Information Security – Access Control

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	Information Security Manager
Document Owner Name	Chief Information Officer (CISO)
Document Owner Title	Geoff King
Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.	

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version
2.0	Jeremy Marshall	23/11/2017	Final Version

Contents

1. Overview

1.1 Purpose

Access control will prevent unauthorised persons accessing sensitive information, ensuring it remains confidential. Authorised users will be able to view and process only the information they are entitled to and have a need to access.

The Waikato DHB must have in place policies and procedures to assess and manage the ongoing suitability for employment of all staff and contractors and is required to ensure that all employees, contractors and temporary staff who require ongoing access to its information assets and resources;

- Are eligible to have access.
- Have had their identity established.
- Are suitable to have access.
- Are willing to comply with government policies, standards, protocols and requirements that safeguard that agency's resources (people, information and assets) from harm.

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as "Users" in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

Physical access into buildings and sections of the hospital.

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the DHB must comply with the DHB's policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.

- Information Services are responsible for:

  (a) Maintaining and advising the Waikato DHB's Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

  (b) Developing access standards to protect Waikato DHB's information assets from unauthorised use, accidental damage and/or malicious attack that could result in loss of information, damage to critical applications, loss of revenue, and/or damage to the DHB's public image.

  (c) Providing procedures and process to manage the provision, management and audit of access.

  (d) Developing procedures to provide and revoke access rights at short notice, to support the requirements of locums and others for temporary access.

  (e) Monitoring access and ensuring a regularised audit program is implemented to validate that all access allocation is documented and traceable and allows verification that the level of access granted is appropriate.

  (f) Ensuring users' access rights are appropriate to their task and are authorised and removed or modified upon termination of employment or change of role.

  (g) Ensuring users are only able to access the resources and services required to carry out their duties.

  (h) Periodically auditing actual user access privileges against authorisation records to ensure that unauthorised privileges have not been obtained.

- Business Owners and Users are responsible for:

  (a) Ensuring compliance with the Information Security Policy and Access Control Protocol.

  (b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.

  (c) Ensuring staff have signed information confidentiality and disclosure agreements along with terms and conditions of employment.

  (d) Ensuring user access to Waikato DHB information assets and resources is for authorised and valid reasons only.

  (e) Ensuring users' access rights are appropriate to their task and are authorised and removed or modified upon termination of employment or change of role.

  (f) Notifying Information Services of new staff requirements, staff terminations and transfers in a timely manner.

(g) Preventing any inadvertent or unauthorised release of information, particularly from unattended equipment, by terminating active sessions, locking the screen or logging off when finished.

(h) Promoting and maintaining a 'clear desk and screen' policy to protect paper and information on computer displays being seen by those who should not have access to the information.

4. Standards

4.1 General

- All Waikato DHB information assets and resources providing access to or storage of sensitive information must be password protected and access to these assets provided subject to an established authorisation process.
- Access to information will be managed in a way that is compliant with all applicable data protection, security and privacy legislation.
- Access control will be consistent across all systems and all access rights will be granted on a "need to have" basis. Any access that is not expressly granted is forbidden.
- The Chief Information Officer (CIO), or delegate, shall authorise network connections between Waikato DHB gateways and other organisations.
- Computers in the Waikato DHB may only access the Internet via approved gateways.
- The system will display a logon banner that requires the user to acknowledge and accept their security responsibilities before access to the system is granted.
- Users must also be made aware that system usage is being monitored and the ramifications for violation of the relevant policies.
- Links to the Waikato DHB policies must be easily accessible to all users.
- All access rights will be subject to formal authorisation and the level of access control will be proportionate to the sensitivity of the information and the identified risks relating to the information asset or resource.
- Access control roles will be segregated so the same person is not performing more than one of these roles – access request, access authorisation, access administration.
- Role based and standard access profiles should be used to simplify management of access rights.
- All users will have uniquely identifiable accounts assigned to them to ensure individual responsibility.
- Users' access rights must be appropriate to their task and be authorised and removed or modified upon termination of employment or change of role.
- All access rights must be monitored, audited and reviewed on a regular basis to ensure they are still appropriate to the users' needs.

- Privileged access rights should be reviewed on frequent basis as they pose a higher level of risk and should be assigned to a different user ID from the one used for standard user access.
- Privileged access must be explicitly authorised before it is granted and wherever possible, the need for privileged access should be minimised by the use of system routines.
- Privileged user accounts (administrator rights) are only used for the special activities requiring their use, and not for day-to-day activities or over-ride access.
- External support staff and/or third party suppliers will be setup with temporary access rights for a fixed period and their accounts are set to expire at the end of that period.
- External support staff and/or third party supplier accounts will be separated from internal staff accounts for easier identification and management.
- Generic accounts will only be used to provide access to basic network and/or desktop functions. Access to clinical and/or corporate applications require users to logon using an individual user identifiable accounts.
- All user access will be disabled upon suspension or cessation of employment or modified upon change of role. Managers can liaise with the IS Service Desk for temporary arrangements to allow email redirection and file management. Logins, stored email and personal directories will be deleted two months following the departure of an employee.
- Access to documentation about installations and computer systems is restricted to authorised personnel. All documentation, software, hardware, commercial and personal information held by Waikato DHB that can be used to eliminate, bypass, or otherwise render ineffective the security safeguards must be protected to prevent unauthorised disclosure, modification, or destruction.
- The IS Service Desk shall periodically check actual user access privileges against authorisation records to ensure that unauthorised privileges have not been obtained.
- The IS Service Desk shall periodically review all security records and identify users who have not accessed the system. After consultation with the user's Line Manager, and unless there are good reasons, the IS Service Desk shall remove access from users who have not logged on for 90 days.
- Access for Third Parties will be disabled upon completion of the expiry period or earlier on receipt of notice from the relevant Waikato DHB Manager.

4.2 Network Connectivity

- All connections to the Waikato DHB network must be requested through the Information Services department and be performed by Information Services staff or an (IS) approved third party.
- All network attached devices must be asset registered and adhere to Information Services Technology Standards including, but not limited to, requirements for anti-virus software, operating system patching, image management, software/firmware upgrades, cabling, IP addressing and Change Control.

- Access to Waikato DHB information assets and resources will be granted based on role and appropriateness to the task.
- All accounts used for handling and management of sensitive information, regardless of the device used, are to be restricted to that purpose.
- Access to Waikato DHB network resources will only be provided following receipt of a completed computer access request form signed by the individual and their line manager, or for Third Parties, the individual and the relevant Waikato DHB manager.

4.3 Secure Log-on Procedures

- Initial log-on will be controlled by a secure procedure designed to minimise the possibility of unauthorised access and will avoid giving any information that may assist unauthorised access.
- After a predetermined number of consecutive invalid sign-on attempts, the user account should be locked requiring resetting by the IS Service Desk.
- Both successful and unsuccessful log-on attempts should be logged and reported.
- After a prescribed period of inactivity (maximum 15 minutes) the screensaver will activate and the workstation will be locked; it can then only be unlocked by the logged-on user or an administrator.
- For particularly sensitive applications, consideration should be given to restricting the times the system can be accessed, such as restricting to office hours only.

4.4 Password Management System

- Password management systems will:
  - Permit users to change their own passwords and include a confirmation process to allow for typing errors.
  - Enforce the use of “quality” passwords as per section 4.7.
  - Enforce periodic password changes
  - Retain a record of at least the last twelve passwords used and prevent re-use
  - Force users to change initial or temporary passwords at first log-on.
  - Store and transmit passwords in encrypted form.

4.5 Passwords

- Logins and passwords are created to ensure secure access to information assets and resources and are for the sole use of the user they are allocated to.
- Passwords will be stored and transmitted in an encrypted non-reversible format.
- Password information must not be communicated via unencrypted emails.
- Logins and passwords may not be shared. Where misuse of information or system resources occurs that can be traced to a user, the user who owns the login will be held responsible.
- Passwords must not be displayed on computer screens or in clear sight.
- Passwords must be changed every 90 days.

- Password length is required to be 8-32 characters, using a combination of case-sensitive alphanumeric characters (a-z, A-Z, 0-9) and special characters (! $ % #).
- Passwords must not contain personally identifiable information, including names (such as partners, children or pets), dates (such as birthdays or anniversaries) and other ID numbers (such as staff ID, NHI, IRD, bank account or car registration).
- Passwords will not be reused for a minimum of 12 cycles.
- Access lockout will be enforced after 3 failed attempts.
- Sessions will be automatically closed down with a locked screensaver requiring re-authentication after 15 minutes of user inactivity.
- Devices used off-site, including laptops, mobile devices, home computers or portable media will be password-protected and encrypted.

4.6 Remote Access

- All remote access requests must be made through the IS Service Desk, will be centrally managed by Waikato DHB's Information Services department and will utilise encryption and strong authentication measures.
- Computer Access Request forms must be approved and signed by the employee's service manager before submission to the IS Service Desk.
- Remote access connections covered by this policy include (but are not limited to) internet dial-up modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, proprietary remote access/control software, wireless, cellular, etc.
- General access to the Internet by remote users through Waikato DHB's network is permitted only for work purposes and in compliance with Waikato DHB's policy on acceptable Internet usage.
- All remote computer equipment and devices used for business interests, whether personal or Waikato DHB-owned, must have installed and up to date antivirus software and will use the client VPN software provided or recommended by the Waikato DHB Information Services Department.
- Employees, contractors, and temporary staff will make no modifications of any kind to the remote access connection without the express approval of the Waikato DHB's Information Services department.
- All remote access connections must include a "time-out" system. In accordance with Waikato DHB's security policies, remote access sessions will time out after 15 minutes of inactivity, and will require the user to reconnect and re-authenticate in order to re-access.
- If equipment, regardless of ownership, used for remote access is damaged, lost, or stolen, the authorised user must notify their manager and Information Services department immediately.
- Remote access users will immediately report to their manager and the Information Services department any incident or suspected incidents of, cyber security attacks, unauthorized access and/or disclosure of sensitive information.

4.7 Wireless

- Waikato DHB devices are to connect to trusted wireless access points only.
- The addition of new wireless access points within Waikato DHB facilities will be managed by the Information Services department.
- All wireless access points within Waikato DHB will be managed by the Information Services department and will utilise encryption and strong authentication.
- Non-sanctioned and/or approved installation of wireless equipment and/or use of unauthorised wireless equipment are forbidden.
- Wireless Internet access for business purposes from a device not managed by the Waikato DHB can be made via the Waikato DHB Guest wireless network only.
- Wireless capable devices managed by the Waikato DHB will automatically connect to corporate wireless networks providing access to Waikato DHB information services.
- All acceptable use requirements which apply to wired LAN access and use of Waikato DHB provided information resources also apply to wirelessly connected devices.
- Information Services will define the traffic types that are acceptable for use over a wireless LAN connection.
- Information Services reserves the right to turn off without notice any access port to the network that puts the Waikato DHB's systems, data, users, and clients at risk.
- Patient wireless Internet access is available using a third party provided public wireless service. (Waikato DHB wireless network service is not to be used for Patient Internet access).

4.8 Third Party Access

- All Third Party access to Waikato DHB information assets and resources shall be subject to a legally binding contractual agreement and must specify inter-alia;
    - The work that is to be accomplished.
    - The hours the work is to be undertaken.
    - The information that the third party will have access to.
    - Required resources.
    - The minimum security requirements and controls that the third party must meet.
    - Confidentiality or non-disclosure agreements required.
    - Agreed methods for the destruction, disposal, or return of Waikato DHB information at the end of the contract.
    - The return of Waikato DHB property such as a laptop, PDA, or cell phone after the completion or termination of the agreement.
    - Process and regulatory compliance.
    - Incident management responsibilities and liability.
- Third party access to systems must be authenticated and password management must comply with the Waikato DHB's Password Policy.

- Any third party owned device connected to the Waikato DHB network must have up-to-date virus protection and patches installed.
- Third-party employees must report all security incidents and events to the Information Services department immediately.
- All third party activity must follow all applicable Change Management procedures and processes.
- All software used by the third party in providing service to Waikato DHB must be inventoried and licensed.
- All third-party maintenance equipment on the Waikato DHB network connecting externally will be firewalled and secured.
- All sensitive information collected must be returned to the Waikato DHB or evidenced as destroyed upon termination of contract.
- All Waikato DHB owned equipment and supplies, access cards and identification badges must be returned upon termination of contract.
- Upon termination of contract the Waikato DHB will;
  - Remove all third party authentication and access to systems.
  - Ensure incoming e-mail is re-routed to an appropriate person.
  - Archive any third-party software configuration, and transfer ownership to designated internal staff.

4.9 Unattended Equipment

- Unattended workstations must be logged off or use a password-protected screen saver to prevent unauthorised access.
- Equipment left unattended for prolonged periods (e.g. overnight or weekends) should be logged off and shut down.
- Mobile equipment should be secured in a locked cabinet or similar.

4.10Clear Desk Policy

- Sensitive information in the form of paper or removable media, when left unattended on desks is exposed to unauthorised viewing, copying, loss, theft or alteration.
- Depending upon the security of the premises and the level of sensitivity, it may be necessary to lock away sensitive information when leaving it unattended even for short periods.
- Documents containing sensitive information must not be left on printers or photocopiers for any longer than necessary.

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.
- Project Assurance Program.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*
- *SANS Top 20*

Waikato District Health Board
Te Hanga Whaioranga Mō Te Iwi – Building Healthy Communities

Document 2

Protocol

Information Security – Anti-Malware

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	Information Security Manager
Document Owner Name	Chief Information Officer (CISO)
Document Owner Title	Geoff King

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version

Information Security – Anti-Malware

Contents

1. Overview

1.1 Purpose

To define the minimum security requirements, standards and processes required to prevent malware or virus infection of Waikato District Health Board's information assets and resources that;

- Ensure that all reasonable steps are taken to maintain the security and reliability of the entire Waikato District Health Board computer network.
- Reduce the risk to the DHB of internal and external threats to the ICT network and the ICT systems and technologies connected to that network

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as "Users" in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

Non digital/computer based initiatives.

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the DHB must comply with the DHB's policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.
- Information Services are responsible for:

  (a) Maintaining and advising the Waikato DHB's Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

(b) Maintaining and updating the Anti-Virus standards and procedures that support this protocol.

(c) Maintaining the currency of operating system security patching on ICT information assets and resources.

(d) Keeping the anti-virus products up-to-date in terms of both virus definitions and software version.

(e) Installing anti-virus software on all ICT information assets and resources including desktop workstations, laptops, tablets and servers.

(f) Establishing and maintaining a virus awareness programme to provide staff with general knowledge about computer viruses and their behaviour.

(g) Providing advice to users on installing anti-virus software according to standards on privately owned computers that will be used for DHB purposes.

(h) Protecting the Waikato DHB's ICT computing environment from external and internal cyber security threats and risks.

(i) Taking appropriate action to contain, remove, and assist in recovery from virus infections on ICT information assets and resources.

- Business Owners and Users are responsible for;

(a) Ensuring compliance with the Information Security Policy, Protocols and supporting processes and procedures and applying the defined standards to information assets and resources maintained within service control.

(b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.

(c) Taking appropriate measures to protect against virus infection. This includes not opening any files or links attached to emails from an unknown, suspicious or untrustworthy source.

(d) Not attempting to either alter or disable anti-virus software installed on any computer attached to the DHB network.

(e) Ensuring that any personally-owned computers that connect to the DHB network have virus protection software installed that is in keeping with the standards set out in this policy.

(f) Advising any Anti-Virus incidents and/or risks to the IS Service Desk.

4. Standards

- Protection against malware will be based on malware detection and repair software, security awareness and appropriate system access and change management controls.

- The use of multiple products and strategies to protect against malware across the information processing environment (defence in depth) will be used to improve the effectiveness of malware protection.

- Care should be taken to protect against the introduction of malware during maintenance and emergency procedures, which may bypass normal malware protection controls.
- The DHB approach should be based on and include;
- PREVENT/DETER = AWARE establishing a formal policy prohibiting the use of unauthorized software.
- PREVENT/AVOID & DETECT = AWARE2 implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting);
- PREVENT/DETER = AWARE establishing a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken.
- PREVENT/AVOID reducing vulnerabilities that could be exploited by malware e.g. through technical vulnerability management.
- DETECT = AWARE2 conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated.
- PREVENT/AVOID & DETECT & RECOVER installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the reviews carried out should include:
  - reviewing any files received over networks or via any form of storage medium, for malware before use;
  - reviewing electronic mail attachments and downloads for malware before use; this review should be carried out at different places, e.g. at electronic mail servers, desk top computers and when entering the network of the organization;
  - reviewing web pages for malware;
- RECOVER defining management procedures and responsibilities to deal with malware protection on systems, training in their use, reporting and recovering from malware attacks;
- PREVENT/AVOID + AWARE/T implementing procedures to regularly collect information, such as subscribing to mailing lists and/or verifying web sites giving information about new malware;
- PREVENT/AVOID + AWARE/T + AWARE implementing procedures to verify information relating to malware, and ensure that warning bulletins are accurate and informative; managers should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malware, are used to differentiate between hoaxes and real malware; all users should be made aware of the problem of hoaxes and what to do on receipt of them;
- PREVENT/AVOID isolate environments where catastrophic impacts may result.
- All 'end points' and network 'entry' points will be protected from, and provide protection to the resources they host, or provide access to, from malware and its effects.

- All ICT information assets and resources, including third party and privately owned devices that connect to the Waikato DHB network must have standard, supported anti-virus software installed and configured and actively running.
- The Waikato DHB authorised, licensed, anti-virus software package must be installed on all computer servers and workstations. Security patches to the operating systems and anti-virus updates must be applied in accordance with manufacturer instructions.
- Any identified or suspected computer virus must be immediately reported to the IS Service Desk, who will organise technical support to remove the virus and prevent any further spread.
- Virus clean-up must be under the supervision of authorised Information Services staff.
- Information Services will conduct periodic reviews of the software and data content of systems supporting critical business processes.
- The presence of any spurious files or unauthorised amendments shall be formally investigated.
- All ICT information assets and resources will be configured so that operating system updates are installed automatically or as managed by the Information Services department.

  (1) Servers running Anti-Virus at least 100% must pass the compliance check by having Anti - Virus signatures within 2 days of the current release.

  (2) Workstations running Anti-Virus at least 98% of the devices that have connected in the last 7 days must pass the compliance check by having; Anti-Virus signatures within 7 days of the current release.
- ICT information assets and resources that cannot have AV software installed are to be configured to operate in a separate 'unprotected' VLAN with appropriate mitigation separating such devices from the rest of the environment.
- System patches must be applied to reduce the likelihood of malicious software attacks.

  (1) Servers: should be no more than 4 months behind available and tested security patches.

  (2) Desktops and Laptops: should be no more than 2 months behind available and tested security patches. This should apply to no less than 90% of systems on or connected to the network.

  (3) Networks: should be no more than 2 month behind available and tested security patches.
- No software programs or executable files are to be downloaded from the Internet and installed on devices without the authority and prior approval of Information Services.
- All email including attachments is to automatically check for viruses before it enters or leaves the email system.
- Approved removable media (e.g., corporate USB stick) must be scanned for viruses before use. Users must contact the IS Service Desk to request transfer of the data required from unapproved removable media (e.g., CD-ROM, DVD, personal USB stick).

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*
- *SANS Top 20*

Document 3

Protocol

Information Security – Communications

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	Information Security Manager
Document Owner Name	Chief Information Officer (CISO)
Document Owner Title	Geoff King

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version
1.1	John Pawlick	22/09/2017	First review (Architects)
2.0	Jeremy Marshall	23/11/2017	Final Version

Information Security – Communications

Contents

Information Security – Communications

1. Overview

1.1 Purpose

To ensure the integrity of information communicated across networks and that any changes are authorised and controlled the Waikato DHB has formally documented:

- The types of systems/devices that may be attached to the network(s) and in what manner this attachment can occur.
- The types of systems/devices that are not permitted on the network.
- The minimum technical standards for packaging and transmission of health information.
- Controls to protect information.

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as “Users” in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

Systems, devices and networks that are not part of the Waikato DHB environment.

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the DHB must comply with the DHB’s policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.
- Information Services are responsible for:

(a) Maintaining and advising the Waikato DHB’s Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

(b) Monitoring and managing the Waikato DHB's network to deliver optimal performance and appropriate security of the environment.

(c) Protecting network integrity and the security of Waikato DHB information assets and resources from risks such as spam, viruses, malware, or denial of service attacks.

(d) Implementing appropriate controls and protections against high risk network protocols, content or traffic.

(e) Ensuring that network traffic types are appropriately differentiated to enable protection of the overall network and ensure quality of service (QoS) prioritisation of traffic types.

(f) Ensuring formal confidentiality or non-disclosure agreements are in place with external parties that receive personally identifiable data.

- Business Owners and Users are responsible for:

(a) Ensuring compliance with the Information Security Policy, Protocols and supporting processes and procedures and applying the defined standards to information assets and resources maintained within service control.

(b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.

(c) Ensuring users are aware of their responsibilities when transmitting information, know the location of and can access the relevant policies, agreements and procedures.

(d) Ensuring information is transferred in accordance with its security classification. (JP Question – Classification – Covered in data and Information Protocol)

4. Standards

- No equipment will be connected to the Waikato DHB computer network without a being subject to a risk assessment and the approval of the Information Services team.

- Information regarding access to or configuration of the Waikato DHB computer and communication systems is considered confidential and must not be made available to the public or third parties without the approval of the Chief Information Officer or authorised delegate.

- Formal confidentiality or non-disclosure agreements will be developed with external parties that receive personally identifiable data. These agreement(s) must cover vendors/contractors dealing with the recipient organisations and include:
  - Definitions of information to be protected.
  - Duration of agreement.
  - Process for notification of leakage.
  - Ownership.
  - The right to audit and monitor activities that involve personal information.

- Appropriate electronic signatures containing legal disclaimers should be used for all electronic messaging.

- HISO interoperability standards should be followed for the exchange of health information within and between organisations.

- Appropriate encryption standards should be used when exchanging health information between external parties.
- The communication of private information such as credentials should not be sent via the same mechanism where more than one part exists.
- Tools to enable the detection and prevention of unauthorised information transfer should be implemented.
- All changes to the DHB's network environment must be authorised and processed through the IS Change Management process.
- All networks will be documented including a record of updates applied via the Change Management process.
- All networking device default accounts will have their passwords changed, and default account names renamed every 90 days.
- All access to network services and equipment will follow the procedures outlined in the Access Control protocol.
- All access to the Waikato DHB Network and information assets and resources will be via a secure login and password and security privileges will be allocated on a needs basis.
- All voice and data network implementations shall be based on standards issued by the Information Services, including but not limited to;
  - Active network equipment including routers and switches
  - Structured network cabling – local and wide area network cabling, cabinets and racks.
- The status of all network devices will be monitored and the management of access control to networking components centralised.
- Appropriate network security zones will be established to allow data flow to follow controlled paths only.
- Only trusted devices and users should be able to gain access to internal networks via wireless access.
- Only trusted devices and users should be able gain access to internal networks.
- Network appliances are configured to support the segregation of networks.
- All wired access points will be disabled when not in use.
- Waikato DHB will use a robust "firewall system" interposed between the DHB's ICT network and external networks. Unless authorised by the Information Services all traffic to or from an external network must pass through the firewall.
- Access from the Internet or other external network to the Waikato DHB public information systems must not make sensitive information or information systems vulnerable to compromise.
- Only network sessions using strong authentication and encryption will be permitted to pass from the Internet to inside through the firewall. Where users are required to access

internal systems and networks from, or across, the Internet, end-to-end encryption and strong authentication controlled by Waikato DHB will be employed.

- The firewall will be configured to deny all services not expressly permitted, and will be monitored to detect intrusions or misuse.
- The firewall will not accept traffic on its external interfaces that appear to be coming from internal network addresses.
- Information Services will review the network security rules and maintenance procedures on a regular basis. Where requirements for network connections and services have changed, the security rules and procedures will be approved then updated.
- The firewall (i.e. system software, configuration data, database files, etc.) must be backed up before each configuration and software change so that in case of system failure, data and configuration files can be recovered.
- Only the firewall administrator(s) will have privileges for updating system executables or other system software. Modification of the firewall component software must be completed by a firewall administrator(s), and requires the formal approval of the Networks Manager.
- Except where authorised by Information Services no access will be granted to third party and/or public to DHB data, systems or servers operating on the Waikato DHB trusted network (Local Area Network).
- Waikato DHB will provide incoming access to selected data and systems from the Internet via use of a DMZ, which will be a part of the firewall architecture.
- All connections from the Waikato DHB network to external networks will be for business or clinical purposes only and must be approved by Information Services.
- Connections will be allowed only with external networks that have acceptable security controls and procedures.
- All connections to approved external networks will pass through Waikato DHB approved firewalls.
- Information Services will validate the need for all such connections on a regular basis. When notified that the need for connection to a particular network is no longer valid, all accounts and parameters related to the connection will be deleted.
- Any connection between firewalls over public networks will use encrypted Virtual Private Networks (VPN) to ensure the privacy and integrity of the data passing over the public network.
- All such VPN connections must be approved by Information Services and must involve appropriate connection agreements which detail the responsibility of the connecting party to maintain their connecting devices appropriately with operating system patching and approved anti-virus solutions.
- All connections between clients to services or applications located behind the firewall within Waikato DHB's trusted network, that are over untrusted public networks will use

encrypted Virtual Private Networks to ensure the privacy and integrity of the data passing over the public network.

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.
- Project Assurance Program.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*
- *SANS Top 20*

Document 4

Information Security – Cryptography Management

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	Information Security Manager
Document Owner Name	Chief Information Officer (CISO)
Document Owner Title	Geoff King

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version

Contents

Information Security – Cryptography Management

1. Overview

1.1 Purpose

To ensure the proper and effective use of cryptography and protect the confidentiality, authenticity, integrity and/or availability of information by using approved cryptographic products, algorithms and protocols and to encrypt sensitive information to secure it from outside and insider threats.

Cryptographic controls and keys must be protected by policies and procedures that ensure they are implemented, continue to be used, and are decommissioned in a manner that reduces the risks of unauthorised access and misuse. Such policies and procedures should exist at different levels across a chain of suppliers, vendors, suppliers, software developers and organisations using cryptographic products.

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as “Users” in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

Initiatives that do not have an ICT or information Security reliance or implication.

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the DHB must comply with the DHB’s policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.
- Information Services are responsible for:

  (a) Maintaining and advising the organisations Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

(b) Provide assurance that cryptographic systems continue to function as intended and that risks continue to be managed and minimised.

(c) Include risk assessments and planning security services for IT systems using cryptography.

- Business Owners and Users are responsible for;

(a) Ensuring compliance with the Information Security Policy and Protocols.

(b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.

(c) Ensure familiarity with the organisation's policy on the usage of cryptography controls and seeking advice from IT support when procuring new technology.

(d) Not sharing passwords and/or access relating to cryptographic keys with unauthorised persons.

(e) Reporting lost and stolen equipment to IT support for appropriate actions to be taken including remotely wiping or disabling the device.

(f) Complying with any notification requirements from IT support.

4. Standards

- All information needing to be protected will be categorised and assigned the relevant encryption standards.
- Systems used for generating and storing cryptographic keys will be treated according to the principles of a higher security classification, as those systems represent potential access to aggregated information and if compromised could undermine the separation of duties.
- All equipment used to generate, store and archive keys will be physically protected
- All passwords and/or access relating to cryptographic keys will be secured.
- Encryption of stored and transmitted information should be facilitated by the use of cryptographic controls in a manner that represents a separation of duty and minimises any single point of failure or single point of compromise.
- New cryptographic products and services should be evaluated during procurement to ensure their cryptographic protocols, algorithms and key strengths are upgradable over the expected lifetime of the system(s) proposed.
- Non-upgradable cryptographic solutions should be avoided, except for short-lifetime disposable technologies (devices) that can be quickly decommissioned and replaced in response to an event or incident.
- Recognise that transition periods where legacy cryptography and replacement solutions running side-by-side represent potentially a higher risk than running either solution alone and residual information security risks are taken into account when accrediting these systems.

- Compromised cryptographic controls (protocols, algorithms and keys) will be revoked and replaced in a timely manner when responding to a security event or incident.
- Cryptographic key lifetime (e.g., validity start date, validity end date, and validity period) should be appropriate and key materials are fit for the renewal cycle. (Keys should not normally have a validity period of more than two to three years).
- Weak cryptographic capabilities when tolerated in legacy systems (supported by time-bound written exemptions and risk assessment), should be improved at the next upgrade.
- Development, test and production environments should have separate chains of trust to support a separation and/or segregation of duties.
- All new purchases (software, hardware, cloud services etc) will require vendors and suppliers to confirm their cryptographic products are secure, in that they:
  - Treat equipment to be returned to the supplier for repair or upgrade in a manner that protects any sensitive information that may still be on it.
  - Provide an alert at least 30 days before the expiry of cryptographic keys, to allow adequate time for arrangements to be put in place for their renewal.
- All systems will be patched and kept up to date with priority given to critical notifications.
- The distribution and revocation of end-user and system certificates will be managed with a minimum of delay.
- A minimum notification period of 30 days will be set for the renewal of any external certificate(s).
- Encryption will be enabled on all equipment that is dependent on its own controls to protect itself, such as mobile devices, backups, and offsite storage.
- Where tick box options are available, configure equipment to enable Federal Information Processing Standards (FIPS) compliance, sometimes referred to as 'FIPS mode' unless backwards compatibility to non-FIPS compliant systems is required (NZISM V2.3 May 2015 section 17.2.11).
- Approval from the Information Security Manager is required for disabling encryption when required for investigative purposes, and reinstate encryption when that work is completed.
- To reduce susceptibility to downgrade attacks weak security solutions should be removed from selection and clear text should only be able to be selected for diagnostic purposes and not operational periods where live data requires protection. Systems will be returned to a secure state after running diagnostics.
- Security expectations for cryptography and key management will be communicated for both new projects and ongoing service delivery.
- Responsibilities should be clear and unambiguous for cryptographic systems and key management including responsibility for planning security services that provide oversight for cryptographic systems.
- All key management related activities will be logged and audited.

- All lost and stolen equipment must be reported to the IS Service Desk for appropriate actions to be taken.
- User passwords must be changed when equipment has been returned after repair.
- Lost and then found equipment, where it has been outside of a user's or an organisation's possession will be treated with suspicion. Such devices will be reloaded with fresh keys and passwords and the old keys revoked.
- Carryover of keys to new equipment is discouraged between legacy to replacement systems, and old hosting providers to new, to reduce the transfer of old risks into new systems.
- Options for the recovery of encrypted information should be considered in contracts, particularly if the data is stored only in one place such as a hosting provider that could suddenly go out of business, or an end user device that could be lost or compromised.

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.
- Project Assurance Program.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*
- *SANS Top 20*

Information Security – Information and Data Management

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	Information Security Manager
Document Owner Name	Chief Information Officer (CISO)
Document Owner Title	Geoff King

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version

Contents

Information Security – Information and Data Management

1. Overview

1.1 Purpose

Information and data quality is vital to the planning and provision of high quality services and the efficient operation of the Waikato DHB and the wider health and disability sector and the DHB must ensure there are reasonable safeguards in place to prevent loss, misuse or disclosure of health information and ensure all information and data is protected and appropriately managed to ensure confidentiality, Integrity and availability;

Agencies must appropriately safeguard all official information to ensure its:

- Confidentiality (that is, information must not be made available or disclosed to unauthorised individuals, entities or processes).
- Integrity (that is, data must not be altered or destroyed in an unauthorised manner and accuracy and consistency must be preserved regardless of changes).
- Availability (that is, information must be accessible and useable on demand by authorised entities).

Agencies must apply safeguards so that:

- Only authorised people, using approved processes, access information.
- Information is only used for its official purpose, retains its content integrity, and is available to satisfy operational requirements.
- Information is protectively marked and labelled as required.
- Information and data needs within the DHB are appropriately identified and prioritised, with plans developed to meet current and future requirements.
- Information and data is available and enable's staff to undertake their roles effectively, support evidence based decision-making and professional learning.
- Information and data is secured and protected and processes exist to ensure the continuity of critical DHB functions.
- The confidentiality, integrity and availability of information and data is maximised and maintained.
- Information is neither accessed, nor used inappropriately, and is maintained in a secure environment to protect against accidental loss, theft, vandalism and/or misuse.
- Information and Data (patient and employee) is protected against identity theft.
- Standards for cataloguing information elements exist to enhance the access to, and retrieval and sharing of, information.
- Secure communication protocols and appropriate connectivity between information systems enables efficient data collection, storage, and communication.

The protocol will apply to hard copy and electronic information, including, but not limited to printed documents, written documents, forms, emails, native electronic documents, scanned documents.

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as "Users" in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the DHB must comply with the DHB's policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.
- Information Services are responsible for:

(a) Maintaining and advising the organisations Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

(b) Ensuring appropriate controls and operating procedures are created, implemented and maintained to protect documents, removable storage media, printed information and system documentation from unauthorised disclosure, modification, removal and destruction.

(c) Ensuring secure communication protocols and processes exist to support the communication of patient, client or staff information within Waikato DHB and between the DHB and external parties in accordance with information security and privacy requirements.

(d) Developing and maintaining procedures for back-up, off-site storage and restore of critical data, systems and applications.

(e) Raising people's awareness and providing advice about how to reduce the chance of identity theft occurring.

(f) Training staff in the processes for data transfers between systems and the authorisations required before transfers can take place.

- Business Owners and Users are responsible for:

  (a) Ensuring compliance with the Information Security Policy, Protocols and supporting processes and procedures and applying the defined standards to information assets and resources maintained within service control.

  (b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.

  (c) Ensuring adequate controls and processes are in place to protect patient, client, and staff information and data from inappropriate access, misuse, unintended destruction and/or malicious damage.

  (d) Ensuring the security of information and data which they access as part of their role and that sensitive information is not disclosed to any unauthorised third party.

  (e) Ensuring the accuracy and completeness of information and data recording.

  (f) Ensuring that any patient, staff or other information they handle and record is as accurate and up to date.

4. Standards

- All information assets and resources must be assessed, classified, protected and appropriately managed for Information Security risk that results from threats to the Confidentiality, Integrity and Availability (CIA) Waikato DHB Information and Data.
- All Waikato DHB information assets and resources remain the property of the DHB.
- All access to and/or use of information and data must be within approved applications, storage devices and locations and for the sole purpose of its creation and in relation to a user's job responsibilities.
- Personal devices may only access the Waikato DHB networks and data through approved technology gateways or as part of an authorised BYOD (Bring your own device plan).
- Users must not store data or information on personal devices or personal removable media.
- Access to information and data by external/third parties shall be governed by individual contractual agreement or memoranda of understanding. Such contractual agreements shall be subject to a risk assessment and where required be approved by the CIO, Information Security Manager, Privacy Officer and Legal Counsel.
- All information and data creation, storage and use must comply with Waikato DHB Information Security Policies, Waikato DHB Corporate (0905) and Clinical Records Management Policy (0182) be managed in accordance with the Corporate Records Management Policy and the Public Records Act 2005.
- Waikato DHB may be required to disclose information and data contained in file systems (including, but not limited to files, folders, drives, group shared areas, logs and backups)

to law enforcement and regulatory agencies in compliance with legal and regulatory requirements.

- Electronic communication or transfer sensitive data should only occur as part of the normal execution of responsibilities and in a manner that is consistent with the Waikato DHB's policies, protocols and standards.
- The use of external file transfer systems to enable the communication of information and data is only permitted only as authorised by Waikato DHB's Information Services department and when approved file transfer systems are used.
- Use of "cloud storage" mechanisms to transfer or store Waikato DHB information and data is not permitted except where approved cloud storage mechanisms are used and where DHB and Ministry risk assessments have been completed and approved.
- Systems and processes that involve identity data should be developed to protect against identity theft in accordance with the Evidence of Identity Standard for government agencies.
- All data and information must be classified in accordance with the HISO framework.
- Consideration must be given to information and data protection when:
    - Developing a new computer system for processing sensitive information and data.
    - Using an existing computer system to process sensitive information and data for a new purpose.
    - Transferring sensitive information and data outside of the Waikato DHB boundaries.
    - Sharing sensitive information and data with third parties.
- All information and data must be managed and retained in accordance with its classification, criticality to the Waikato DHB and the requirements of the Public Records Act 2005.
- All information and data backup and recovery activities will be in accordance with the Information Security Operations Security protocol and supporting standards.
- Disaster Recovery programmes will be established and maintained to minimize the risks associated with temporary or permanent loss of data, information and records.
- Waikato DHB responsibilities for maintaining the confidentiality of data extend to data communicated to external parties and all communication or transfer of Waikato DHB information and data must be in accordance with Waikato DHB policy, protocol and standards.
- When transferring sensitive information and data users must ensure that the means used are appropriate for the security classification and confidentiality of the data be limited to the minimum information necessary for the permitted purpose.
- The sender of sensitive data has an obligation to ensure they have verified the accuracy of the recipient address.
- Procedures to interpret classification labels from other organisations where information is shared will be established.

- The use of media containing classified information within a system that has a security classification lower than that of the media is prohibited.
- Standards and processes must be implemented to ensure:
  - Information and records are appropriately disposed of when no longer required for contractual, legal or operational purposes.
  - Services responsible for the destruction of data, information and records they hold adopt processes appropriate for the information data and media utilised.
- Information that has reached end of life must be subject to controlled archive and where applicable destruction, to ensure the Waikato DHB meets its Privacy obligations and commitments under the Public Records Act 2005.
- All equipment containing storage media must be checked to ensure that any sensitive information and data is removed or overwritten prior to disposal.
- All information and data must be backed up and removed before equipment is sent to vendors for repair or maintenance, and restored on return, if required.
- Media containing sensitive information and data must be sanitised prior to disposal or re-use in accordance with asset disposal standards.
- Vendors providing destruction services must comply with expected standards of destruction and contract requirements.

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.
- Project Assurance Program.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Identity Standards v 2.0*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*

- *SANS Top 20*

Document 6

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	IS Security Manager
Document Owner Name	Director Information Services
Document Owner Title	Geoff King

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version
2.0	Jeremy Marshall	23/11/2017	Final Version

Contents

1. Overview

1.1 Purpose

To ensure the appropriate tools, processes and procedures are in place to detect report and manage information security incidents.

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as "Users" in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

Non-ICT incidents and ICT incidents that are not security related or have no potential security implications or impacts.

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the DHB must comply with the DHB's policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.
- Information Services are responsible for;

  (a) Maintaining and advising the Waikato DHB's Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

  (b) Establishing management responsibilities to ensure procedures for Information Security Incident management are developed and communicated within the organisation/applicable external parties.

  (c) Ensuring all employees and contractors are aware of their responsibilities to report information security incidents.

(d) Ensuring all security incidents are logged in the Information Services Service Desk and call management system, managed through to resolution and lessons learned/recommendations developed and implemented.

(e) Identifying and assessing threats to ICT assets and resources and categorise and prioritise incidents in accordance with the organisations established standards for risk and impact.

(f) Recording and managing security risks resulting from incidents.

(g) Communicating with system users as required to effectively manage and control responses to security incidents.

(h) Responding to security incidents and facilitating protection and collection of evidence related to them.

(i) Liaising with the Privacy Officer to effectively manage the interaction between security incidents and privacy risks.

- Business Owners and Users are responsible for:

(a) Ensuring compliance with the Information Security Policy, Protocols and supporting processes and procedures and applying the defined standards to information assets and resources maintained within service control.

(b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.

(c) Reporting any suspected security weakness in, or threats to, systems or services to the IS Service Desk immediately.

(d) Following instructions and guidelines issued by Information Services in response to security incidents.

- Privacy Officer is responsible for:

(a) Maintaining and advising the organisations Information Privacy Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

(b) Providing guidance and direction in relation to Privacy Risks associate with or resulting from security incidents.

- HR is Responsible for;

(a) Facilitating reviews related to security incidents involving staff and/or that result in disciplinary procedures.

4. Standards

- All information security incidents must be reported to Information Services through the IS Service Desk.
- All procedures for handling suspected information security incidents should be followed including:
  - Recording of symptoms and any messages appearing on the screen.
  - Immediately stop using the computer.

- Informing the IS Service Desk immediately.
- Removable media should not be transferred to other computers.
- Any recovery must be carried out by authorised Information Services staff only and under no circumstances should users attempt to resolve an incident themselves.

- All high severity incidents, including those involving breaches of sensitive and/or personally identifiable information, must be escalated to the Information Security Manager.
- Vendor advisories must be reviewed, logged and actioned to resolve information security risks and any residual risk recorded and managed.
- System logs will be monitored and reviewed to identify information security breaches and weaknesses.
- Information security risk assessments will be performed to determine where weaknesses may exist and improvements can be made.
- All reported and identified information security incidents must be recorded in the Information Services call management system and categorised including but not limited to;
  - Confidential personal identity data exposure
  - Password violation
  - Account sharing
  - Loss or theft of equipment
  - Identity Theft
  - Inappropriate Internet access
  - Denial of Service
  - Malicious code activity
  - Policy violation
  - Spam
  - Phishing
  - Unauthorized access
  - Un-patched vulnerability
- All information security incidents must be prioritised in accordance with risk and impact.
  - High – P1
  - Medium – P2
  - Low – P3
- All information security incidents will be responded to based on priority and in accordance with the IS Departments Incident Management process and SLA's.
- Any changes required to address information security incident impacts will be made in accordance with the IS departments Change and Release Management process.
- As far as practical all parties affected or impacted by an information security incident will be notified and advised of possible consequences.
- Significant information security incidents will be reported to the National Cyber Security Centre.

- The protection and collection of evidence related to an information security incident will be assured in particular those involving staff disciplinary or legal action.
- All information security incidents will be reviewed and recommendations made for avoiding a similar incident in the future.
- Lessons learnt will be logged and used to drive ongoing improvements in process, tools or policies to reduce the likelihood of incident recurrence.
- Any resulting Privacy issues will be managed in accordance with the DHB's Privacy Policy and under the conveyance of the organisations Privacy Officer.
- Information Services will audit, monitor and report usage and initiate appropriate remediation and HR action in response to information security incidents and/or breaches of policy.

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.
- Project Assurance Program.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*
- *SANS Top 20*

Document 7

Protocol

Information Security – Information Security Management

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	Information Security Manager
Document Owner Name	Chief Information Officer (CISO)
Document Owner Title	Geoff King

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version
1.1	John Pawlick	22/09/2017	First review (Architects)
2.0	Jeremy Marshall	23/11/2017	Final Version

Information Security – Information Security Management

Contents

Information Security – Information Security Management

1. Overview

1.1 Purpose

Based on the Health Information Security framework (HISF 10029) the appropriate application of protective security measures by the Waikato DHB will ensure the operational environment necessary for the confident and secure conduct of government business.

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as "Users" in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

The following areas within information security are not covered in this document, as there are separate policies that address them:

Acceptable Use: A separate policy 'Information Systems Acceptable Use Policy' covers the use of Waikato DHB's technology equipment, systems, resources and data.

Mobile Communications Devices: The 'Mobile Communications Devices Policy' covers the use of Waikato DHB's mobile technology equipment including 'BYOD' devices.

Social Media and the Internet/Intranet: Use of Social Media and the Internet/Intranet is covered by the 'Media and Communications Policy'.

Intellectual Property: The 'Intellectual Property Policy' covers the ownership of intellectual property created by an employee in the course of their employment.

Patient Data Privacy and Confidentiality: Matters relating to patient data privacy and confidentiality are managed under the conveyance of the DHB's Privacy Office in accordance with the 'Information Privacy Policy'.

Physical Security: Matters relating to physical security are additionally managed by the Property and Infrastructure team in accordance with the Property and Infrastructure 'Security Policy'.

Clinical Records: Clinical Records Management is subject to the 'Clinical Records management Policy'.

Corporate Records: Corporate Records Management is subject to the 'Corporate Records management Policy'.

Human Resources (HR): Matters relating to HR and/or disciplinary issues must be managed by the relevant Service manager, HR department and in accordance with relevant DHB policies and procedures.

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the DHB must comply with the DHB's policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.
- Information Services are responsible for:

  (a) Maintaining and advising the Waikato DHB's Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

  (b) Developing the framework, process and procedures to enable the effective identification and management of information security risk.

  (c) Ensuring that all employees, vendors, consultants and contracted personnel are aware of the Information Security Policy and are kept informed of any changes and updates.

  (d) Developing appropriate security management strategies and approaches and advising the Board, Executive and Security Governance Group of the security controls and risk position.

  (e) Developing a *System Security Plan* describing the implementation and operation of controls within the system derived from NZISM, HISF, SANS 20 and the *Security Risk Management Plan*.

  (f) Developing security assurance program and working with Internal Audit and key stakeholders to ensure the development and implementation of external assurance to measure and report effectiveness of security framework, approaches and control/risk position.

  (g) Provide training, awareness and guidance as required to support informed security decision making.

- Business Owners and Users are responsible for:

  (a) Ensuring compliance with the Information Security Policy and Security Policy Protocol.

  (b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.

(c) Establishing information security risk appetite and making decisions in accordance with the risk appetite and security baseline standards.

(d) Identifying and advising Information Services of any information security risks and weaknesses they become aware of.

(e) Reporting security events to the IS Service Desk as quickly as possible.

4. Standards

- The Security Policy and protocols will establish the overarching security principles and control objectives for the Information Security Management System (ISMS) based on the HISF 10029.2015 Framework, NZISM and SANS 20.
- An Information Security Management Systems (ISMS) will be established to provide a systematic and structured approach to managing information security and will define roles and responsibilities to direct, monitor and control the implementation, operation and management of information security within Waikato DHB.
- Information security management will be carried out in accordance with all relevant Waikato DHB policies and legal, regulatory and contractual requirements allowing information to be processed, managed and shared with the confidence that its security is assured and that information security risks have been identified, understood and treated appropriately.
- The Information Security Policy and supporting documents will be approved by management and published, reviewed and communicated to all employees and relevant external parties.
- Security policies and protocols will be reviewed and updated annually or more frequently, if required.
- All employees, board members, vendors, consultants and contracted personnel should be made aware of the Information Security policy and supporting protocols.
- All employees, vendors, consultants and contracted personnel should read, review and follow obligations under the information security policy and supporting protocols.
- Information Security will be embedded into everyday practice by defining roles and responsibilities and clarifying the actions required of all staff to protect the Waikato DHB's information assets and information and communications technology (ICT) assets.
- Any exceptions to the security policy and supporting protocols must be authorised and based on informed understanding and acceptance of risk.
- All security exceptions and breaches are to be registered and recorded in the Information Services call management application with associated attachments.
- All ICT information assets and resources will be covered by an information security risk management plan to identify and reduce potential information security risks.
- An agreed system security plan will describe the implementation and operation of controls within the system derived from the NZISM and the information security risk management plan.

- Standard operating procedures and processes will be developed for systems to provide step-by-step guides to undertaking information security related tasks and activities.
- Information Services will audit, monitor and report usage and initiate appropriate action in response to security incidents and/or breaches of policy in accordance with Waikato DHB policy.
- Information Services will leverage the Protective Security Requirements (PSR) and Operational Assurance (OA) framework to assure security approaches and will additionally work with the internal audit function and develop and implement an audit programme to measure and report the effectiveness of security controls and approaches.
- Monitoring and/or usage activity requests by service managers must be made through an HR Consultant set out in detail the reasons for the monitoring, including grounds for suspecting unacceptable use or inappropriate behaviour and steps that have been taken to address the manager's concerns.
- The Human Resource Consultant will consult with the Privacy Officer (if advice on privacy or legal issues is required) and Information Security Manager (if advice on information security is required).

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.
- Project Assurance Program.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*
- *SANS Top 20*

8. Appendix A

The Protective Security Requirements (PSR) outlines the Government's expectations for managing personnel, physical and information security. It includes mandatory requirements that all government agencies must implement to ensure a consistent and controlled security environment throughout the public sector.

These requirements will form the basis for operational and audit assurance measurement and reporting over the ISMS and information security approaches.

INFOSEC1 - Agencies must address information security requirements through the development and implementation of an information security policy as part of the agency security plan.

The policy and plan should:

- Detail the objectives, scope and approach to the management of information security risks and issues within the agency.
- Be endorsed by the agency head.
- Identify information security roles and responsibilities.
- detail the types of information an employee:
  - can lawfully disclose in the performance of his or her duties
  - needs to obtain authority to disclose
- Be reviewed and evaluated in line with changes to agency business and information security risks.
- Be consistent with the requirements of the agency's wider protective security plan and information security risk assessment findings.
- Address the issue of data aggregation.
- Include details of the agency's declassification programme.
- Explain the consequences of breaching the policy or circumventing any associated protective security measure.
- Be communicated on an ongoing basis, be accessible to all employees and, where practical, be publicly available.

INFOSEC2 - Agencies must establish a framework to provide direction and coordinated management of information security. Frameworks must be appropriate to the level of security risk in the agency's information environment and consistent with business needs and legal obligations.

Agencies should:

- Document requirements for information security when entering into outsourcing contracts and arrangements with contractors and consultants.
- Enter into Memoranda of Understanding (MOU) with other agencies when regularly sharing information and, where reasonable and practical, make these MOUs publicly available.
- Ensure that prior to providing third parties with access to government information and ICT systems, security measures that match the protective marking of the information or ICT systems are in place and clearly defined in relevant agreements or contracts.
- Ensure appropriate permissions are received before providing third parties with access to information not originating within the agency.

INFOSEC3 - Agencies must implement policies and protocols for the protective marking and handling of information assets in accordance with the Protective Security Requirements New Zealand Government Security Classification System and the New Zealand Information Security Manual.

When addressing policies and procedures for protective marking and control, agencies should:

- Identify, document and assign owners for the maintenance of security measures for all major information assets, including hardware, software and services used in agency operations (including ICT assets used to process, store or transmit information).
- Require all agency information be classified and protectively marked in accordance with the New Zealand Government Security Classification System.
- Implement controls for all security classified and protectively marked information (including for handling, storage, transmission, transportation and disposal) in accordance with the Handling Requirements for Protectively Marked Information and Equipment.
- Develop and maintain a protective marking guide specific to the agency which is accessible to all employees.

Additionally, agencies should ensure:

- The agency's protective marking guide does not limit the provisions of relevant legislative requirements or other obligations (including international) under which the agency operates.
- Disposal of public records is in accordance with legislative and regulatory requirements.

INFOSEC4 - Agencies must document and implement operational procedures and measures to ensure information, systems development and systems operations are designed and managed in accordance with security, privacy, legal and regulatory obligations under which the agency operates.

Operational procedures and responsibilities

Agencies must document and implement operational procedures and measures to ensure information, ICT systems and network tasks are managed securely and consistently in accordance with required levels of security and privacy protection.

Agencies should:

- Have in place incident management procedures and mechanisms to review violations and to ensure appropriate responses to security incidents, breaches and failures.
- Have in place adequate controls to prevent, detect, remove and report attacks and malicious code on ICT systems and networks.
- Operate comprehensive systems maintenance processes and procedures, including operator, audit and fault logs, and backup procedures.
- Implement operational change control procedures to ensure appropriate management and approval of all changes to information processing facilities or ICT systems.
- Comply with legal obligations when exchanging information in any form with other agencies or third parties.
- Apply the protective marking standards and controls specified in the Information Security Management Protocol and the New Zealand Information Security Manual.

Information access controls

Agencies must have in place measures for controlling access to all information, ICT systems, networks (including remote access), infrastructures and applications. Access control rules must be consistent with the agency's risk assessment, business requirements, security classifications and legal obligations.

Agencies should:

- Assess access requirements against the New Zealand Information Security Manual.
- Require specific authorisation to access agency ICT systems.
- Assign each user a unique personal identification code and secure means of authentication.
- Define, document and implement policies and procedures to manage operating systems security, including user registration, authentication management, and access rights and privileges to ICT systems and application utilities.
- Display restricted access and authorised use only (or equivalent) warnings upon access to all agency ICT systems.
- Where wireless communications are used, appropriately configure security features to at least the equivalent level of security of wired communications.
- Implement control measures to detect and regularly log, monitor and review ICT systems and network access and use, including all significant security-relevant events.
- Conduct risk assessments and define policies and processes for mobile technologies and teleworking facilities.
- Prior to connection, assess security risks and implement appropriate controls associated with the use of ICT facilities and devices not owned by government such as mobile telephones, personal storage devices, Internet and email.

Information systems development and maintenance

Agencies must have in place security measures during all stages of ICT system development and implementation. These measures must match the assessed security risk of the information holdings contained within the systems.

When implementing new ICT systems, or changing existing systems, agencies must:

- Address security from the early phases of the system development lifecycle, including concept development, planning, requirements analysis and design.
- Consult internal and/or external audit functions when implementing new or significant changes to financial and critical business systems.
- Incorporate processes in applications, including data validity checks, audit trails and activity logging, to ensure the integrity and accuracy of data captured or held by systems.
- Apply authentication policies and techniques set out in the New Zealand Information Security Manual.
- Identify and implement access controls.
- Control access to ICT system files to ensure the integrity of business systems, applications and data.
- Carry out appropriate change control, system and acceptance testing and migration control measures when installing or upgrading software.
- Conduct certification and accreditation of all new systems to confirm they meet security standards.

Compliance

In order to ensure legal, regulatory, privacy and contractual obligations relevant to information security are managed appropriately, agencies must:

- Take all reasonable steps to monitor, review and audit agency information security effectiveness, including assigning appropriate security roles and engaging internal auditors, external auditors and specialist organisations when required.
- Regularly review all agency information security policies, processes and requirements, including contracts with third parties, and report their compliance to agency management.

INFOSEC5 - Agencies must ensure there is a formal process to approve ICT systems to operate. This process, known as 'certification and accreditation', is an essential component of the governance and assurance of ICT systems and supports risk management. The process is described in the New Zealand Information Security Manual.

GOV1 - Agencies must establish a governance structure within their agency that ensures the successful management of protective security risk.

Agencies should:

- Develop a governance structure to enable the effective identification and management of security risks.
- Gain endorsement from the agency head for security risk management structures, assurance mechanisms and resource allocation.

GOV2 - Agencies must appoint a member of senior management as the Chief Security Officer (CSO), responsible for the agency protective security policy and oversight of protective security practices.

Agencies should:

- Identify and establish protective security roles, with defined responsibilities.
- Assign the role of CSO and any other security lead roles as appropriate.
- Be aware of the functions of the CSO as described in Security Structure and Agency Responsibilities.

GOV3 - Agencies must adopt a risk management approach to cover all areas of protective security activity across their organisation, in accordance with the New Zealand standard AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines.

Agencies should develop a security risk management process to:

- Identify risks specific to their people, information and assets.
- Specify the agency's level of risk tolerance.
- Determine appropriate protections to reduce or eliminate risks.
- Identify and accept responsibility for residual risks.

What is appropriate will vary from agency to agency, but the process should be transparent and justifiable. Risk avoidance is not risk management. Agencies should consider the impact on their business when determining the consequences of the compromise or loss of agency information or assets, or of harm to people.

In addition to agency's individual functions and security concerns, common messages for managing security risks are:

- Security risk management is the responsibility of every staff member, including contractors.
- Risk management, including security risk management, is part of day-to-day business.
- The process for managing security risk is logical, systematic and should be a part of the agency's standard management processes.
- Changes in the threat environment should be continuously monitored, and necessary adjustments made, in order to maintain an acceptable level of risk and a good balance between operational needs and security.

Agencies should also:

- Establish the scope of any security risk assessment and identify the people, information and assets to be safeguarded.
- Determine threats to people, information and assets, in New Zealand and abroad, and assess the likelihood and impact of a risk occurring.
- Assess risks against vulnerabilities and the adequacy of existing safeguards.
- Implement supplementary protective security measures to reduce risks to acceptable levels.

GOV4 - Agencies must develop their own set of protective security policies, plans and protocols to meet their specific business needs. Policies and plans must be reviewed every two years or sooner if changes in risks or the agency's operating environment dictate

Policies and protocols should:

- Detail the objectives, scope and approach to the management of the protective security issues and risks the agency faces.
- Be endorsed by the agency head.
- Identify protective security roles and responsibilities.
- Be reviewed in the context of changes to agency business and security risks.
- Be consistent with the agency's security risk assessment findings.
- Explain the consequences for breaching the policy or circumventing any associated protective security measure.
- Be communicated on an ongoing basis, be accessible to all agency employees and, where reasonable and practical, be publicly available.

GOV5 - Agencies must have an assurance system to conduct an annual security assessment against the mandatory requirements detailed within the Protective Security Requirements. Agencies must be prepared to report this assessment information upon request from lead security agencies.

The assurance, review and reporting process aims to help agencies assess how well they are ensuring the safety of people and the confidentiality, integrity and availability of essential resources.

The process comprises internal self-assessment and reporting, and in some cases external reporting to lead security agencies.

GOV6 - Agencies must provide all staff, including contractors, with sufficient information and security awareness training to meet the obligations of the Protective Security Requirements.

Agencies should:

- Ensure individuals who have specific security duties receive appropriate and up-to-date training.
- Communicate and make available to all staff, including contractors, agency protective security policies.
- Have an ongoing security awareness programme to inform and regularly remind people of security responsibilities, issues and concerns.
- Brief national security clearance holders on the access privileges and prohibitions attached to their clearance level when they gain or renew a clearance and when otherwise required in the clearance renewal cycle.

Agencies should also provide all staff, including contractors, with guidance on relevant sections of legislation covering the unauthorised disclosure of official information, including the:

- Official Information Act 1982 (sections 6, 9, 27 and 31)
- Privacy Act 1993 – Information Privacy Principles (section 6)
- Crimes Act 1961 (sections 78, 78A, 78B, 78C and 79)
- Summary Offences Act 1981 (section 20A).

The combined effect of the *Crimes Act 1961* and the *Summary Offences Act 1981* is that the unauthorised disclosure of information held by the New Zealand government is subject to the sanction of criminal law. All personnel need to be aware of whether and how such legislation applies to their role.

GOV7 - Agencies must have established procedures for reporting and investigating security incidents, and for taking corrective action.

Security investigations are intended to establish the cause and extent of incidents that have, or could have, compromised the New Zealand government.

Through effective reporting and investigation of security incidents, agencies should determine vulnerabilities and reduce the risk of future occurrences.

A security investigation should protect both the interests of the New Zealand government and the rights of affected individuals.

Agencies must apply the principles of natural justice and procedural fairness to all security investigations.

Procedures should give due regard to ensuring the integrity of any other current or future investigation by the agency or that of another.

If an incident is potentially serious then agencies must consult with the New Zealand Police, the New Zealand Security Intelligence Service (NZSIS), the Government Communications Security Bureau (GCSB) and/or the Government Chief Information Officer (GCIO).

Agencies must also report:

- Incidents suspected of constituting criminal offences to the appropriate law enforcement authorities.
- Incidents suspected of involving the compromise of information or assets protectively marked at or above CONFIDENTIAL to the NZSIS.
- Major ICT incidents to the GCSB and/or the GCIO.

GOV8 - Agencies must ensure contracted providers comply with the Protective Security Requirements and agency-specific protective security protocols.

Agencies should:

- Apply necessary personnel security procedures to private sector organisations and individuals who have access to New Zealand government assets.
- Ensure government assets, including ICT systems, are safeguarded through;
  - specifying necessary protective security requirements in the terms and conditions of any contract documentation
  - undertaking assessment visits to verify the contracted service provider complies with the terms and conditions of any contract

GOV9 - Agencies must adhere to any provisions concerning the security of people, information and assets contained in multilateral or bilateral agreements and arrangements to which New Zealand or the agency is a party.

Agencies involved in sensitive work with international organisations, or those that handle another jurisdiction's protectively marked information on their behalf, should ensure their internal procedures comply with relevant obligations.

GOV10 - Agencies must establish a business continuity management (BCM) programme to provide for the continued availability of critical services and assets, and of other services and assets when warranted by a security threat or risk assessment.

Agencies should:

- Ensure governance arrangements establish authorities and responsibilities for a BCM programme and for the development and approval of business continuity plans.
- Within the context of asset identification, undertake impact analyses to identify and prioritise the agency's critical services and assets, including identifying and prioritising information exchanges provided by or to other agencies and external parties.
- Develop plans, measures and arrangements to ensure the continued availability of critical services and assets, and of any other service or asset when warranted by a threat or risk assessment.
- Undertake activities to monitor the agency's level of overall preparedness.
- Make provisions for the continuous review, testing and audit of business continuity plans.

For more information refer to:

- ISO 22301:2012 Societal Security – Business Continuity Management Systems – Requirements
  Business Continuity Institute – Good Practice Guidelines 2013: A Guide to Global Good Practice in Business Continuity.

PHYSEC1 - Agencies must provide clear direction on physical security through the development and implementation of an agency physical security policy, and address agency physical security requirements as part of the overall agency security plan.

The policy and plan should:

- Detail the objectives, scope and approach for the management of physical security issues and risks within the agency.
- Be endorsed by the agency head.
- Identify physical security roles and responsibilities.
- Continuously review physical security measures to reflect changes in the threat environment and take advantage of new and cost-effective technologies.
- Be consistent with the requirements of the agency's protective security plan and physical security risk assessment findings.
- Explain the consequences of breaching the policy or circumventing any associated protective security measure.
- Be communicated on an ongoing basis and be accessible to all agency employees.

PHYSEC2 - Agencies must have in place policies and protocols to:

- Identify, protect and support employees under threat of violence, based on a threat and risk assessment of specific situations. In certain cases agencies may have to extend protection and support, for example to family members
- report incidents to management, human resources, security and law enforcement authorities, and/or Worksafe NZ as appropriate
- provide information, training and counselling to employees
- Maintain thorough records and statements on reported incidents.

PHYSEC3 - Agencies must ensure they fully integrate physical security early in the process of planning, selecting, designing and modifying their facilities.

Physical security includes the proper layout and design of facilities, and the use of measures to prevent or delay unauthorised access to government assets.

It includes measures to detect attempted or actual unauthorised access, and to activate appropriate responses.

Physical security also provides measures to safeguard employees from violence.

Agencies should:

- Select, design and modify their facilities to facilitate the control of access.
- Determine restricted access areas and have the necessary entry barriers, security systems and equipment based on threat and risk assessments.
- Include security specifications in planning, requests for proposals and tender documentation.
- Incorporate related costs in funding requirements.

PHYSEC4 - Agencies must ensure any proposed physical security measure or activity is consistent with relevant health and safety obligations.

Agencies should conduct a risk assessment, taking into account the likelihood and consequence of an accident or injury arising as a result of a physical security measure or activity, and put in place appropriate control measures

PHYSEC5 - Agencies must show a duty of care for the physical safety of members of the public interacting directly with the New Zealand government. Where an agency's function involves providing services, the agency must ensure clients can transact with the New Zealand government with confidence about their physical wellbeing.

Agencies should:

- Take all reasonable precautions which could avoid or reduce the risk of harm to clients.
- Where there are a number of effective physical security measures which would reduce the risk of harm, choose the option which is least restrictive to the client.
- Ensure the agency physical security plan addresses the risk of harm to clients.
- Develop relevant requirements and procedures that identify the precautions to be taken to address the identified risk factors.

PHYSEC6 - Agencies must implement a level of physical security measures that minimises or removes the risk of information assets being made inoperable or inaccessible, or improperly accessed or used.

Agencies should:

- Have in place appropriate building and entry control measures for areas used in the processing and storage of protectively marked information.
- Have in place physical security protection (matching the assessed security risk of aggregated information holdings) for all agency premises, storage facilities and cabling infrastructure.
- Where practical, locate ICT equipment in areas with access control measures in place to restrict use to authorised personnel only and, where physical access control measures are not possible, have in place other control measures.
- Implement policies and procedures to monitor and protect the use and/or maintenance of information, equipment, storage devices and media away from agency premises and, in situations where a risk assessment determines it is necessary, put in place additional control measures.
- Implement policies and processes for the secure disposal and/or re-use of ICT equipment, storage devices and media (including delegation, approval, supervision, removal methods and employee training) that match the assessed security risk of the information holdings stored on the asset.
- Implement general control policies, including a clear desk and clear screen policy.

PHYSEC7 - Agencies must develop plans and protocols to move up to heightened security levels in case of emergency and increased threat. The New Zealand Government may direct its agencies to implement heightened security levels.

Agencies should integrate and coordinate physical security plans and procedures with other emergency prevention and response plans, for example fire, bomb threats, hazardous materials, power failures, evacuations and civil defence emergencies.

PERSEC1 - Agencies must ensure New Zealand government employees, contractors and temporary staff who require ongoing access to New Zealand government information and resources:

- Are eligible to have access.
- Have had their identity established.
- Are suitable to have access, and
- Are willing to comply with government policies, standards, protocols and requirements that safeguard that agency's resources (people, information and assets) from harm.

Agencies must have in place policies and procedures to assess and manage the ongoing suitability for employment of all staff and contractors.

PERSEC2 - Agencies must:

- Identify positions within their agency that require access to CONFIDENTIAL, SECRET and TOP SECRET assets and information.
- Ensure the level of security clearance sought is necessary, and
- Ensure personnel have the requisite level of security clearance prior to being granted access to information protectively marked as CONFIDENTIAL or higher.

PERSEC3 - Agencies must maintain a register of personnel and contractors who hold a security clearance.

- The fundamental rule of personnel security is that agencies should base all access decisions on the need-to-know principle.
- Before granting access, agencies should establish the existence of a legitimate need to access protectively marked resources to carry out official duties.
- Other justifications, such as a position of authority or the desire to enter controlled areas for the sake of convenience, are not valid.

PERSEC4 - An application for a security clearance must be sponsored by a New Zealand government agency.

PERSEC5 - Agency heads must obtain a recommendation from the NZSIS prior to granting a security clearance. Agencies must follow the Protective Security Requirements Personnel Security Management Protocol and supporting requirements for personnel security.

- The NZSIS has the statutory mandate for the security vetting process and for making recommendations on security trustworthiness. Only the NZSIS may conduct security vetting for the New Zealand government. Agencies must receive a security vetting recommendation from the NZSIS before granting a national security clearance.
- The security vetting process is intrusive by its very nature and the NZSIS must conduct the process with care and sensitivity, and in accordance with government policy.

- All vetting decisions are based on an assessment of the whole person and at all stages must be made in accordance with the principles of natural justice and procedural fairness.
- NZSIS must resolve any doubts about the suitability of a candidate to access national security classified resources.

PERSEC6 - Agencies must have personnel security clearance management arrangements in place for all staff, including contractors, who hold a security clearance.

There are four levels of national security vetting, each involving more rigorous checking. They are listed below.

- CONFIDENTIAL – an assessment of the individual's suitability for ongoing access to New Zealand government resources protectively marked at the CONFIDENTIAL level.
- SECRET – an assessment of the individual's suitability for ongoing access to CONFIDENTIAL and SECRET protectively marked resources.
- TOP SECRET – an assessment of the individual's suitability for ongoing access to resources that have been protectively marked CONFIDENTIAL, SECRET or TOP SECRET. This includes resources that carry compartmented markings.
- TOP SECRET SPECIAL – an assessment of the individual's suitability for ongoing access to all resources protectively marked under the security classification system, including resources that carry compartmented markings. This level of security vetting usually relates to employment within an agency in the New Zealand Intelligence Community.

PERSEC7 - Agencies must notify the NZSIS of the granting, downgrading, suspension or cancellation of a security clearance. Any reason associated with disciplinary action or unsuitability of the candidate to obtain/maintain the appropriate level of clearance must be reported to the NZSIS.

Personnel security is an important element of an agency's protective security regime, as is sound overall management practice.

The initial security vetting process only provides a snapshot of an individual at a particular point in time.

Aside from formal periodic and NZSIS-initiated reviews of national security clearances, agency managers are responsible for providing ongoing support, awareness and education as part of an agency's security clearance management regime.

Agencies should have in place security clearance management processes that provide for the timely identification and assessment of issues that may impact an individual's continued suitability to hold a security clearance.

These processes should complement, but not substitute, clearance review and security education processes.

Security clearance management processes should:

- Include tailored, agency-specific security clearance management programmes.
- Provide clear instructions and requirements in agency security clearance management policy and procedures.
- Through security education and training, regularly reinforce the requirement for staff to report relevant contacts and changes in personal circumstances.

Information Security – Operations Security

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	Information Security Manager
Document Owner Name	Chief Information Officer (CISO)
Document Owner Title	Geoff King

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version
2.0	Jeremy Marshall	23/11/2017	Final Version

Document 8

Information Security – Operations Security

Contents

Information Security – Operations Security

1. Overview

1.1 Purpose

To ensure appropriate controls are implemented to protect the operational integrity and recoverability of the Waikato DHB's applications and information including;

- The requirements for the backup of information, software, and systems. This must include the level of protection required for the different categories of systems and the expected retention of the data being protected.
- The IT response to a disaster event and where it sits in the Waikato DHB's business continuity plan.
- The removal or upgrade of unsupported legacy software.
- Protection against malicious software such as malware, ransomware is implemented.
- Requirements for the frequency and type of testing of information, software, and system integrity.

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as "Users" in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

Operational systems not supported by or under the control of information Services (IS) or have no dependency on or impact to IS operational service and security activities.

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the DHB must comply with the DHB's policies and protocols and are responsible for ensuring that information security is adequately

addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.

- Information Services are responsible for:

(a) Maintaining and advising the Waikato DHB's Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.

(b) Ensuring appropriate operating procedures are created, implemented, and maintained to manage and protect the Waikato DHB computer and network environment.

(c) Ensuring appropriate service level agreements are agreed with business owner(s) for each category of system/service implemented and operated.

(d) Managing security incidents and events, including physical security breaches or incidents associated with a malware, hacking or cyber-security attack.

(e) Ensuring all systems are monitored, with operator and fault logs checked regularly to ensure problems are identified and corrected before presenting an operational impact.

(f) Completing regular checks to ensure access to systems and networks are secure including penetration tests and vulnerability assessments.

(g) Implementing tools to enable the detection and prevention of unauthorised information transfer.

(h) Ensuring data is backed up and stored in a protected location.

- Business Owners and Users are responsible for:

(a) Ensuring compliance with the Information Security Policy and Operations Security Protocol.

(b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.

(c) Using information assets and resources in accordance with IS Security and Acceptable Use policies.

(d) Logging faults and incidents with the IS Service Desk in a timely manner.

(e) Developing and testing Business Continuity Plans (BCP).

4. Standards

- Operating procedures will be documented and should specify, at a detailed level, the steps necessary to perform operational tasks for the system or service including;
  - Processing and handling of information.
  - Backups and restores.
  - Scheduling of regular jobs or tasks; dependencies on other jobs, systems or events.
  - Handling of error or unusual conditions.
  - Support contacts.
  - Certificate renewals.

  - Handling instructions for confidential output or special stationery, including secure disposal of output.
  - Capacity management.
  - Availability Management.
  - System restart and recovery procedures.
  - Management of audit trails and system logs.

- A formal regime of backups must be in place to enable bot partial and full recovery of the Waikato DHB's systems and data in the event of a failure or disaster.

- The procedure for recovery of the Waikato DHB's systems and data from backup must be fully documented and tested on a regular basis including both partial and full system restores.

- A Disaster Recovery Plan should be developed and outline the steps and approaches required to restore services in the event of various disaster scenarios and must be reviewed and tested on an annual basis.

- The level and frequency of the backups and the number of generations of backup should be defined and be sufficient to fulfil both the recovery and archiving requirements of the Waikato DHB.

- All data must be classified according to data security standards so the appropriate retention policy can be applied.

- Backups should be stored at a separate and secure and media containing backups should be stored under appropriate environmental conditions and be subject to the same levels of security as the production environment.

- Formal procedures should control the secure disposal and/or transfer of media containing sensitive information in order to minimise the risk of information being exposed to unauthorised persons.

- All physically stored media, including that stored or transported off-site, should be encrypted.

- Any reusable media must be rendered unreadable if it is to be removed from the Waikato DHB's premises for reuse elsewhere.

- All computer time clocks should be synchronised to the same source, preferably a known accurate time source.

- All changes to information assets and resources must be subject to change control processes in accordance with the Waikato DHB's Change and Release Management policy.

- The change control procedure should be documented, approved by management and complied with to ensure proper control is maintained over changes and include:

  - Categorisation of change based on risk and impact.
  - Recording of changes.
  - Risk assessments of;
    - Applying the change.

    - Not applying the change.
    - Security and privacy implications.
  - Mitigations and controls.
  - Planning and testing the change.
  - Formal review and approval process.
  - Communication/training plan.
  - Back-out plan in case the change fails or unforeseen results occur.

- Testing must not be carried out on production systems and development, test and production environments must be separated to minimise the risk of unauthorised or unintentional changes being applied to production systems.

- Usage will be monitored and reported to ensure satisfactory system performance is maintained and expected future changes in capacity demands taken into account and planned for accordingly. This will include current trends in the requirements of existing systems and services, and also planned new systems and services.

- Processes will be developed to regularly:

  - Decommission systems that are not required.
  - Optimise databases.
  - Archive data that is not accessed regularly.

- To reduce the risks in service transition new or upgraded systems and services will be subject to a formal acceptance/approval process.

- Requirements for acceptance should be agreed, documented and tested prior to the system or service being implemented.

- Test results and acceptance of the new or upgraded system or service should be formally documented and the following considered:

  - Capacity requirements
  - Error recovery and restart procedures
  - Contingency plans
  - Testing plan against user requirements
  - Security controls
  - Residual Risk acceptance
  - Manual procedures
  - Business continuity plans
  - Potential effect on existing systems and services
  - Training plans

- Information security requirements should be incorporated into third party service delivery agreements and providers monitored to ensure requirements are being fulfilled.

- Key points for consideration for inclusion in third party agreements/contracts will include, but not be limited to:

  - Responsibility for any residual risks
  - Security requirements placed upon the third party
  - Security of sensitive information held by the third party

  - Non-disclosure clauses
  - Service Level Agreements
  - Escrow arrangements
  - Change management procedures
  - Penalties for breach of confidentiality or misuse of information and/or systems
  - Permitted access levels
  - Authentication of third party users
  - Methods of access
  - Rights to monitor third party activity and audit security processes
  - Third Party's duty to report any actual or suspected security breaches of its own systems.
  - Third party compliance with the DHB's security policies and protocols
  - Requirements to return or destroy all information and assets when the
  - agreement expires or is terminated
  - The right of the DHB to renegotiate the terms of the agreement in the event that security requirements change.

- All third party supply agreements must be subject to a full information security risk assessment prior to contract engagement and where required attestation and evidence of information security controls obtained and reviewed with any residual risk identified and controlled.

- Responsibility for managing the relationship with a third party will be assigned to a designated individual or team and service delivery reports provided by the third party will be reviewed and reported on a regular basis.

- Service audits will be carried out to ensure the conditions of the third party agreement are being fulfilled and performance levels are acceptable.

- Any changes to the provision of third party services should trigger a reassessment of the risks. The risk assessment should be proportionate to the criticality of the service and the magnitude of the proposed changes.

- The Information Services Configuration Management Data Base (CMDB) will be used to record and manage all information assets and resources and procedures developed to ensure information currency and accuracy.

- A configuration control system will be used to track versions/revisions of software implemented and their relevant documentation.

- Roles and responsibilities for vulnerability management including vulnerability monitoring, assessment and coordination responsibilities will be defined and assigned.

- A formal processes outlining standard and urgent patch application, setting out the criteria that must be met before urgent patching takes place will be defined and implemented.

- Where a vulnerability is known or identified but no patch is currently available, other alternatives to mitigate risk (such as firewall controls to limit functionality or restrict access), and prevent execution of suspect executable files will be used.

- Firmware on devices will be updated annually, with a more regular requirement if security vulnerabilities are behind the reason for the update.

- Where devices are no longer supported and software updates are not available, a risk assessment must be performed to determine the impact of an incident and the increased vulnerability.
- Anti-virus software will be installed on all servers and clients and configured to carry out "on-access" scanning of files. The software will also be configured to automatically download and install updates to signature files and scanning engines.
- All information assets and resources will be protected in accordance with standards defined in the anti-malware protocol.
- All new versions of software and features will be tested before deployment and vendors will be required evidence adequate testing, before deploying new versions and features.
- Monitoring over the complete ICT environment will be carried out to log and/or alert for the following activities:
  - Unauthorised activity.
  - Performance.
  - Capacity.
  - The installation of unauthorised software.
  - Data integrity.
  - Hardware faults.
  - Ensure logging is occurring.
  - Changes to system configuration.
  - The activation/deactivation of prevention systems such as malware protection.
- Logs recording user activities, including security-related events, should be retained for a prescribed period for investigatory purposes.
- System administrators will be prohibited from changing, erasing or deactivating logs of their own activities.
- All activity logs should be protected against unauthorised access, changes or erasure. It may be necessary to preserve some logs for business reasons or for retention of evidence in the event of a security breach.

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.
- Project Assurance Program.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*
- *SANS Top 20*

Information Security – Suppliers

Protocol Responsibilities and Authorisation

Department Responsible for Protocol	Information Services
Document Facilitator Name	Suranwan Wickramasuriya
Document Facilitator Title	Information Security Manager
Document Owner Name	Chief Information Officer (CISO)
Document Owner Title	Geoff King

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Protocol Review History

Version	Updated by	Date Updated	Description of Changes
1.0	Jeremy Marshall	04/05/2017	Initial version

Information Security – Suppliers

Contents

Information Security – Suppliers

1. Overview

1.1 Purpose

To implement procedures to protect sensitive information exposed to third party organisations involved throughout a supply chain process agreed upon within contractual agreements.

The review and auditing of services against contractual agreements by external suppliers must be informed by the following policies;

- Define and document the criteria for selecting a supplier.
- Assess supplier risks.
- Create a formal contract and confidentiality agreement.
- Establish access controls appropriate to the degree of risk identified.
- Monitor compliance with all contractual terms.
- Ensure that all information assets and resources are returned and all access rights revoked, on the termination of agreements.
- Ensure all information and/or data is disposed of securely , on the termination of agreements
- Ensure suppliers and government information is appropriately protected

1.2 Scope

This protocol applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB and (collectively referred to as “Users” in this Policy).

The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.

1.3 Out of Scope

Procurement initiatives that does not have an ICT or information Security reliance or implication.

1.4 Exceptions/Contradictions

Any exceptions to this protocol will be subject to a risk assessment and require sign-off by the CIO/CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.

- All vendors and partners working with or for the DHB must comply with the DHB's policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.
- Information Services are responsible for:
  (a) Maintaining and advising the Waikato DHB's Information Security Policy and supporting protocols and ensuring all required controls, procedures and processes are in place.
  (b) Mandating security controls to identify and manage security risks.
  (c) Assessing and managing technical security risks associated with suppliers.
  (d) Implementing controls for the monitoring and auditing of supplier information access.
  (e) Implementing controls for monitoring the exchange of information between various parties to ensure agreed requirements are met and any risk not covered in the original agreement are highlighted.
- Business Owners and Users are responsible for:
  (a) Ensuring compliance with the Information Security Policy, Protocols and supporting processes and procedures and applying the defined standards to information assets and resources maintained within service control.
  (b) Ensuring staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.
  (c) Assess and manage business, commercial, financial and legal risk associated with suppliers.
  (d) Approve potential suppliers based on risk profile.
  (e) Determine the frequency of audits.
  (f) Appoint legal representation to oversee contracts and agreements.
  (g) Assign responsibility for managing supplier relationships to an individual (eg, contracts or commercial manager).

4. Standards

- Supplier agreements will be established to clarify the roles and responsibilities of all parties involved in fulfilling information security requirements.
- Types of information access should be defined and procedures for monitoring and controlling access implemented.
- All information security risks to the Waikato DHB's information assets and resources from external parties shall be identified and appropriate controls agreed and implemented before confirming contracts or engagement.

- Legal and regulatory requirements, including data protection, intellectual property rights, and copyright should be clearly identified and addressed.
- Supplier service delivery should be monitored, reviewed and assessed to ensure it meets appropriate security and contract or SLA requirements.
- Suppliers will implement agreed information security controls to safeguard the confidentiality, availability and integrity of the Waikato DHB and its information.
- Suppliers will provide the Waikato DHB with evidence and/or attestation of security controls that;
  - Protect the Confidentiality, Integrity and Availability of DHB systems and data.
  - Prevent unauthorised access to and/or use of DHB systems and Data.
  - Reduces the risk of misuse of Information.
  - Detect and resolve security breaches.
- All Suppliers of hosted, outsourced or 'Cloud' based services will be subject to information security and privacy risk assessments including all necessary GCIO/DIA mandated compliance checks.
- Suppliers should be regularly monitored to assure ongoing compliance with information security requirements and to ensure security controls are operated and maintained properly.
- Controls for managing the exchange of information between parties should be implemented to ensure;
  - All sensitive information is protected.
  - Information is encrypted when stored on portable devices and media or when transmitted over non-secure communication channels (e.g. internet, email or wireless networks).
  - Information is disposed of securely.
- Suppliers will confirm the identities of personnel using independent, verifiable identity prior to creating any accounts that will provide access to the Waikato DHB's Information Systems.
- Suppliers must ensure security controls are implemented to prevent, detect, mitigate and protect against the introduction of Unauthorised Code or Malware into either the Supplier's Information Systems or any Waikato DHB Information Systems.
- The Waikato DHB will periodically review the Supplier's and/or Supplier Affiliates' operations, processes and systems to assure and confirm ongoing compliance with agreed security controls.
- Suppliers shall implement all recommendations resulting from any such audit having been conducted.
- Supplier's will have an information security incident management policy and process in place and will immediately notify the Waikato DHB of any suspected and/or actual security events, incidents and cybercrime attacks by contacting the IS Service Desk.

5. Patient Information

A large number of DHB information assets and resources store and process patient identifiable information which can be confidential or sensitive in nature.

All impacts and risks to patient information must be measured against both security and privacy standards.

6. Audit Indicators

- Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.
- Project Assurance Program.

7. References

- *Health Information Security Framework (HISO 10029.2015)*
- *New Zealand Information Security Manual (NZISM)*
- *New Zealand Health Information Privacy Code*
- *New Zealand Privacy Act*
- *All-of-Government ICT Project Assurance Framework*
- *All-of-Government ICT Operations Assurance Framework*
- *WDHB IS Security Policy*
- *WDHB Privacy Policy*
- *SANS Top 20*

Information Security Policy

Policy Responsibilities and Authorisation

Department Responsible for Policy	Information Services
Document Facilitator Title	Information Security Manager
Document Facilitator Name	Suranwan Wickramasuriya
Document Owner Title	Executive Director Corporate Services
Document Owner Name	Maureen Chrystal
Target Audience	All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB (collectively referred to as “Users” in this Policy).
Committee Approved	Policies and Guidelines Committee
Date Approved	24 May 2018
Committee Endorsed	Executive Group
Date Endorsed	6 July 2018
Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.	

Policy Review History

Version	Updated by	Date Updated	Summary of Changes
2	S. Honig	30/04/2015	Current published policy
3	S. Wickramasuriya	30/05/2017	Redraft into new format with HISF changes included
4	Tony Haigh	14/03/2018	Add links, standard format, distribution copy for review
5	Jeremy Marshall	10/5/2018	Amend following Consultation and feedback

Information Security Policy

Contents

Information Security Policy

1. Introduction

1.1 Purpose

The Waikato DHB is required to ensure threats to the confidentiality, integrity and availability of its information assets and resources are effectively identified, assessed, recorded, prioritised and managed.

This policy establishes the Waikato District Health Board's (Waikato DHB) approach to managing information security including:

- Establishing clear lines of accountability for information security management and governance.
- Maintaining a secure computing environment and to protect Waikato DHB information assets and resources against loss or unauthorised access and use.
- Promoting patient safety through the application of security controls and guidance.
- Embedding information security into everyday practice by clarifying the actions required of all staff to protect the Waikato DHB's information assets and resources.
- Identifying, assessing and effectively managing information security risks.
- Meeting statutory and regulatory compliance requirements for the management of information security risks and controls.
- Formal recognition of the commitment to the continuous improvement of information security within the organisation.
- Ensuring Information collected, stored, transmitted and processed by the Waikato DHB will be classified in accordance with the protective markings defined in the Government Communications Security Bureau (GCSB) Protective Security Requirements and the endorsements mandated in the Health Information Security Framework (HISF).
- Formal recognition of the Waikato DHB Director of Information Services as the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).
- Formal recognition that the Waikato DHB's information security management system (ISMS) based on and comply with the Health Information Security Framework (HISF) 10029.1 and the New Zealand Information Security Manual (NZISM).

1.2 Scope

This policy applies to:

- All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB (collectively referred to as "Users" in this Policy).
- The use of all information assets and resources, data and information, electronic and computing devices, and networks used to conduct Waikato DHB business.
- All third parties providing ICT goods and services to the Waikato DHB must be assessed in against the security policy and supporting protocols.
- Additional areas within information security are supported by the following policies:

Acceptable Use: A separate policy 'Acceptable Use of Information Systems' covers the use of Waikato DHB's technology equipment, systems, resources and data.

Change Management: A separate policy 'Information Communications Technology (ICT): Change Management' establishes the Waikato District Health Board's (Waikato DHB) requirements for managing change to its Information Communications Technology (ICT) environment

Mobile Communications Devices: The 'Mobile Communications Devices policy' covers the use of Waikato DHB's mobile technology equipment.

Social Media and the Internet/Intranet: Use of social media and the internet/intranet are covered by the 'Media and Communications policy'.

Intellectual Property: The 'Intellectual Property policy' covers the ownership of intellectual property created by an employee in the course of their employment.

Patient Data Privacy and Confidentiality: Matters relating to patient data privacy and confidentiality are managed under the conveyance of the Waikato DHB's Privacy Office in accordance with the 'Information Privacy policy'.

Physical Security: Matters relating to physical security are additionally managed by the Property and Infrastructure service in accordance with the Property and Infrastructure 'Security policy'.

Clinical Records: Clinical Records Management is subject to the 'Clinical Records Management policy'.

Corporate Records: Corporate Records Management is subject to the 'Corporate Records Management policy'.

Risk Management: Management of Waikato DHB risk is subject to the 'Risk Management policy'.

1.3 Exceptions

Any exceptions to this policy and/or supporting protocols must be initiated by a request to the Information Services 'Service Desk', be subject to a security risk assessment and authorisation by the CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Policy Statements

It is the Waikato DHB's policy;

- To ensure the confidentiality, integrity and availability of information assets and resources is maintained and that all reasonable steps are taken to maintain the security and reliability of the Waikato DHB computing environment.

- To enable Waikato DHB users to provide the best service possible while exchanging information and ideas in a secure environment where risk is managed and protection of assets is comprehensive.

4. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to take all reasonable precautions to protect the security of all sites, services, systems and information assets and resources.
- **Waikato DHB Board** - Approving the Risk Appetite statement to serve as the foundation for security programs, reviewing risk and evaluating management decisions on security responses.
- **Chief Executive Officer (CEO)** - Overall accountability for the operations of the Waikato DHB ensuring information protection and assurance activities are funded and supported to meet the Waikato DHB's objectives.
- **Information Security and Privacy Governance Group (ISPGG)** - Establishing the Waikato DHB's Risk Appetite and ensuring management processes support the effective management and control of information security risks.
- **Chief Information Security Officer (CISO)** - Responsible for managing the security strategy, endorsing the supporting security policies and control measures and ensuring adequate funding and resources are available to achieve objectives.
- **Information Security Manager (ISM)** - Acts as a conduit between strategic directions from the CISO and their implementation. Maintaining the management, administrative and process controls relating to organisational information security. The Information Security Manager will maintain the Information Security Risk Register and will advise the Security Governance Group and Board on the status, risks, issues and breaches related to information security.
- **Information Services (IS)** - Responsible for maintaining and advising the organisations Information Security Policies and ensuring all required supporting controls, protocols, procedures and processes are in place to protect and control the use of information assets and resources and that all employees, partners and suppliers are aware of policy and are kept informed of any changes and updates.
- **Corporate Records** - Responsible for ensuring compliance with the Waikato DHB's 'Corporate Records Management Policy' and that the policy aligns with the 'Information Security Policy' and supports the organisations Information Security objectives.
- **Human Resources** - Responsible for ensuring HR policies and process support the Waikato DHB's information Security objectives and providing guidance and support in the resolution of security breaches.
- **Internal Audit** - Responsible for ensuring an audit and assurance program is in place and where required carrying out audit and assurance activities to measure and assess the adequacy and efficacy of the security controls and approaches in place.

- **Media and Communications** - Ensuring that the promotion of health services and information through social media aligns with policy is fit for purpose, follows best practice and supports the organisation's vision, values and priorities.
- **Privacy Officer** - Responsible for promoting privacy and ensuring compliance with the Health Information Privacy Code 1994 and the Privacy Act 1993, managing and responding to any investigations by the Privacy Commissioner and advising on privacy related matters and risks.
- **Property and Infrastructure** - Responsible for ensuring safe and secure environments for patients, visitors, non-employees, volunteers, contractors and staff at Waikato DHB sites (including staff working in the community).
- **Managers and Business Owners** - Responsible for ensuring that information security has been adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems and that staff are aware of their security responsibilities and adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.
- **Users** - Complying with information security policies and protocols and reporting any information security weaknesses, breaches or violations to Information Services. All users of Waikato DHB information assets and resources are responsible for exercising good judgment regarding appropriate use in accordance with both Waikato DHB policies and standards, and local laws and regulations.

5. Governance

- Governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, risks are managed appropriately and Waikato DHB resources are used responsibly.
- Information security governance consists of the leadership, organisational structures and processes that safeguard information. The five basic outcomes of information security governance will include:
  - Strategic alignment of information security with business strategy to support organisational objectives.
  - Risk management by executing appropriate measures to manage and mitigate risks and reduce potential impacts on information resources to an acceptable level.
  - Resource management by utilising information security knowledge and infrastructure efficiently and effectively.
  - Performance measurement by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved.
  - Value delivery by optimising information security investments in support of organisational objectives.
  - The Executive will appoint a multi-disciplinary Information Security and Privacy Governance Group (ISP-GG) and set its Terms of Reference.

6. ISMS (Information Security Management System)

- An Information Security Management Systems (ISMS) is a systematic and structured approach to managing information so that it remains secure and includes the policies, processes, procedures, organizational structures and software and hardware functions required to meet the organisations security objectives.
- The ISMS will define roles and responsibilities and direct, monitor and control the implementation, operation and management of information security within Waikato DHB, in accordance with its policies and legal, regulatory and contractual requirements allowing information to be processed, managed and shared with the confidence that its security is assured and that information security risks have been identified, understood and treated appropriately.
- The ISP-GG will be responsible for ensuring that;
  - The DHB's Risk Appetite is defined and management processes support the effective management and control of information security risks.
  - Security by Design is embedded into the culture of the organisation.
  - The security framework is promoted and adopted by the organisation including;
    - Reviewing and endorsing Information Security policies and protocols.
    - Monitoring significant changes in the exposure of information assets to major threats.
    - Reviewing and monitoring Information Security incidents.
    - Approving major initiatives to enhance Information Security.
  - The ISP-GG will review the ISMS annually and Internal Audit will audit the ISMS framework as part of the agreed audit program.
  - The Information Security Manager is responsible for preparing the ISMS, in consultation with the CIO, Corporate Privacy Officer and other members of the Executive and the ISP-GG.

7. Protocols

7.1 Risk Management

Health care organisations are responsible for reducing or mitigating risks to their assets. They must show a clear understanding of the risks to and potential impacts on information security that the organisation faces.

Risk management applies to day-to-day operations, as well as to major failures of information systems or other disruptive events.

For more information refer to the Information Security - Risk Management protocol.

7.2 Information Security

Based on the HISF framework the Information Security protocol addresses security principles and security responsibilities for Waikato DHB's information assets and resources.

For more information refer to the Information Security - Information Security Management protocol.

7.3 Asset Management

To identify assets belonging to the organisation and define and allocate responsibilities for the protection of these assets based on their importance to the organisation and to ensure assets are continuously maintained to an appropriate security baseline that minimises their vulnerabilities and threat exposure, such as regular patching and other activities.

For more information refer to the Information Security - Asset Management protocol.

7.4 Human Resource Security

Patients expect their health information to be maintained confidentially and securely by those authorised to use it and Human Resource security will ensure that employees, contractors and third party users conform to the organisation's health information security policy and procedures.

For more information refer to the Information Security - Human Resources Security protocol.

7.5 Physical and Environmental Security

To prevent unauthorised physical or electronic access to the organisation's information assets and resources and information processing facilities in order to guard against loss, damage, theft, interference or compromise of assets, and interruption to the organisation's operations.

For more information refer to the Information Security - Physical and Environmental Security protocol.

7.6 Communications

To ensure the confidentiality, integrity and availability of information communicated across networks.

For more information refer to the Information Security - Communications protocol.

7.7 Operations Security

To ensure appropriate controls are implemented to protect the operational integrity and recoverability of the organisation's information assets and resources.

For more information refer to the Information Security - Operations Security protocol.

7.8 Access Control

Access control will prevent unauthorised persons accessing health information, ensuring it remains confidential. Authorised users will be able to view and process only the information they are entitled to and have a need to access.

For more information refer to the Information Security - Access Control protocol.

7.9 Information Systems Acquisition, Development and Maintenance

To ensure health information security is an integral part of the information system lifecycle and that all change initiatives to information assets and resources meet "Security and Privacy' by design objectives.

For more information refer to the Information Security - IS Acquisition, Development and Maintenance protocol.

7.10 Information Security Incident Management

Ensure the appropriate tools, processes and procedures are in place to detect, report and manage information security incidents.

For more information refer to the Information Security - Information Security Incident Management protocol.

7.11 Business Continuity Management

Information security must be embedded in the organisation's business continuity management systems to ensure ongoing availability of information assets and resources.

For more information refer to the Information Security - Business Continuity Management protocol.

7.12 Compliance

To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and/or security requirements the organisation's approach to meeting these requirements must be explicitly identified, documented and kept up to date for each information system.

For more information refer to the Information Security - Compliance protocol.

7.13 Cryptography and Cryptographic Key Management

To ensure the effective use of cryptography to protect data and maintain the confidentiality, integrity and availability of information assets and resources.

For more information refer to the Information Security - Cryptography protocol.

7.14 Suppliers

Implement procedures to protect health information exposed to third party organisations involved throughout a supply chain process agreed on within contractual agreements.

For more information refer to the Information Security - Suppliers protocol.

7.15 Cloud Computing and Outsourced Processing

To ensure security controls applied by cloud service providers are appropriate, clearly specified and where required, are built into contracts and agreements.

For more information refer to the Information Security - Cloud Computing protocol.

7.16 Assurance over Security

To provide stakeholders, management and users with a degree of confidence that information and processes requiring protection have had their security scrutinised and have been found to be robust and clearly meet or exceed the security aspects of the Health Information Privacy Code.

For more information refer to the Information Security - Assurance protocol.

7.17 Anti-Malware

To define the minimum security requirements, standards and processes required to prevent malware infection of Waikato District Health Board's information assets and resources.

For more information refer to the Information Security – Anti-Malware protocol.

7.18 Information and Data Management

All information and data should be classified, protected and appropriately obtained and managed to ensure confidentiality, integrity and availability.

For more information refer to the Information Security - Information and Data Management protocol.

8. Principles

The following principles will be used to guide activities related to information security.

8.1 Security by Design

Promote a culture within the organisation where everyone recognises the importance of information security, are aware of their responsibilities and establish an information security policy as the foundation for informed design decisions.

8.2 Managed Risk

Manage risk consistent with the risk appetite as defined by the ISP-GG and provide decision-makers with information that enables the Waikato DHB to balance risk and opportunity and to reduce or mitigate risks and manage the potential impacts on information security the organisation faces.

8.3 Confidentiality, Integrity and Availability

Confidentiality, integrity and availability are the concepts most basic to information security and will be the core objectives of information security efforts.

Confidentiality - information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity - maintaining and assuring the accuracy and completeness of data over its entire life-cycle.

Availability - information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

8.4 Defence in Depth

Enable information security through a balanced and cost-effective mix of countermeasures, distributed physically and logically.

8.5 Simplicity

Use common language in developing information security requirements and base information security on open standards for portability and interoperability.

8.6 Usability and Manageability

As much as possible, automate identity and access management and design information security to allow for adoption of new technology and upgrades and ease of operational use.

9. Audit

The Policy and supporting protocol will be subject to audit as part of;

- Annual ICT Audit Program
- Annual NZ Audit ICT Controls Audit
- IS Operational Assurance Framework

10. References

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- Protective Security Requirements 2014
- Health Information Security Framework (HISO 10029.1)
- New Zealand Information Security Manual (NZISM, December 2014)
- Health Information Privacy Code (1994, as amended)
- Security in the Government Sector (2002)
- SANS Top 20

11. Associated Documents

- Waikato DHB Acceptable Use of Information Systems policy (Ref. 2191)
- Waikato DHB Clinical Records Management policy (Ref. 0182)
- Waikato DHB Corporate Records Management policy (Ref. 0905)
- Waikato DHB Risk Management policy (Ref. 0118)
- Waikato DHB Information Communications Technology (ICT): Change Management policy (Ref. 2744)
- Waikato DHB Information Privacy policy (Ref. 1976)
- Waikato DHB Intellectual Property policy (Ref. 1036)
- Waikato DHB Media and Communications policy (Ref. 1816)
- Waikato DHB Mobile Communications Devices policy (Ref. 1853)
- Waikato DHB Security policy (Ref. 0120)
- Waikato DHB Definitions – Information Services protocol (Ref. 5799)
- Waikato DHB Information Security - Access Control protocol (Ref. 5848)
- Waikato DHB Information Security - Anti Malware protocol (Ref. 5857)
- Waikato DHB Information Security - Asset Management protocol (Ref. 5848)
- Waikato DHB Information Security - Assurance protocol (Ref. 5856)
- Waikato DHB Information Security - Business Continuity Management protocol (Ref. 5851)
- Waikato DHB Information Security - Cloud Computing protocol (Ref. 5855)
- Waikato DHB Information Security - Communications protocol (Ref. 5846)
- Waikato DHB Information Security - Compliance protocol (Ref. 5852)
- Waikato DHB Information Security - Cryptography protocol (Ref. 5853)
- Waikato DHB Information Security - Human Resources Security protocol (Ref. 5844)
- Waikato DHB Information Security - Information and Data Management protocol (Ref. 5858)
- Waikato DHB Information Security - Information Security Incident Management protocol (Ref. 5850)
- Waikato DHB Information Security - Information Security Management protocol (Ref. 5842)
- Waikato DHB Information Security - IS Acquisition, Development and Maintenance protocol (Ref. 5849)
- Waikato DHB Information Security - Operations Security protocol (Ref. 5847)
- Waikato DHB Information Security - Physical and Environmental Security protocol (Ref. 5845)
- Waikato DHB Information Security - Risk Management protocol (Ref. 5841)
- Waikato DHB Information Security - Suppliers protocol (Ref. 5854)

Mobile Communication Devices

Policy Responsibilities and Authorisation

Department Responsible for Policy	Information Services
Document Facilitator Title	Suranwan Wickramasuriya
Document Facilitator Name	Information Security Manager
Document Owner Title	Executive Director, Office of the Chief Executive
Document Owner Name	Neville Hablous
Target Audience	All staff
Committee Approved	Policies and Guidelines
Date Approved	14 December 2017
Committee Endorsed	Executive Group
Date Endorsed	19 February 2018

Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.

Policy Review History

Version	Updated by	Date Updated	Summary of Changes
7.0	J.Scott	05/09/2014	Current published policy
8.0	J.Marshall	08/08/2017	Redraft into new policy format and to support clearer definition of monitoring and OIA requirements.
9.0	J.Marshall	22/11/2017	Changes following feedback from review group.
9.1	J.Marshall	25/05/2018	Additional changes following CSC form changes and networks input.
9.2	J.Marshall	28/09/2018	Changes to accommodate devices issued for shared usage
9.3	J.Marshall	7/12/2018	Changes to use of equipment in proximity to mobile devices,

Mobile Communication Devices

Contents

Mobile Communication Devices

1. Overview

1.1 Purpose

To ensure that mobile communications devices accessing Waikato DHB information assets and resources are used appropriately, responsibly and ethically and establish the management and safety controls necessary for the appropriate use of these devices in Waikato DHB facilities by staff, contractors, visitors and patients.

1.2 Background

The Waikato DHB is required to ensure that threats to the confidentiality, integrity and availability of its information assets and resources are effectively identified, assessed, recorded, prioritised and managed.

1.3 Scope

This policy applies to all Waikato DHB employees, Board members, contractors, consultants, temporary staff and all personnel affiliated with third parties providing services to Waikato DHB (collectively referred to as "Users").

The policy includes all mobile communications devices and mobile connections that are used to gain access to Waikato DHB information, networks and systems, whether;

- Provided by the Waikato DHB
- Personally owned and used for Waikato DHB purposes under an authorised Bring Your Own Device (BYOD) programme
- Provided by other parties (external contracting firms, outsourced providers etc.)
- Using mobile data networks or Waikato DHB Wireless networks

A mobile device is defined as any smartphone, tablet, laptop, notebook, or ultra-book which is capable of connecting to the Waikato DHB's network infrastructure or to the mobile phone network to send and receive data. These devices are typically built around the Apple, Android, or Microsoft operating systems.

1.4 Out of Scope

Desktop computer equipment, modalities and biomedical equipment and personal mobile devices not connecting to or accessing Waikato DHB networks and/or data, excepting where those devices and/or their use could negatively impact the provision of clinical services.

1.5 Exceptions/Contradictions

Information Security: A separate policy "Information Security Policy' covers overall application, management and control of Information Security within the Waikato.

Acceptable Use: A separate policy 'Information Systems Acceptable Use Policy' covers the use of Waikato DHB's technology equipment, systems, resources and data.

Social Media and the Internet/Intranet: Use of Social Media and the Internet/Intranet is covered by the 'Media and Communications Policy'.

Intellectual Property: The 'Intellectual Property Policy' covers the ownership of intellectual property created by an employee in the course of their employment.

Patient Data Privacy and Confidentiality: Matters relating to patient data privacy and confidentiality are managed under the conveyance of the DHB's Privacy Office in accordance with the 'Information Privacy Policy'.

Physical Security: Matters relating to physical security are additionally managed by the Property and Infrastructure service in accordance with the Property and Infrastructure 'Security Policy'.

Clinical Records: Clinical Records Management is subject to the 'Clinical Records Management Policy'.

Corporate Records: Corporate Records Management is subject to the 'Corporate Records Management Policy'.

Human Resources (HR): Matters relating to HR and/or disciplinary issues must be managed by the relevant Service manager, HR department and in accordance with all relevant DHB policies and procedures.

Any exceptions to this policy will be subject to a risk assessment and require formal sign-off by the CIO/CISO and the Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Policy Statements

It is the Waikato DHB's policy;

- To ensure the confidentiality, integrity and availability of information assets and resources is maintained and that all reasonable steps are taken to maintain the security and reliability of the Waikato DHB's computing environment.
- To enable our staff and partners to provide the best care possible for our patients while exchanging information and ideas in a secure environment where risk is managed and protection of assets is comprehensive and pervasive.
- To monitor Mobile communications devices and networks and ensure usage is acceptable and compliant with organisational policy and regulatory controls or in support of a legal discovery process, complaints processes, or Official Information Act (OIA) request.
- To ensure patient care is not compromised by the use of mobile communication devices and Patient safety incidents are monitored as part of this policy implementation.

4. Roles and Responsibilities

- Every employee, consultant or contractor in the health and disability sector has responsibility to maintain day-to-day security of all sites, services, systems and information.
- All vendors and partners working with or for the Waikato DHB must comply with the DHB's policies and protocols and are responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems or service they provide.
- Information Services - Responsible for maintaining and advising the organisations Information Security Policies and ensuring all required controls, protocols, procedures and processes are in place to protect and control the use of information assets and resources and that all employees, partners and suppliers are aware of policy and are kept informed of any changes and updates.
- Managers and Business Owners - Responsible for ensuring that information security is adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems and that staff are aware of their security responsibilities and adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols and ensuring that patient care is not compromised by the use of mobile communication devices and Patient safety incidents are monitored as part of this policy implementation.
- Users - Complying with information security policies and protocols and reporting any information security weaknesses, breaches or violations to Information Services. All users of Waikato DHB information assets and resources are responsible for exercising good judgment regarding appropriate use in accordance with both Waikato DHB policies and standards, and local laws and regulations and ensuring that patient care is not compromised by the use of mobile communication devices and Patient safety incidents are monitored as part of this policy implementation.

5. Standards

- Any mobile communications device used to conduct Waikato DHB business must be utilised appropriately, responsibly, ethically and legally. This includes the use of content, services and applications as well as calling and messaging.
- Waikato DHB Policies including but not limited to; the Vehicle Usage and Safe driving policy and Information Security and Acceptable Use policies apply to all mobile communication devices used for Waikato DHB purposes.
- The Waikato DHB is not accountable for the loss of any personal data or content on any mobile communications device for any reason.
- All requests for the issue of mobile communication devices must:
    - Comply with Information Services 'End User Device Standards'
    - Be made through the IS Customer Portal
    - Be authorised by a Level 4 Manager (as defined within the Delegations of Authority Policy)
    - Be purchased in accordance with the Waikato DHB Procurement policy

- All mobile communications devices provided by the Waikato DHB will be registered to a named individual who is responsible for ensuring the security of the device and payment of personal usage costs.
- All cellular devices will be issued with an international toll bar, no roaming and have GPRS disabled as standard.
- Requests for the removal of the toll bar must be made through the Information Services Customer Portal with Level 4 Manager approval.
- If an employee requires international roaming for Waikato DHB purposes notification to the IS Service Desk is required seven (7) working days prior to departure.
- When purchasing new clinical equipment assurances must be sought from the manufacturer that the equipment is immune to electromagnetic interference and complies with AS/NZS standards (Guide to safe use of electricity in patient care and Medical equipment-General requirements of safety-Parent Standard).
- Users are responsible for securing and taking all reasonable precautions to protect mobile communications devices and the information stored on them.
- All mobile communications devices accessing the Waikato DHB's network or data must be connected to a central management system to ensure security and system integrity of that device.
- All mobile communications devices must be patched and updated on a regular basis in accordance with the standards defined in the anti-malware protocol.
- Laptops must be secured through the Waikato DHB's encryption, anti-malware and configuration management systems.
- Windows based devices must be secured by domain policy and active directory.
- Non-Windows devices must be secured through the Waikato DHB's mobile device management (MDM) solution.
- Patches and firmware upgrades for windows devices must be managed by Microsoft System Centre Configuration Manager (SCCM).
- Patches and firmware upgrades for non-windows devices must be managed through the Waikato DHB's mobile device management (MDM) solution.
- All smartphones that require additional applications (apps) to be installed must be secured through the Waikato DHB's MDM solution.
- The Waikato DHB will make available approved clinical and non-clinical apps, whether public or purchased, through the DHB's MDM corporate application store.
- All Mobile Communications Devices carrying Waikato DHB data or accessing Waikato DHB Information assets and resources, including but not limited to email, photos, images and remote desktop, must:
    - Dependant on model, deploy a minimum 4-5 character PIN or password;
    - Be secured with a PIN/password-protected screen saver with automated activation set to a maximum of 5 minutes;

  - ○ Have Mobile Device Management (MDM) software installed with remote lock/wipe control.

- Devices shared by multiple users must have individual unique login credentials.
- Users may be permitted to connect Waikato DHB laptop PCs to the Internet over 3G or 4G telephone networks by using Mobile Devices as tethered connections or personal wireless hotspots, subject to line manager approval of costs;
- Where devices are provided for use by Waikato DHB staff groups, patients or non-Waikato DHB personnel they must be appropriately configured to maintain the confidentiality, integrity and availability of Waikato DHB systems and data and all users made aware of their responsibilities in relation to the Waikato DHB's policies and usage expectations. The issuing service will be accountable for managing the distribution and use of equipment ensuring users awareness and policy compliance and will be liable for all costs associated with personnel, excessive and/or inappropriate usage.
- Any loss or damage must be reported to the IS Service Desk as soon as possible and where required police reports for stolen equipment forwarded to the IS Service Desk.
- New equipment may be issued where a device has been lost, stolen, damaged or broken and the cost charged against the users RC.
- Cost differential for upgrades over and above standard issue will be charged against the users RC.
- Remote lock/wipe software will be used to disable devices that are lost, stolen or for some other reason compromised.
- Batteries from mobile communication devices must be returned to IS Service Desk for safe disposal.
- All devices must be returned to IS Service Desk for disposal when no longer required.
- Prior to the mobile communications device being returned to Information Services the user and/or their department manager must ensure that all personal settings are removed including but not limited to, any PIN numbers, passwords, account settings for Google Play Store and Apple iTunes and/or iCloud. (Failure to do so renders the device unusable and incurs an unnecessary financial cost to the organisation).
- All devices must be disposed of securely in accordance with IS asset disposal and security standards.
- All mobile communication devices issued by the Waikato DHB, SIM cards and all DHB data stored on a device remain the property of the Waikato DHB.
- When staff terminate their employment with the Waikato DHB their mobile number is retained by the Waikato DHB for future use. Any exceptions to this policy will require approval by the level 4 reporting manager and the Chief Information Officer or authorised delegate.

5.1 Personal Usage

- Mobile communication devices are issued for employment related use unless formally agreed through the signing of the Mobile Communications Devices Acceptance and Responsibility form and approval from a Level 4 manager or above.
- Where it has been agreed that device may be used for personal use, the user is responsible for payment of personal calls and/or data usage.
- Users will be required to sign an automatic payment via payroll for at minimum the sum of $10 per fortnight to cover reasonable personal usage.
- Any personal usage that is identified as excessive and/or exceeds the $10.00 minimum coverage charge will be reimbursed to Waikato DHB.
- Where appropriate data caps will be applied by Information Services to manage costs and usage.

5.2 Monitoring

- All mobile communication devices issued by the Waikato DHB will be subject to monitoring and periodic audit.
- Location and usage information, texts & call logs for any device used for DHB purposes, may be requested in the event of a legal discovery process, complaints processes, or Official Information Act (OIA) request.
- Any mobile communications device used for DHB purposes may be monitored in order to identify usage patterns and as necessary to address excessive or unacceptable use and to optimise spend and identify devices that may have been compromised.
- Monitoring of an employee's use of a mobile communication device must be carried out by Information Systems and/or its contracted providers.
- Managers must request monitoring via a written request in writing to the Waikato DHB HR department.
- The request must set out in detail the reasons for the employee's mobile device use to be monitored, including grounds for suspecting unacceptable use and any other steps (short of monitoring) which can be taken to address the manager's concerns.
- Monitoring and/or auditing devices may include accessing of personal data stored on the phone.

5.3 Major telecommunications failure

- In the event of a major communications failure of either the hospital phone system or the public telephone network, restrictions on staff use of mobile communication devices may be lifted for the duration of the emergency. The hazard of a general communication blackout is considered to pose a greater threat to patient safety than that associated with cellular phone or radio device use close to susceptible medical electronic equipment.
- Mobile communication devices may be recalled from staff for redistribution in the event of an emergency.

5.4 Security of information, networks and systems

- Access to the Waikato DHB's network and information assets and resources for mobile communication devices is allocated at the DHB's discretion and as such reserves the right to restrict, prevent or remove this access at any time.
- Confidential and/or sensitive information must not be stored or used on mobile devices unless using Waikato DHB provided or approved applications.
- Using mobile device's storage or applications (such as Dropbox, Evernote, iCloud, SkyDrive, Drop.net) to store this information is unsafe and may breach public records and privacy legislation and must not be used to store sensitive data and/or patient information.
- The Waikato DHB reserves the right to remove all DHB information and access from any mobile communications device and to monitor and inspect any mobile communications device for the purpose of usage and security compliance.
- Any attempt to contravene or bypass security controls on mobile communications devices will be treated as a security breach and may result in disciplinary action.

5.5 Software and Applications

- The Waikato DHB reserves the right to have visibility of all applications installed on any mobile communications device and will provide and remove any software or applications (and related licensing) required for DHB purposes at its discretion.
- Where authorised to access an iTunes account the user will ensure a complex iTunes User Name and Password is maintained, will not load, store or distribute copyrighted material or install applications other than those authorised by the Waikato DHB.
- Employees are responsible for purchasing and paying for any other application(s) or content that employees choose to use.
- The Waikato DHB will maintain a list of "Blacklisted" applications that are prohibited on any mobile communications device.
- The use of pirated software on any mobile communications device is illegal and is explicitly prohibited.
- Employees must not make unsanctioned physical modifications nor modify the software (e.g. replacing / overriding, "jailbreaking" or "rooting") to any mobile communications device.

5.6 Patient Information

- Mobile communications devices can be used to access and process patient identifiable information which may be confidential or sensitive in nature. All access to and/or use of patient information must be consistent with all security and privacy standards and in compliance with supporting policies.

- Mobile devices must not be used to record images, video or audio of staff, patients or visitors without an appropriate medical and/or business reason and informed consent.
- The consent for recording images, video or audio of a patient in the course of their treatment must be documented in the patient's record. The recordings may not be used, stored or shared for any purpose other than as appropriate for a medical record.
- Staff who record images, video or audio of patients for clinical purposes must ensure that:
  - Adequate steps are taken to accurately identify the patient to whom the recording relates.
  - The recording is placed on the patient's record through the most secure method available.
  - The recording is deleted from the mobile device immediately after being placed on the patient's record.
  - The recording may not be stored on an unencrypted portable storage device.

5.7 Patient Safety

- Areas where mobile communication devices may affect patient safety must be identified and a risk reduction exercise completed; e.g., clearly signposted as a restricted and/or at risk area (particularly for patients and visitors).
- All high risk devices (i.e. those devices that have been shown to be affected by mobile electronic devices such as Ventilators, dialysis equipment, IV infusion pumps, etc. must be labelled.
- Walkie-Talkie devices must not be switched on or used within eight metres of electronic medical equipment.
- Mobile communication devices must not be operated in areas identified as high risk and care should be taken at all times when operating devices in proximity to medical devices. If in doubt check with either the Bio Medical team or the applicable clinical service manager.
- Visitors/patients shall not use mobile devices in areas identified as cell phone restricted areas.

6. Potential Complications

- Non-compliance
- Additional regulatory requirements
- 'Shadow IT' and non IS Managed assets
- 'BYOD' devices

7. Audit

The Policy and any supporting protocol(s) will be subject to audit as part of;

- Annual ICT Audit Program (ICT Controls and Security Assessment Audits)
- Annual NZ Audit ICT Controls Audit
- IS Operational Assurance Framework

8. Legislative Requirements

- Health Act (1956)
- Health and Safety at Work Act 2015
- Human Rights Act 1993
- Privacy Act (1993)
- Employment Relations Act 2000
- Treaty of Waitangi Act 1992.
- Official Information Act (1982)
- IS Call Management System

9. References

- Health Information Security Framework (HISO 10029.1)
- New Zealand Information Security Manual (NZISM, December 2017)
- Health Information Privacy Code (1994, as amended)
- Security in the Government Sector (2002)
- AS/NZS2500:2004: Guide to the safe use of electricity in patient care.
- AS/NZS 3200.1.0.1998: Medical electrical equipment-General requirements for safety-Parent Standard
- AS/NZS 3200.2.2:2005: Medical electrical equipment-General requirements for safety-Collateral standard: Electromagnetic compatibility-Requirements and tests.
- AS/NZS 3551:2004: Technical management programs for medical devices.

10. Associated Documents

- Waikato DHB Acceptable Use of Information Systems policy (Ref. 2191)
- Waikato DHB Clinical Records Management policy (Ref. 0182)
- Waikato DHB Corporate Records Management policy (Ref. 0905)
- Waikato DHB Intellectual Property policy (Ref. 1036)
- Waikato DHB Definitions – Information Services protocol (Ref. 5799)
- Waikato DHB Information Privacy policy (Ref. 1976)
- Waikato DHB Information Security policy (Ref. 3153)
- Waikato DHB Managing Behaviour and Performance policy (Ref. 5250)
- Waikato DHB Non-Employee Engagement policy (Ref. 1042)
- Waikato DHB Media and Communications policy (Ref. 1816)
- Waikato DHB Vehicle Usage and Safe Driving policy (Ref. 0112)
- Waikato DHB Visiting Patients at Waikato DHB Facilities guideline (Ref. 0125)

Information Services Acceptable Use Policy

Policy Responsibilities and Authorisation

Department Responsible for Policy	Information Services
Document Facilitator Title	Information Security Manager
Document Facilitator Name	Suranwan Wickramasuriya
Document Owner Title	Executive Director Corporate Services
Document Owner Name	Maureen Chrystall
Target Audience	All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB (collectively referred to as “Users” in this Policy).
Committee Approved	Policies and Guidelines Committee
Date Approved	24 May 2018
Committee Endorsed	Executive Group
Date Endorsed	6 July 2018
Disclaimer: This document has been developed by Waikato District Health Board specifically for its own use. Use of this document and any reliance on the information contained therein by any third party is at their own risk and Waikato District Health Board assumes no responsibility whatsoever.	

Policy Review History

Version	Updated by	Date Updated	Summary of Changes
3.0	S. Honig	20/04/2015	Current Published Policy
3.1	S. Wickramasuriya	30/05/2017	Redraft into new format with HISF changes included
3.2	Tony Haigh	14/03/2018	Add links, standard format, distribution copy for review
4	Jeremy Marshall	10/05/2018	Amend following Consultation and feedback
4.1	Jeremy Marshall	21/11/2018	Add policy position on data caps

Information Services Acceptable Use Policy

Contents

Information Services Acceptable Use Policy

1. Introduction

1.1 Purpose

The purpose of this policy is to maintain a secure computing environment and to protect Waikato District Health Board (Waikato DHB) information assets and resources against unauthorised access or use and should be read in conjunction with the Information Security Policy (3153) and supporting protocols.

1.2 Background

Under the Health Information Security Framework (HISF) healthcare organisations must have an information security policy to meet the needs of their organisation and an 'acceptable use policy' for any organisation technology equipment, systems, resources and data.

1.3 Scope

This policy applies to:

All Waikato DHB employees, board members, contractors, consultants, temporary staff, personnel affiliated with third parties providing services to Waikato DHB (collectively referred to as "Users" in this Policy).

The policy recognises the Waikato DHB Director of Information Services as the Chief Information Officer (CIO) and Chief Information Security Officer (CISO).

Additional areas within information security and acceptable use are supported by the following policies:

Information Security: A separate policy 'Information Security policy' covers application, management and control of Information Security within the Waikato.

Change Management: A separate policy 'Information Communications Technology (ICT): Change Management' establishes the Waikato District Health Board's (Waikato DHB) requirements for managing change to its Information Communications Technology (ICT) environment

Mobile Communications Devices: The 'Mobile Communications Devices policy' covers the use of Waikato DHB's mobile technology equipment.

Social Media and the Internet/Intranet: Use of social media and the internet/intranet are covered by the 'Media and Communications policy'.

Intellectual Property: The 'Intellectual Property policy' covers the ownership of intellectual property created by an employee in the course of their employment.

Patient Data Privacy and Confidentiality: Matters relating to patient data privacy and confidentiality are managed under the conveyance of the Waikato DHB's Privacy Office in accordance with the 'Information Privacy policy'.

Physical Security: Matters relating to physical security are additionally managed by the Property and Infrastructure service in accordance with the Property and Infrastructure 'Security policy'.

Clinical Records: Clinical Records Management is subject to the 'Clinical Records Management policy'.

Corporate Records: Corporate Records Management is subject to the 'Corporate Records Management policy'.

Risk Management: Management of Waikato DHB risk is subject to the 'Risk Management policy'.

1.4 Exceptions

Any exceptions to this policy and/or supporting protocols must be initiated by a request to the Information Services 'Service Desk', be subject to a security risk assessment and authorisation by the CISO and Information Security Manager.

2. Definitions

Refer to the Definitions – Information Services protocol (Ref. 5799).

3. Policy Statements

The Waikato DHB policy for Information Systems Acceptable Use is that:

- Waikato DHB's information assets and resources are provided for authorised users to carry out their responsibilities and perform their day-to-day duties.
- Usage must not contravene Waikato DHB policies nor breach the security of Waikato DHB or any organisation external to Waikato DHB.
- All usage of Waikato DHB's information assets and resources must be carried out in consideration of patient data privacy and ensure the confidentiality, integrity and availability of Waikato DHB information and data.
- Information Services will establish and publish operational controls and performance and usage caps as required to safeguard the DHB's operational and financial position.

4. Roles and Responsibilities

Every employee, consultant or contractor in the health and disability sector has responsibility to take all reasonable precautions to protect the security of all sites, services, systems and information assets and resources.

- **Chief Executive Officer (CEO)** - Overall accountability for the operations of the Waikato DHB ensuring information protection and assurance activities are funded and supported to meet the Waikato DHB's objectives.
- **Chief Information Security Officer (CISO)** - Responsible for managing the security strategy, endorsing the supporting security policies and control measures and ensuring adequate funding and resources are available to achieve objectives.
- **Information Security Manager (ISM)** - Acts as a conduit between strategic directions from the CISO and their implementation. Maintaining the management, administrative and process controls relating to organisational information security. The Information Security Manager will

maintain the Information Security Risk Register and will advise the Security Governance Group and Board on the status, risks, issues and breaches related to information security.

- **Information Services** - Responsible for maintaining and advising the organisations IS Security Policies and ensuring all required controls, protocols, procedures and processes are in place to protect and control the use of information assets and resources and that all employees, partners and suppliers are aware of policy and are kept informed of any changes and updates.
- **Managers and Business Owners** - Responsible for ensuring that information security has been adequately addressed during the design, development and implementation or operation of any existing, new or altered information systems and that staff are aware of their security responsibilities and adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.
- **Users** - Complying with information security policies and protocols and reporting any information security weaknesses, breaches or violations to Information Services. All users of Waikato DHB information assets and resources are responsible for exercising good judgment regarding appropriate use in accordance with both Waikato DHB policies and standards, and local laws and regulations.

4.1 Acceptable Use

- The Waikato DHB's information assets and resources must only be used as part of the normal execution of a user's responsibilities and in a manner that is consistent with the Waikato DHB's values, standards of conduct and policies.
- All incidents and/or requests relating to Waikato DHB Information assets and resources must be logged through the IS Service Desk.

4.2 Unacceptable Use

Other than for properly authorised and lawful healthcare work or research users must not use Waikato DHB's information assets and resources for inappropriate or unacceptable purposes including but not limited to:

- To intentionally create, hold, transmit or view material that has an obscene, pornographic, sexually offensive, racist, sexist, homophobic or otherwise inappropriate content.
- For any purpose that conflicts with policies/procedures and contractual obligations to the Waikato DHB.
- To conduct private or freelance work for the purpose of commercial and/or personal gain.
- To intentionally use, create, hold, transmit or view material that is abusive, defamatory, bullying, harassing or otherwise illegal.
- To make untrue, inaccurate, misleading or offensive statements about any person or organisation.
- To download or install any unauthorised software or hardware or interfere with device management or security system software including, but not limited to, anti-virus tools.

- To access information and/or data they are not entitled to access or use as part of their normal responsibility.
- To contravene software licensing agreements, copyright laws and other applicable regulations.
- Undertake activities and usage that would damage the Waikato DHB's reputation and/or are in conflict with the organisations values and culture.
- Undertake activities and usage that would threaten the security and privacy of Waikato DHB systems and the sensitive information and data they hold.

5. User Accounts

- Access to Waikato DHB information assets and resources is granted to users who have signed a Waikato DHB confidentiality agreement.
- It is expected that managers will ensure all new 'users' complete the Waikato DHB's security training programme.
- Accounts are created appropriate to a user's needs and must be authorised by the employee's immediate line manager.
- Account details, including passwords, are for the sole use of the identified account holder and must be secured at all times.
- Employees must not share account details and passwords, nor attempt to obtain or use another employee's account details, passwords, user identification or other secure information.

5.1 Account Auto-Login Profiles

- Auto-Login profiles are created for specific work groups or departments that require an automated login for shared access.
- Auto-Login accounts are for the sole use of the specified group or department and provide access to a controlled set of network services only.
- Users with access to an Auto-Login profile must have a corresponding individual user account that is used to access all applications, email and Internet resources.
- Each Auto-Login profile must have an identified business owner who is accountable for its use, confidentiality and security.

5.2 Passwords

- Passwords are created to ensure secure and controlled access to information assets and must be secured by users.
- Passwords must be changed every 90 days.
- Password length is required to be 8-32 characters, using a combination of case-sensitive alphanumeric characters (a-z, A-Z, 0-9) and special characters (! $ % #).
- Passwords should not contain personally identifiable information.

- Passwords standards for mobile devices are covered in the 'Mobile Communications Devices policy'.

5.3 Removal of Logins for Terminated Employees

- Managers must advise the IS Service desk when an employee either ceases their employment with the Waikato DHB and/or transfers within the Waikato DHB so that account details and changes can be managed appropriately.
- All user access will be disabled upon line management notification to the IS Service desk of a staff suspension or cessation of employment.
- Managers may liaise with the IS Service desk for temporary arrangements to cover handovers, email and file transfers.
- Logins, stored email and personal directories will be disabled and data deleted in accordance with Corporate Records guidelines.

6. Clear Desk Policy

- The Waikato DHB has a clear desk policy for papers and removable storage media and a clear screen policy in order to reduce the risks of unauthorised access to, loss of, and damage to information during and outside normal working hours.

7. Computer Equipment

- Users are responsible for the protection and care of all computer equipment allocated to them and all reasonable precautions should be taken to protect and secure computer equipment
- No 'ICT' dependant equipment is to be purchased or modified without the approval of Information Services and completion of appropriate planning and risk assessment activities.
- Hardware or storage media containing Waikato DHB data or applications must be securely erased and disposed of when no longer required.

8. Software Procurement and Installation

- All software remains the property of Waikato DHB and only IS-authorised and legally licensed and approved software can be installed on Waikato DHB computer systems.

9. Waikato DHB Network

- No equipment is to be connected, removed or modified on any Waikato DHB network without the approval of Information Services and completion of appropriate planning and risk assessment activities.
- All Third Party access must be authorised and managed by Waikato DHB's Information Services department, be subject to a legally binding contractual agreement and identifiable and authenticated password management must comply with the Waikato DHB's password and access standards.

10. Information and Data

- All Waikato DHB information and data remains the property of the Waikato DHB, must be accessed and stored by approved equipment, applications, storage devices and locations.
- Information and data must be used for the sole purpose of its creation and in relation to a user's job responsibilities.
- Personal devices may only access the Waikato DHB networks and data through approved technology gateways or as part of an authorised BYOD (Bring Your Own Device) plan. Users must not store Waikato DHB data or information on personal devices or personal removable media.
- Waikato DHB may be required to disclose information and data contained in file systems (including, but not limited to, files, folders, drives, group shared areas, logs and backups) to law enforcement and regulatory agencies in compliance with legal and regulatory requirements.
- The use of external file transfer systems to enable the communication of information and data is permitted only if authorised by Waikato DHB's Information Services department and when approved file transfer systems are used.
- Use of "cloud storage" mechanisms to transfer or store Waikato DHB information and data is not permitted except where approved cloud storage mechanisms are used and where the Waikato DHB and Ministry of Health risk assessments have been completed and approved.

11. Malware

- Users must not attempt to alter or disable anti-virus software installed on any information asset or resource attached to the Waikato DHB network nor attempt to destroy or remove a virus, or any evidence of a virus.
- Managers should ensure staff are aware of their security responsibilities and are adequately trained and equipped to carry out their roles in compliance with Waikato DHB security policies and protocols.
- Users should take appropriate measures to protect against virus infection including not opening any files or links attached to emails from an unknown, suspicious or untrustworthy source.
- Users should ensure that any personally-owned computers that connect to the DHB network have virus protection software installed that is in keeping with the standards set out in this policy.
- Users must advise any Anti-Virus incidents and/or risks and concerns to the IS Service Desk.

12. Email and Instant Messaging

- Email and Instant Messaging (IM) accounts will be provided to non-Waikato DHB employees (third parties) only under agreed circumstances where authorised by Information Services.
- Email and IM access will be disabled when an employee leaves the organisation and the Waikato DHB will be under no obligation to store or forward the contents of an individual's email inbox / outbox after their employment has ceased.
- Access to another employee's mailbox may be granted if approved by the Service Manager and required for business continuity purposes.
- Users must ensure that emails and/or instant messages containing sensitive data or health information are encrypted and marked as **[IN-CONFIDENCE]** within the email or IM body.
- Non Waikato DHB email and/or IM services must not be used for the sending or receiving of sensitive data and/or health information.
- External email/webmail systems such as Gmail, Yahoo! and Hotmail are blocked and may not be used within the Waikato DHB.
- Users must not use the Waikato DHB email or IM system to send harassing or objectionable email or unsolicited (SPAM) email or use email in any way that contravenes Waikato DHB policies.
- Synchronised email and IM onto mobile communication devices is permitted where the device is approved and where the device is managed by the Waikato DHB security toolset.

13. Audio and Video conferencing

- Users may have access to the audio and video conferencing as part of the normal execution of their employment responsibilities.

14. Intranet

- Use of the Waikato DHB intranet is subject to the Media and Communications policy and streaming of business-related media (video and audio) is permitted providing this meets technology standards and does not disrupt other critical services.

15. Internet

- Staff use of the Internet that supports the goals and objectives of the Waikato DHB is permitted and should be used in a manner that is consistent with the Waikato DHB's policies and standards of conduct.
- Streaming of business-related media (video and audio) is permitted providing this meets technology standards and does not disrupt other critical services.
- Web sites are blocked where they present a security risk or are assessed to be inappropriate.
- Access to blocked sites will require a request to 'whitelist' though the IS Service Desk and will be subject to a risk review and authorisation by the Information Security Manager.

16. Mobile Devices

- Where a mobile communication device connection and / or access to Waikato DHB information assets and resources have been provided to an employee, it is subject to the Mobile Communication Devices policy.

17. Removable Media

- Removable media applies to any external memory device that can store data including, but not limited to, USB-based memory sticks, memory cards, USB card readers, portable disk drives, portable media players, DVDs and CDs and must not be used on Waikato DHB network unless the device is approved by Information Services and is encrypted.
- Removable media that requires a password for encryption must be secured with a minimum password length of 8 characters, using a combination of case-sensitive alphanumeric characters (a-z, A-Z, 0-9) and special characters (! $ % #).
- Waikato DHB data may only be transferred to removable media upon appropriate management approval, subject to the provisions of this policy and the Information Security Policy (3154).
- All removable media must be malware checked before use on Waikato DHB information systems.

18. Monitoring and Disclosing

- Waikato DHB may be required to disclose information to law enforcement and regulatory agencies in compliance with legal and regulatory requirements or as part of an Official Information Act request.
- Information Services will audit, monitor and report usage and initiate appropriate action in response to operational requirements and/or breaches of policy.
- Monitoring and/or auditing devices may include accessing of personal data stored on the device.
- If a manager wishes to initiate a monitoring or usage activity request they must make a written request to their Human Resource Consultant setting out in detail the reasons for the monitoring, including grounds for suspecting unacceptable use or inappropriate behaviour.
- The Human Resource Consultant will coordinate monitoring activity via the IS Service Desk coordinators who will manage the request in consultation with relevant IS Service Managers.
- The Human Resource Consultant will consult with the Privacy Officer (if advice on privacy or legal issues is required) and Information Security Manager (if advice on information security is required).
- The Waikato DHB will comply with its privacy obligations and its obligations as an employer and action taken will be in accordance with Waikato DHB's Performance Management and Discipline Policy (5250).

19. Audit

The Policy and supporting protocol will be subject to audit as part of;

- The Internal Audit annual ICT Audit Program.
- Annual NZ Audit Controls Audit.
- IS Operational Assurance Framework.

20. References

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- Health Information Security Framework (HISO 10029.1)
- New Zealand Information Security Manual (NZISM, December 2014)
- Health Information Privacy Code (1994, as amended)
- Security in the Government Sector (2002)

21. Associated Documents

- Waikato DHB Clinical Records Management policy (Ref. 0182)
- Waikato DHB Corporate Records Management policy (Ref. 0905)
- Waikato DHB Risk Management policy (Ref. 0118)
- Waikato DHB Information Communications Technology (ICT): Change Management policy (Ref. 2744)
- Waikato DHB Information Privacy policy (Ref. 1976)
- Waikato DHB Intellectual Property policy (Ref. 1036)
- Waikato DHB Media and Communications policy (Ref. 1816)
- Waikato DHB Mobile Communications Devices policy (Ref. 1853)
- Waikato DHB Security policy (Ref. 0120)
- Waikato DHB Definitions – Information Services protocol (Ref. 5799)