



# Access to Information Systems Procedure

Procedure Number

CHC-ITP-0001

Version Nos:

5

## 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:

- WCDHB Information Systems

## 6. Process

1.00 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.

1.01 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.

1.02 It is a mandatory requirement that, as the network drives are provided, data must be moved from individual hard drives to network drives. WCDHB data is not, under any circumstances, to be stored in individual Personal Computer (workstation) hard drives.



## Access to Information Systems Procedure

Procedure Number

CHC-ITP-0001

Version Nos:

5

In the absence of network facilities, the staff member who uses the machine must maintain data security for locally stored data.

- 1.03 Individual Service/Unit/Department Managers are responsible for authorising access to the WCDHB Information Systems for staff members they are responsible for.
- 1.04 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*).
- 1.05 The Information Technology Department shall:
- i) be responsible for ensuring the security and integrity of user accounts with regard to systems management.
  - ii) ensure that data or information belonging to the WCDHB is removed from contractor equipment before it leaves WCDHB facilities.
- 1.06 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.
- 1.07 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.
- 1.08 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).*



## Access to Information Systems Procedure

Procedure Number  
*CHC-ITP-0001*

Version Nos:  
**5**

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.

- 1.09 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

<b>Revision History</b>	<b>Version:</b>	5
	<b>Developed By:</b>	Information Technology Manager
	<b>Authorised By:</b>	Chief Executive Officer
	<b>Date Authorised:</b>	July 2001
	<b>Date Last Reviewed:</b>	November 2009
	<b>Date Of Next Review:</b>	November 2011



# Access to Information Systems Procedure

Procedure Number

*CHC-ITP-0001*

Version Nos:

**5**

**This Page Is Deliberately Blank**