Access to Information Systems Procedure

Please note: This Procedure is currently under review by ISG as part of a Transalpine approach to policy alignment with the CDHB. If you have any questions regarding this document please contact the Chief Information Officer in the first instance.

1. Purpose

This Procedure outlines the process for accessing the West Coast District Health Board (WCDHB) Information Systems.

2. Application

This Procedure is to be followed by all staff members and contractors of the WCDHB.

3. Definitions

For the purposes of this Procedure:

User is taken to mean any individual having authorised access to WCDHB Information Systems, whether internally or externally, and includes both staff members and contractors.
Information Systems is taken to mean any networked, stand alone, or portable workstation or personal computer and any peripheral devices attached to such a machine.
Data is taken to mean any information stored electronically in any format.

4. Responsibilities

For the purposes of this Procedure:

All ***WCDHB staff members and contractors*** are required to:
- ensure they abide by the requirements of this Procedure.

5. Resources Required

This Procedure requires:

i) WCDHB Information Systems

6. Process

1.00 Introduction

1.01 Access to the West Coast District Health Board's (WCDHB) Information Systems is an important part of organisational facilities and if properly used can provide an efficient and effective means of communicating internally and externally. It is critical that WCDHB protects information resources and information processed, stored, or transmitted via the WCDHB Information Systems. Sensitive information accessed via WCDHB Information Systems is to be safeguarded against unauthorised disclosure, modification, access, use, destruction, or delay in service.

1.02 WCDHB is committed to a number of strategic initiatives, which include the provision of secure, consistent, sound, and stable information systems that will minimise risk and support the business objectives of the organisation.

As a result every effort will be made to ensure that all data which is stored centrally (on approved networked drives) is secure, backed up, and accessible. This commitment cannot be made for stand-alone machines or non-networked hard drives.

2.00 Data Storage

2.01 It is a mandatory requirement that, as the network drives are provided, data must be moved from network drives to individual PC hard drives. WCDHB data is not, under any circumstances, to be stored in individual Personal Computer (workstation) hard drives. In the absence of network facilities, the staff member who uses the machine must maintain data security for locally stored data.

3.00 Information System Access

3.01 Individual Service/Unit/Department Managers are responsible for authorising access to the WCDHB Information Systems for staff members they are responsible for.

3.02 All WCDHB staff members shall:

i) be provided with appropriate training in the use of the information system that their Manager has determined will be required by the user in order for that staff member to complete their duties.

ii) on completion of their training, be provided with a unique username and password. This username and password is the responsibility of the staff member or contractor and will provide access to the information system that their Manager has determined will be required by the staff member in order for that staff member to complete their duties.

iii) be responsible for ensuring that their Username and Password are not know to any other person and that their password is changed at regular intervals.

iv) be held responsible for all messages or communications generated from their account and will be responsible for all transactions carried out using their account.

v) be aware of and understand their liabilities and responsibilities under the laws of New Zealand and the Policies and Procedures of WCDHB.

vi) only access a WCDHB Information System where they have some legitimate reason for doing so, most often in connection with their lawful employment duties and functions, or when instructed to do so by their Manager or another WCDHB Manager.

vii) not access a WCDHB Information System for personal purposes (with the exception of Email and Internet for which personal use is defined in the *WCDHB Email Use Procedure* and the *WCDHB Internet Use Procedure*).

3.04 Many staff have ready access to patient health information via the electronic records. Obtaining access to this information to provide ongoing care and treatment, or for administrative purposes is an acceptable and legitimate use of the information.

However, staff may not look up their own results, appointments, referrals etc or information pertaining to relatives or friends without following the appropriate WCDHB Procedures relating to requesting personal health information.

3.05 The inactive life of a user's account is 120 days. All inactive accounts are deactivated after this time.

3.06 Users will be allowed three attempts to login before their account is locked, and will only be unlocked by a WCDHB Information System Administrator.

4.00 Contractors

4.01 Contractors may use privately owned computer equipment on WCDHB facilities on the clear understanding that WCDHB takes no responsibility for privately owned computer equipment used on its facilities. The relevant Service/Unit/Department Manager is responsible for ensuring that contractors are aware of this requirement prior to their arrival at the WCDHB facility.

4.02 The Information Technology Department shall:

i) be responsible for ensuring the security and integrity of WCDHB information with regard to contractor access.

ii) ensure that data or information belonging to the WCDHB is removed from contractor equipment before it leaves WCDHB facilities.

5.00 Passwords

5.01 Strong passwords are critical to computer security. They are the first line of defence for user accounts. A poorly chosen password (easy to guess) or one left in open view on a post-it note could cause the entire network to be compromised.

5.02 Users must note that passwords are for their own personal use and must not be shared or disclosed to anyone.

5.03 It is a breach of this Procedure for any user to misuse their own or other user's password. If any such misuse results in a user knowingly elevating their system privileges above those that they have been authorised to use then this will be considered an act of gross misconduct.

5.04 All system-level passwords must be changed every four months.

5.05 All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at least every four months.

5.06 If a password has expired and is not changed within 30 days, the account is automatically disabled.

5.07 User must have a password that is unique from all other accounts held by that user.

5.08 Passwords must not be inserted into email messages or other forms of electronic communication.

5.09 All user-level and system-level passwords must be aware of how to select **strong password that** conform to the following password construction guidelines:

- **A strong password has the following characteristics:**
  - It is least six characters long.
  - It includes upper and lower case letters (e.g. a–z, A–Z); digits and other characters: ! @ # $ % ^ & * ( ) _ + | ~ -= \ ` { } [ ] : " ; ' < > ? , . /)
  - It is not a word in any language, slang, dialect, jargon, etc.
  - It is not based on personal information, names of family, etc.

- **Weak passwords have the following characteristics:**
  - The password contains less than six characters.
  - The password is a word found in a dictionary (English or foreign).
  - The password uses names of family, pets, friends, co-workers, fantasy characters, etc.
  - The password uses computer terms and names, commands, hardware, software.
  - The password uses predictable words e.g. 'West Coast DHB'
  - The password uses personal information such as addresses and phone numbers.
  - The password uses word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - The password uses names of any of the above spelt backwards or preceded/followed by a digit (e.g. secret1 - 1secret).

5.10 Users are not to use the same password for WCDHB accounts as for other non-WCDHB accounts (e.g. personal internet account, online banking, online shopping, etc).

5.11 Users are not to:

i) Reveal a password over the phone to **ANYONE**.
ii) Reveal a password in an email message.
iii) Reveal a password to their Line Manager.
iv) Talk about a password in front of others.
v) Hint at the format of a password (e.g. 'my family/whanau name').
vi) Reveal a password on questionnaires or security forms.
vii) Share a password with their family/whanau members.
viii) Reveal a password to co-workers while on holiday.
ix) Write **passwords** down and store them anywhere in their work area

x) Store **passwords** in a file on ANY computer system (including PDAs or similar devices) without encryption.

5.12 In the event that an account or password is suspected to have been compromised, the incident must be reported to IT Help Desk immediately. All passwords are to be changed immediately.

6.00 Breaches

6.01 Any possible breaches of this Procedure are to be reviewed by the Manager – Information Technology and the Quality Assurance and Risk Manager to determine if a breach has actually occurred.

6.02 Where the Manager – Information Technology and the Quality Assurance and Risk Manager agree that a breach has occurred, then it is to be reported (as soon as practicable) to the relevant General Manager. (*For the purposes of Sections 1.07 and 1.08 the relevant General Manager is the General Manager who has responsibility for the Unit/Department/Service within which the computer on which the breach was detected is located*).
Where the detected breach involves a General Manager, then this is to be reported to the Chief Executive Officer. Where the detected breach involves the Chief Executive Officer, then this is to be reported to the Chair of the Board.

6.03 All breaches detected are to be investigated at the discretion of the relevant General Manager/Chief Executive Officer/Chair in accordance with the WCDHB Staff Discipline Procedure.

7. Precautions and Considerations

➔ Individual Service/Unit/Department Managers are responsible for authorising access to the WCDHB Information Systems for staff members they are responsible for

➔ Users are responsible for ensuring that their Username and Password are not know to any other person

➔ The WCDHB takes no responsibility for privately owned computer equipment used on at it's facilities

8. References

There are no references associated with this Procedure.

9. Related Documents

WCDHB Email Use Procedure.

WCDHB Internet Use Procedure.

WCDHB Staff Access to Personal Health Information.

Revision History	**Version:**	7
	Developed By:	Information Technology Manager
	Authorised By:	Chief Executive Officer
	Date Authorised:	July 2001
	Date Last Reviewed:	June 2019
	Date Of Next Review:	June 2020