts and microfiche must be treated carefully and that staff must not disclose personal information obtained from computers or any computer output in any way other than as required for the discharge of their duties to the UHB.

If an individual is found to have made any unauthorised disclosures of personal information they can face prosecution.

If you are in any doubt as to which disclosures are authorised, ask to see a copy of the UHB's registration covering your work. No disclosure that is not covered by this registration or one of the exemptions under the Act is permitted.

Remember

TREAT PERSONAL INFORMATION WITH CARE

DON'T PASS ON PERSONAL INFORMATION TO UNAUTHORISED PERSONS

All non-routine requests for access to personal information should be passed on to the UHB's Information Governance Department without delay who will see that the request is handled within the legal time limit.

Use of Non UHB Computers

Staff wishing to use such computers for any aspect of NHS business must ensure by discussion with the UHB's Information Governance Department proposed activities comply with the registrations, Policies and Code of Practice. An appropriate user manual will specify the particular arrangements for the use envisaged.

If you have any queries please contact the Information Governance Department at CV.IG.DEPT@WALES.NHS.UK

The Data Protection Act 1998 can be found at:
http://www.legislation.gov.uk/ukpga/1998/29/contents

The Computer Misuse Act 1990

Background

The Computer Misuse Act was created following some controversy in the mid to late nineteen eighties. At this time, hacking was not an offence and the hacker was relatively free to attempt to break into computer systems, if he or she had the intellect to bypass the various security measures employed by the system owners. Whilst hackers may have been viewed as a minor irritation, some are more daring and others potentially harmful. Damage to data is being caused and there is perhaps an understandable concern that hacking has developed into something much more serious.

This Act came into force to make provision for securing computer programs and data against unauthorised access or modification. Authorised users have permission to access certain applications and data. If users go beyond specified bounds then an offence has been committed. The Act makes provision for accidental transgressions, as well as covering fraud, extortion and blackmail. It is worth emphasising that whilst the three offences are not the most serious in British law, each offence is punishable by a period of imprisonment. Section 2 and Section 3 offences are what are termed arrestable offences and an individual may be arrested without warrant by a police officer if the police officer has reasonable suspicion that they have committed that offence. These offences are more serious than the Section 1 offence.

A Royal Commission was set up to look at the whole area of computer misuse. As a result of the findings and recommendations of the Commission, the Computer Misuse Act 1990 was enacted.

The Computer Misuse Act 1990 can be found at:
http://www.legislation.gov.uk/ukpga/1990/18/introduction