THE UNIVERSITY OF
WAIKATO
Te Whare Wānanga o Waikato

Information Security Standards

Aligned With: NZISM & ISO/IEC 27002

Version 1.2

Title	Information Security Standards Framework
Subtitle	Aligned With: NZISM & ISO/IEC 27002
V1.0 Author	Shahn Harris– Lateral Security (IBM sub-contractor) and Dougal Mair – ITS
Contributors	Andrew Evans – Lateral Security, Dougal Mair – ITS, Milton Markose – ITS
Date	22 March 2016
Requested By	Dougal Mair
Reviewed By	The Information Security Forum (ISF), the ICT Managers Advisory Forum (IMAF) and the ICT Committee.
Document Version	V1.2

Revision History

Version	Date	Description/Notes	Author(s)
0.1 DRAFT	01/12/2012	'Information Security Policy' created	Shahn Harris (Lateral Security)
0.2 Draft	27/12/2012	Review/Minor adjustments	Shahn Harris (Lateral Security)
0.3 Draft	31/12/2012	Final Review	Andrew Evans (Lateral Security)
0.4 Draft	29/05/2013	Updated with UoW context and simplified the document layout (removed duplicate controls) for clarity.	Dougal Mair (ITS)
0.5 Draft	24/06/2013	Change from "Policy" to "Standards Framework" in that this document is the framework and standards supporting the University's Information Security Policy.	Dougal Mair (ITS)
0.6 Draft	22/07/2013	Merged separate standards documents into this document.	Milton Markose (ITS) and reviewed by Dougal Mair
0.7 & 0.8 Draft	29/07/2013	Review by IMAF Working Group and then endorsed by IMAF (19/9/2013)	Various
0.9 Draft	13/09/2013	Amended Human Resource Security section	K Adamson, C Gunn
0.10 Draft	17/09/2013	Proof Read and Minor Formatting Changes	Rachel Prasad
1.0 Final	27/09/2013	Endorsed by the ICT Committee, so finalised for release.	Dougal Mair
1.1 Update	15/08/2014	Updated Password standard 7.2.3, after endorsed by ICTC and IMAF	Dougal Mair
1.2 Draft	13/01/2016	Annual review completed by ISF	ISF (Dougal Mair – editor)
1.2 Final	22/03/2016	Endorsed for adoption by IMAF and ICTC	Dougal Mair

Related Documents

- The University of Waikato Information Security Policy (Computer Systems Regulations 2005)
- `Information Technology - Security Techniques - Code of Practice for Information Security Management' [ISO/IEC 27002]
- `New Zealand Information Security Manual v2.3 – May 2015 - New Zealand Government Communication Security Bureau` [NZISM]

Tables

Introduction

Information is an asset that, like other important business assets, is essential to the University of Waikato's business and consequently needs to be suitably protected. This is especially important in today's increasingly interconnected business environment. As a result of this increasing interconnectivity, information is now exposed to a growing number and a wider variety of threats and vulnerabilities.

Information can exist in many forms - it can be printed or written on paper, stored electronically, transmitted by post or electronic means, or spoken in conversation. Whatever form information takes - or whatever means it is shared or stored - it must always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimise business risk - and maximise return on investment and business opportunities. It is best achieved by implementing a suitable set of controls - including policies, standards, processes, procedures, organisational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved (when necessary), to ensure that the specific security and business objectives of the University of Waikato are met.

Obviously this cannot be done in isolation - but must be done in conjunction with other established business management processes.

Why is Information Security Important?

Information and the supporting processes, systems, and networks are important business assets, and defining, achieving, maintaining - and improving - information security is essential when seeking to maintain the University of Waikato's competitive edge, legal compliance, and corporate image.

Information security must function as an enabler, and seek to avoid or reduce relevant risks. The interconnection of public and private networks and the sharing of information resources increase the difficulty of achieving access control.

Many information systems have simply not been designed to be secure - and what security can be achieved through technical means is limited. Therefore, such systems must be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires - as a minimum - participation by all staff in the University of Waikato. It may also require participation from suppliers, third parties, customers or other external parties. Specialist advice from outside organisations may also be needed.

Selecting Controls

Once security requirements and risks have been identified - and decisions for the treatment of risks have been made - appropriate controls should be selected and implemented to ensure risks are reduced to an acceptable level.

ISO/IEC 27002

ISO/IEC 27002 is an internationally-recognised security standard of practice and includes a comprehensive list of security practices that can be applied - in varying degrees - to all organisations.

NZISM

Aimed primarily at New Zealand government organisations, the New Zealand Information Security Manual (NZISM) provides up-to-date technical policy to assist in securing information systems and the data stored in those systems. It is considered the best practice guide for information assurance within New Zealand.

Scope

The University Of Waikato Information Security Policy (Computer Systems Regulations 2005) and supporting standards framework (this document) establishes principles for initiating, implementing, maintaining, and improving Information security management in the University of Waikato.

This document serves as a practical framework for setting the University of Waikato Information Security Standards and effective security management practices - and to help build confidence in our business activities.

Structure of this Standards Framework

This framework document supports the University's Information Security Policy and contains the 11 security control clauses carried over from ISO/IEC 27002 and includes the standards in support of each clause.

Note: The order of the clauses in this document does not imply their importance. Some controls are relevant to more than one clause, however for clarity each control has been attributed to the most appropriate clause – rather than duplicating controls throughout the document.

1. Security Policy

1.1 Information Security Policy

A strong Computer Systems Regulations policy sets the security tone for the University of Waikato and informs staff what is expected of them. All staff should be aware of the sensitivity of the University of Waikato data and systems - and their responsibilities for protecting them.

1.1.1 The Computer System Regulations

- The University Of Waikato must:
  - Establish and maintain the Computer Systems regulations that fully address all information security requirements.
  - Ensure the Information Security Standards clearly define the information security responsibilities for all staff (including contractors).

1.1.2 Review of the Computer Systems Regulations and Security Standards

- The Computer Systems Regulations, and security standards, must be reviewed annually, or if significant changes occur to any relevant systems.
- This Computer System Regulations and security standards review must take into account any identified threats and vulnerabilities, and must result in a formal risk assessment being undertaken.

2. The Organisation of Security

2.1 Internal Security Organisation

To manage Information Security within the University of Waikato, the Computer Systems Regulations and Security Standards should initiate - and control - the implementation of information security.

2.1.1 Information Security Co-Ordination

The responsibility for information security management must be assigned to a specific individual[1] or team within the University of Waikato.

2.1.2 Information Security Activities

- Responsibility for the following information security activities must be assigned individuals and teams within The University of Waikato (refer to Information Security responsibility matrix in Appendix A):
  - Administering user accounts;
  - Establishing processes to identify newly discovered security vulnerabilities, assigning risk ratings, and updating information security standards to address these;
  - Implementing assessment trails for all system components;
  - Monitoring and analysing security alerts and information;
  - Using up-to-date network intrusion prevention systems (IPS) to monitor all network traffic;
  - Deploying file integrity monitoring software;
  - Managing and controlling all data access
  - Establishing and distributing an incident response plan.
- Overall management and authority for these activities remains the responsibility of the Manager, ICT Infrastructure.

2.1.3 On-going Information Security Activities

- This individual's or teams on-going activities include:

1. Weekly:
   a. Configuring file integrity monitoring software to perform critical file comparisons

2. Quarterly:
   a. Running internal and external network vulnerability scans (also after any significant changes in the network)

[1] Typically an 'Information Security Manager' or equivalent

3. Annually:
   a. Performing penetration testing (also after any significant infrastructure or application upgrade or modification)
   b. Reviewing security controls, limitations, system and network connections, and restrictions

2.1.3.1 Information Security Activity Scheduling

- The University of Waikato must identify and document all information security activities for completion.
- For each task, the following should be identified and documented:
  - Description
  - Responsible Role/Team
  - Frequency (Daily, Weekly, Monthly, Annually)
- The University of Waikato must schedule and record the completion of all information security activities.
- Any failure to complete information security activities must be recorded and escalated to the Manager, ICT Infrastructure.

2.1.3.2 Non-scheduled Information Security Activities

- Additional information security activities and reviews may be required to support significant projects, incidents or systems change.
- Such activities must be scheduled and documented.
- The requirement for ad-hoc/project based information security activities must be scheduled to avoid conflict with business-as-usual activities.
- Where business-as-usual activities are impacted by ad-hoc/project activities, this impact must be escalated to the Manager, ICT Infrastructure.

2.1.4 Information Security Risk Management

2.1.4.1 The Risk Register

- The University of Waikato must create a risk register to catalogue all Information Security risks faced by the organisation
- Each risk must be assessed in terms of the following:
  - Name
  - Description
  - Threat Posed
  - Impact
  - Vulnerability

  - Risk Rating (Low, Medium, High, Critical)
  - Risk Owner

- Every risk identified by The University of Waikato must be assigned a risk owner.
- The University of Waikato risk owner is responsible for the management and mitigation of that risk.
- The University of Waikato risk owner is responsible for ensuring that the risk register entry for this risk remains up to date.

2.1.4.2 Review and Update of Risk Register

- The University of Waikato must review the contents of their Information Security risk register on a quarterly basis.
- During the review process any changes to The University of Waikato or its operating environment must be reflected in the risk register.

2.1.5 The Authorisation Process for Information Processing Systems

- An appropriate management authorisation process for new systems must be defined and implemented. This to include:
  - Establishing a formal process for approving all external network connections and changes to network configuration for new systems.
  - Establishing a formal process for checking the security, and compatibility with existing systems, for new systems before released.
  - Following release and change management procedures for all system and software configuration changes (to include appropriate management approval).

2.1.6 Contractual Requirements

- If Restricted Data is shared with a service provider, then contractually the service provider must conform with the University of Waikato's information security requirements.
- When considering a contract with service providers, the following elements must be considered:
  - Strict control must be maintained over the internal or external distribution of any kind of media that contains Restricted Data - with all such media being classified as 'Confidential'
  - Electronic transmission of Restricted Data between external service providers and the University of Waikato must be via encrypted connections.
  - The service provider must acknowledge that they are responsible for the security of Restricted Data they possess.

2.1.7 Incidents and Contact with External Authorities

- The incident response plan must address communication and contact strategies around informing the required external authorities and organisations of any breach.

2.1.8 Review of Information Security

- The University Of Waikato must include security review in all projects and changes. This includes regular update and maintenance activities such as patching.

2.2 Identifying and Addressing Risks Related to Third Parties

The University Of Waikato management seeks to maintain the security of their Restricted Data and systems whenever these are accessed, processed or managed by third parties. Therefore the risks to the University of Waikato's data and systems from third parties must be quantified - and appropriate controls implemented - before access is granted.

2.2.1 Service Delivery

2.2.1.1 Adherence to the University of Waikato Information Security Policy and Standards

- If Restricted Data is shared with service providers then the contractual requirements in 2.1.6 above apply.
- All third party processors and service providers must maintain and implement policies and procedures to manage connected entities, including the following:
  - Maintain a list of connected entities;
  - Ensure proper due diligence is conducted prior to connecting an entity
  - Only connect and disconnect entities by following an established process.

2.2.1.2 Data Sharing

- When considering a contract with service providers, the following elements must be considered:
  - If Restricted Data is shared with service providers then the contractual requirements in 2.1.6 above apply.
- The University of Waikato must maintain a record of all restricted information shared with service providers including the following:
  - Date shared
  - Information Classification
  - Data Custodian
  - Purpose

2.2.1.3 Incident Response, Business Continuity and Disaster Recovery

- The University of Waikato must include incident response times, responsibilities and contact strategies in all agreements with third parties.

- The University of Waikato must ensure that all third parties have the following documented policies, standards and procedures:
    - Business Continuity
    - Disaster Recovery
    - Incident Response
- The University of Waikato must ensure that in the case of an incident, emergency or disaster any engaged third party will respond in such a way as to:
    - Maintain the confidentiality, integrity and security of The University of Waikato information.
    - Protect The University of Waikato information and systems from additional risk.
    - Protect the privacy and reputation of The University of Waikato and its affiliates.
- The University of Waikato must ensure that incident response, business continuity and disaster recovery are included in third party service level agreements.

2.2.1.4 Right to Audit

- The University of Waikato must ensure that the 'right to audit' (a periodic review of the service provider's security controls) is included in every commercial service agreement.
- The 'right to audit' must extend to a minimum of the following activities:
    - Penetration Testing (checking that the service provider does periodic testing)
    - Vulnerability Assessment (checking that the service provider assesses and addresses vulnerabilities on an ongoing basis)
    - Configuration Review (checking that the service provider's security controls are still appropriate and reviewing any changes that have been made)
    - Information Security Audit (checking that the service provider does regular audits)
    - Physical Review (Premises, Data centres), if there have been changes

2.2.1.5 Service Levels and Information Security

- The University of Waikato must review the service levels provided by service providers on an annual basis to ensure that all obligations have been met.
- The University of Waikato must include information security objectives in service provider service level reviews.
- The University of Waikato must reserve the right to amend, terminate or otherwise renegotiate all agreements with third parties based on reviews.

2.2.2 Establish Firewall Configuration Standards

- Firewall configuration standards must include:
    - The documentation of services and ports, and other network access controls required for third parties to obtain access to only the systems and data they need in order to provide service to and/or transact with the University.

3. Asset Management

3.1 Responsibility for the University of Waikato's Assets

3.1.1 The Asset Inventory

3.1.1.1 Creation and Maintenance

- The University of Waikato must maintain an inventory of all server, storage, and PC assets and mobile devices which have Restricted Data. The Asset Inventory must contain all removable media (see glossary) used for the storage of information classified as Restricted.

3.1.2 Securing the Asset Lifecycle

3.1.2.1 Acquisition

- The University of Waikato must ensure that all ICT assets are recorded in the asset inventory system.
- The asset inventory must contain a minimum of the following for each item listed:
  - Asset ID
  - Classification
  - Name
  - Make/Manufacturer
  - Acquisition Date
  - Acquisition Source
  - Serial Number (or other unique identifier)
  - Delivery Location
  - Service/Warranty Details
  - Purchasing Department or Cost Centre
  - Restricted Data details (if it's purpose is for use with Restricted Data)
  - Asset Owner (University of Waikato staff member responsible for the asset)
- All end-user devices should have as a minimum password/pin protection and remote wiping enabled via the University's Device Management system.

3.1.2.2 Labelling and Classification

- All The University of Waikato inventoried assets must be labelled.
- Asset labels must include at a minimum the Asset Identification number.
- Asset labels must link a physical asset to an entry in The University of Waikato asset inventory.

3.1.2.3 Storage

- In the case of media or devices containing media, this must take into account the requirements enforced by the University of Waikato media handling standard (see section 6.7), physical security standard (see section 5) and information classification standard (see section 3.2).

3.1.2.4 Transfer and Change of Ownership

- The University of Waikato must record any change or transfer of asset ownership in the asset inventory for Data Systems (servers & storage) and computers holding Restricted data.

3.1.2.5 Transportation

- Where assets contain Restricted Data, transportation must be conducted in accordance with the University of Waikato Media Handling Standard (see section 6.7).

3.1.2.6 Disposal

- All assets that have been approved for disposal must be recorded as such in the University of Waikato asset inventory.
- Where assets containing Restricted Data, destruction and disposal must be conducted in accordance with the University of Waikato Media Handling Standard (see Section 6.7).
- All assets must be disposed of through an approved disposal channel.

3.2 Acceptable Use of Assets

Staff must adhere to the Computer Systems Regulations 2005.

3.3 The University Of Waikato Information Classification

To ensure the University of Waikato's data receives an appropriate level of protection, it must be classified in order to indicate the need, priorities, and expected degree of protection required.

3.3.1 Information Classification

- The University must establish a framework for classifying institutional data based on its level of sensitivity, value and criticality. Classification of data will aid in determining baseline security controls for the protection of data.
- Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels, or classifications:
    - *Restricted Data* - Data should be classified as Restricted when the unauthorised disclosure, alteration or destruction of that data could cause a significant level of risk to the University or its affiliates. Examples of Restricted data include data protected by government privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to Restricted Data.

- *Private Data* - Data should be classified as Private when the unauthorised disclosure, alteration or destruction of that data could result in a moderate level of risk to the University or its affiliates. By default, all Institutional Data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

- *Public Data* - Data should be classified as Public when the unauthorised disclosure, alteration or destruction of that data would results in little or no risk to the University and its affiliates. Examples of Public data include press releases, course information and research publications. While little or no controls are required to protect the confidentiality of Public data, some level of control is required to prevent unauthorized modification or destruction of Public data.

- Access to Restricted Data must be limited to those individuals with need-to-know.

3.3.1.1 Calculating Classification

- Unfortunately there is no perfect quantitative system for calculating the classification of a particular data element. In some situations, the appropriate classification may be more obvious, such as when government Acts require the University to protect certain types of data (e.g. personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide:

Security Objective	**Potential Impact**		
	Low	**Medium**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
As the total potential impact to the University increases from Low to High, the classification of data should become more restrictive moving from Public to Restricted.			

4. Human Resources Security

4.1 Prior to Employment

The University of Waikato must ensure staff, contractors and third party users understand their responsibilities, are suitable for the roles they are considered for, and are screened to reduce the risk of theft, fraud or misuse of the University of Waikato data and systems.

4.1.1 Roles and Responsibilities

- The University of Waikato must provide a position description and responsibility definition for all positions within the organisation.
- Role and responsibility definitions must include all information security responsibilities.

4.1.2 Background Screening and Checking

- Potential employees must be screened to minimise the risk of attacks from internal sources.
- Background screening and checks must be completed for staff with access to information classified as Restricted.
- Background screening should include (at a minimum):
  - Reference checking
  - Qualification checking (including validity)
  - Police checks for certain roles as agreed with the University Risk Manager

4.1.3 Terms and Conditions of Employment

- The University of Waikato must provide a copy of the Computer Systems Regulations 2005 to concisely explain and define the information security responsibilities for all staff (including contractors).
- Information security responsibilities must be included in The University of Waikato staff terms of employment.
- The University of Waikato staff must acknowledge that they have read and understood The University of Waikato's Acceptable Use Policy (Computer Systems Regulations 2005).

4.2 During Employment

The University Of Waikato's Information Security responsibilities in regard to staff, contractors and third party users must be clearly defined - to ensure Information Security can be applied throughout an individual's employment within the University of Waikato.

4.2.1 Management Responsibilities

4.2.1.1 Definition and Dissemination of Responsibilities

- The University of Waikato must ensure that all information security standards and procedures are disseminated to and accessible by all staff, contractors and third party users via the ICT Self Help web pages.

4.2.1.2 Accountability and Performance Management

- The University of Waikato management must highlight information security responsibilities in annual performance management activities.
- Sustained failure to perform information security and incident response activities must be escalated to the Director of ITS.

4.2.1.3 Operational Security Procedures

- The University of Waikato must develop daily operational security procedures that are consistent the University of Waikato information Computer Systems Regulations and security standards.
- Daily operational security procedures must be regularly reviewed and updated to ensure they remain relevant and accurate.

4.2.2 Information Security Awareness, Education, and Training

4.2.2.1 Provision of Training

- The University of Waikato must implement a formal security awareness program to make all staff aware of the importance of data security upon hire.

4.3 Termination or Change of Employment

The University Of Waikato's responsibilities include ensuring an employee's, contractor's or third party user's exit is managed - and that the return of all equipment and the removal of all access rights are completed.

4.3.1 Termination Responsibilities

- The University Of Waikato must control the deletion of user IDs, credentials, and other identifier objects.
- Access must be disabled for any ex-employees on exit, and accounts parked and resources deleted after 6 months.

4.3.2 Removal of Access Rights

- To ensure proper user authentication and password management for users and administrators on all system components, the University Of Waikato must:
    - Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.
    - Immediately disable access for any ex-employee or finished contractor users.
    - Enable accounts used by vendors for remote maintenance only during the time period needed.
    - Assign to an individual or team the responsibility for administering user accounts (including additions, deletions, and modifications).

5. Physical and Environmental Security

5.1 Secure Areas

To prevent unauthorised physical access and damage to - and interference with - its premises and information, the University of Waikato's data and systems must be housed in secure areas, protected by defined security perimeters - and with appropriate security barriers and entry controls.

5.1.1 Physical Security Perimeters

5.1.1.1 Monitoring of Secure Areas

- Cameras must be used to monitor sensitive areas, and the data stored for at least two weeks (unless otherwise restricted by law).

5.1.2 Physical Entry Controls

5.1.2.1 Entry Controls

- Appropriate facility entry controls must be used to limit and monitor physical access to systems that store, process, or transmit Restricted Data.

5.1.2.2 Pin Based Entry Control Systems

- Where a pin based entry control is required, this pin must be changed on an annual basis or upon security incident.
- Pin codes for secure areas must be securely recorded and stored.
- The distribution of pin codes must be limited to those with a need for access.

5.1.2.3 Key Based Entry Control Systems

- The University Of Waikato must control the creation, distribution and storage of all keys.
- All issued keys must be registered to an individual staff member. This individual will remain responsible for the storage and security of this key at all times.
- Lost or stolen keys must be reported immediately.
- If a key is lost or stolen, the Security Manager must conduct a risk assessment to determine if the lock must be replaced.
- All locks must be regularly checked for evidence of tampering or damage. Any identified damage must be reported as a security incident.

5.1.2.4 The Visitor Log

- A 'visitor log' must be maintained to provide a physical assessment trail of visitor activity, and this must be kept for a minimum 2 years.
- The University Of Waikato must ensure all visitors:
    - Are authorised prior to entering areas where Restricted Data is processed or maintained;

- Are escorted or are given a distinguishing and expiring physical token that identifies them as non-employees - surrendering the physical token before leaving the facility or on the expiration date.

5.1.2.5 Visitor Access

- Visitor access must be restricted to only those areas required for the purpose of their visit.
- Where visitors have need to access sensitive or secure areas, they must be escorted by a University of Waikato employee at all times.

5.1.3 Security Obligations and Incidents

5.1.3.1 Employee Obligations

- All of University Of Waikato employees must be made aware of their obligation to:
    - Limit the distribution of pin codes
    - Challenge unidentified visitors in secure areas
    - Remain vigilant for and report all security incidents

5.1.3.2 Physical Security Incidents

- All of The University of Waikato employees are obliged to report any physical security incidents to the UniSafe immediately.
- Physical security incidents include (but are not limited to):
    - Unauthorised entry to secure areas
    - Unescorted visitors
    - Visitors without proper identification, name badge or visitor pass

5.2 The University Of Waikato Equipment Security

To prevent the loss, damage, theft or compromise of the University of Waikato assets - and interruption to business activities - equipment must be protected from both physical and environmental threats.

5.2.1 Secure Systems Configuration and Defence

5.2.1.1 Separation of Purpose and Function

- Separate environments should be provided for development, test and production systems.
- Test systems must be configured such that the test systems provide an accurate representation of the production environment.
- Each University of Waikato host (whether physical or virtual) must have a minimal function.
- Backup and secondary data storage systems must be physically separated from the production storage systems and servers.

5.2.1.2 Attack Surface Reduction

- University of Waikato must disable all unnecessary and insecure services and protocols.
- The following protocols and services must not be used within University of Waikato systems that contain Restricted Data:
  - FTP
  - Telnet
- All exposed services and ports must be configured to ensure the following:
  - Unauthorised access is not permitted
  - All activity is logged
  - Configuration represents best practice for that particular technology
  - Software versions are up-to-date and represent good security practice
- All unnecessary functionality - such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers - must be removed prior to system production deployment.
- System security parameters must be configured to prevent misuse.
- Access control privileges must ensure that only systems administrators or those with explicit permission can install, remove or reconfigure system components.
- Compilers must be removed from all production systems.

5.2.2 Security of Equipment On-Premises

- The University Of Waikato must restrict physical access to:
  - Network jacks that are 'live' and logically connected to the University's internal network security zones.
  - Wireless access points, network distribution points and gateways.
  - Racked infrastructure and other systems devices and servers.
- The University Of Waikato must ensure that all equipment is stored in a suitable secure location.
- The following must be considered (as a minimum) when choosing a secure location for The University Of Waikato equipment:
  - Information Classification
  - Physical Requirements (Power, Ventilation)
  - Access Requirements and Frequency

5.2.3 Equipment Maintenance

- The University Of Waikato must ensure all system components and software have the latest and most relevant vendor-supplied security patches installed as soon as practical for critical patches, or within planned upgrade schedules for less critical patches.
- Change control procedures must be established for all system and software configuration changes. Refer UOW Change Management Process.

5.2.4 Security of Equipment Off-Premises

- Back-up media must be stored in a secure location.
- The University Of Waikato must maintain strict control over the internal or external distribution of any equipment that contains any kind of media containing Restricted Data, including sending this via secured courier or other traceable delivery method.
- The University Of Waikato must ensure that all off-site equipment is registered, secured and managed in accordance with the following The University Of Waikato standards:
  - Asset Management (see section 3)
  - Media Handling (see section 6.7)
  - Access Control (see section 7)
  - Mobile Communications and Teleworking (see section 7.6)

6. Communications and Operations Management

6.1 Operational Standards and Responsibilities

To ensure the correct and secure operation of the University of Waikato's systems - responsibilities and appropriate standard operating procedures for their management and operation must be established.

6.1.1 Documented Operating Standards

- The University Of Waikato must develop daily operational security procedures that are consistent with the requirements of this Information Security standards framework;
- All service providers must maintain and implement policies and procedures consistent with the University security standards.

6.1.2 Change Control Management

- There must be a formal process in place for approving and testing all external network connections and changes to the firewall configuration.
- Change control procedures must be followed for all system and software configuration changes. These procedures must include:
  - Documentation of the impact;
  - Management approval;
  - Testing of operational functionality, or peer review;
  - Back-out procedures.
- The University's Change Management Process must be used for all changes to data systems and PC assets that have Restricted Data.

6.1.3 Separation of Development, Test and Production Facilities

- The University Of Waikato should separate development, test, and production environments.
- Staff must be aware of their responsibilities when working on development, test and production environments.
- Live production data is not to be used for testing or development. If a copy of production data is used for testing or development, production level security controls must be employed to keep the data secure.
- All test data and accounts must be removed before systems are released into production.
- All custom application accounts, usernames, and passwords must be removed prior to applications being released to production.

6.2 Third Party Service Delivery Management

To implement and maintain an appropriate level of security and service delivery in line with third party service delivery agreements, the University Of Waikato must check the implementation of agreements, monitor compliance with the agreements - and manage changes - to ensure the services delivered meet all the requirements agreed with the service provider.

6.2.1 Monitoring and Review of Third Party Services

- All service provider developed custom code must be reviewed prior to release to production in order to identify any potential coding vulnerability.
- All service provider developed web applications must be based on secure coding guidelines to ensure common coding vulnerabilities are prevented.

6.3 System Planning and Acceptance

To minimise the risk of the University of Waikato systems failures, advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance.

6.3.1 Capacity Management

- The University Of Waikato must manage storage capacity in order to ensure the integrity of media that contains Restricted Data.

6.3.2 System Acceptance

- Internal and external network vulnerability scans must be completed after any significant network changes.
- Penetration testing must be completed after any major infrastructure or application upgrade or modification.

6.4 Protection against Malicious and Mobile Code

To protect the integrity of the University of Waikato's systems and data, precautions are required to prevent and detect the introduction of malicious code.

6.4.1 Controls against Malicious Code

- Anti-virus software must be deployed on all systems commonly affected by viruses.
- The University Of Waikato must ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software - including spyware and adware.
- All anti-virus mechanisms must remain current, actively running, and capable of generating assessment logs.

6.5 Backups

To maintain the integrity and availability of the University Of Waikato data and systems, routine procedures must be established to implement an agreed backup standard and strategy for taking back-up copies of data - and rehearsing their timely restoration.

6.5.1 Information Backups

- The University Of Waikato must create a data retention and disposal policy.
- Backups of Restricted Data must be kept for 90 days for business, legal, and/or regulatory purposes (as documented in the data retention policy).
- All media backups must be stored in a secure location.
- Strict control must be maintained over the storage and accessibility of backup media containing restricted data.
- All backup media must be properly inventoried and securely stored.

6.6 Network Security Management

- The secure management of the University Of Waikato's networks - which may span organisational boundaries - requires careful consideration to dataflow, legal implications, monitoring, and protection.

6.6.1 Network Controls

- Firewalls must be configured to restrict connections between publicly accessible servers and any system component storing restricted data. This must include:
  - Implementing a DMZ, or appropriate security zones, to filter and screen all traffic and prohibit direct routes for inbound and outbound Internet traffic;
  - Restricting inbound Internet traffic to authorised IP addresses, services, ports and protocols within the DMZ and/or security zones;
  - Not allowing internal addresses to pass from the Internet into the DMZ and/or security zones;
  - Implementing dynamic packet filtering;
  - Placing the database in an internal network zone, segregated from the DMZ;
  - Securing and synchronizing router configuration files;
  - Installing perimeter firewalls between any wireless networks and the internal network environment where systems with Restricted Data are connected to deny traffic from the wireless environment (or at least controlling it if deemed necessary for business purposes);
  - Installing personal firewall software on any mobile and employee-owned computers with direct Internet connectivity - which are used to access the University Of Waikato's internal network;
  - Prohibiting direct public access from external networks to any system component that stores Restricted Data;
  - Restricting outbound traffic from all applications to IP addresses within the DMZ or appropriate security zones;
  - Implement NAT to prevent internal private addresses from being translated and revealed on the Internet.

- Strong cryptography and security protocols must be used to safeguard restricted data during transmission over open, public networks.
- Wireless networks transmitting restricted data must have the transmissions strongly encrypted (WEP must not be used).
- Administration accounts and accounts with administrator privileges should not be used for remote access to the network by staff, administrators, and third parties.
- Firewall configuration standards must be established that:
  - Documents lists of services and ports necessary for business only;
  - Firewall configuration standards must be established that identifies connections and policies to systems with Restricted Data;
  - Describes the groups, roles, and responsibilities for logical management of network components;
  - Includes a formal process for approving and testing all external network connections and changes to the firewall configuration;
  - Documents the justification for any protocols allowed which includes the reasons for the use of such protocol and security features implemented;
  - Requires a firewall at each Internet connection and between any DMZ and the internal network zones;
  - Includes a six monthly review of firewall and router rule sets
  - Documents the configuration standards for routers.

6.7 Media Handling

To prevent the unauthorised disclosure, modification, removal or destruction of the University of Waikato's data and systems - and interruption to the University of Waikato's business activities - all removable media (see glossary) must be controlled (classified, labelled and inventoried) and physically protected based on the classification level of the data being held on the media.

6.7.1 Management of Media

6.7.1.1 Control of Media

6.7.1.1.1 Media Registration, Records, Logs and Audit

- The University of Waikato must maintain strict control over all removable media, containing Restricted Data.
- The University of Waikato must maintain strict control over all information stored on The University of Waikato controlled removable media.
- The University of Waikato must not store Restricted Data in the public cloud (see glossary).

6.7.1.1.2 Connecting removable media to systems

- The University of Waikato must disable any automatic execution features within operating systems for connectable devices and removable media.

6.7.1.2 Media Storage

- The University of Waikato must ensure that removable media containing restricted information meets the minimum physical security storage requirements as specified in The University of Waikato Physical Security Standard (see section 5).

- When accumulating removable media, consideration must be given to the aggregation effect - which may cause a large quantity of non-sensitive information to become sensitive.

6.7.1.3 Media Transportation

6.7.1.3.1 Approval and Accountability

- The University of Waikato management approval must be sought before any/all removable media classified as restricted is moved from a secured area.

- The University of Waikato management approval must be sought before distribution of any removable media containing restricted information.

6.7.1.3.2 Packaging for Transportation

- The University of Waikato must take all possible measures to protect restricted removable media when in transit off campus.

6.7.1.3.3 Transportation

- The University of Waikato should encrypt removable media containing Restricted Data with an Approved Cryptographic Algorithm when in transit off campus.

6.7.1.4 Off-site Media

- University owned off-site mobile devices (see glossary) containing Restricted Data should have a Trusted Operation Environment (TOE) that includes:
    - unnecessary hardware, software and operating system components are removed;
    - unused or undesired functionality in software and operating systems is removed or disabled;
    - anti-malware and other security software is installed and regularly updated;
    - patching of installed the operating system and other software is current;
    - if applicable, software-based firewalls limiting inbound and outbound network connections are installed;
    - PIN and\or password protection should be used.
- Removable media, other than University owned mobile devices, containing Restricted Data must be encrypted with an Approved Cryptographic Algorithm.

6.7.2 Disposal of Media

- Media containing Restricted Data must be destroyed when no longer needed for business or legal reasons.

- The University Of Waikato must conduct media disposal activities in accordance with this University of Waikato Media Handling standard.

6.7.2.1 Storage of Media for Disposal

- Media for disposal must be securely stored until it can be disposed of in accordance with this University of Waikato Media Handling standard.
- The University Of Waikato must remain aware of the aggregation of sensitivity and value when storing large quantities of unclassified media in one location.
- Access to all storage locations should be restricted to ensure that it can only be accessed by authorised parties. This includes (but is not limited to):
    - Secure locked storage for mass storage media and removable devices.

6.7.2.2 Use of Third Party Disposal Service Providers

- Third party disposal service providers may be engaged to dispose of The University of Waikato media but must be subjected to due diligence checks prior to engagement.

6.7.2.3 Sanitisation and/or Destruction of Media Containing Restricted Data

- The University of Waikato should sanitise whenever possible and\or destruct the media containing Restricted Data.

6.7.2.3.1 Server Hard Drives

- Server hard drives must be securely wiped to GCSB or internationally recognised Standards (e.g. DOD) and physically destroyed.
- Exceptions can be made with written approval of the Management.

6.7.2.3.2 Backup Tapes

- The University of Waikato must disposed magnetic tapes in a secure manner by physically destroying them.

6.7.2.3.3 Printers, Fax Machines and Copiers

- Many of these devices contain hard drives or other types of media in them. They often store past data that has been copied or printed and pose a data security risk. The University of Waikato should make sure that these devices do not have data on them when they are returned or disposed of.

6.7.2.3.4 Other Media

- All other media containing Restricted Data should be destroyed when it is no longer useful to the University. Just erasing the media is not secure enough; it must be destroyed so that it is not recoverable by any means:
    - Digital Cameras – Securely erase internal memory (if possible) or destruct.
    - Floppy Disk – Physically destroy by breaking the case and cutting the disk inside or by shredding the disk.
    - Caseless Optical (CD/DVD) – Physically destroy by cutting into pieces or by shredding.
    - ZIP/Cartridge Media – Physically destroy by breaking with hammers, drilling or shredding.

- Solid State, USB/Flash Drives, SD memory – Physically destroy by breaking with hammers, drilling or shredding.

6.7.2.3.5 Use of Third Party Data Destruction Services

- The destruction of media must only be outsourced to an approved commercial facility, and The University of Waikato must take care when selecting such contractors - ensuring they have adequate controls and experience.

6.7.2.4 Media Disposal

- The University of Waikato must document procedures for the disposal of media.
- The University of Waikato must declassify all media prior to disposing of it into the public domain.

6.8 Information Handling Standards

6.8.1.1 Audit and Accountability

6.8.1.1.1 Control of Information

- Access to computing resources and restricted information must be limited to those individuals whose job requires such access.
- The University of Waikato must establish a mechanism for systems with multiple users that restricts access based on a user's 'need to know' - and is set to 'deny all' unless specifically allowed.

6.9 Exchange of Information

To maintain the security of the University of Waikato Restricted Data exchanged within the company or with any external entity - exchanges of information and software must be based on a formal exchange policy, carried out in line with exchange agreements, and must be compliant with any relevant legislation.

6.9.1 Exchange Agreements

- If Restricted Data is shared with service providers, then contractually the following is required:
  - They must adhere to the University Of Waikato Information Security Policy and standards framework
  - An acknowledgement that the service provider is responsible for the security of Restricted Data the provider possesses.

6.9.2 Physical Media in Transit

- Physical access must be restricted to handheld devices that store, process, or transmit Restricted Data.
- All paper and electronic media that contain Restricted Data must be physically secured.
- Media must be sent by secured courier or other delivery method that can be accurately tracked.

- Management approval must be sought before any/all restricted media is moved from a secured area.

6.9.3 Electronic Messaging

- Sensitive information such as system configurations and passwords must never be sent unencrypted by instant messaging technologies such as e-mail.

6.10 E-Commerce Services

The security implications associated with using e-commerce services - including on-line transactions and the requirements for controls - must be considered by the University of Waikato.

6.10.1 E-Commerce and On-Line Transactions

- The University Of Waikato must maintain firewall configuration standards.
- Firewall configuration must:
    - Deny all traffic from 'untrusted' networks and hosts (except for protocols necessary for communication with the Restricted Data network environment).
    - Restrict connections between publicly accessible servers and any system component providing e-commerce (including any connections from wireless networks).
- Direct public access between external networks and any system component that stores Restricted Data must be restricted.
- Strong cryptography and security protocols must be used to safeguard Restricted Data during transmission over open, public networks.
- All e-commerce web applications must be developed based on secure coding techniques.
- The University Of Waikato must ensure all web-facing e-commerce applications are protected against known attacks.

6.11 Monitoring

To detect unauthorised systems activities and Restricted Data access, the University of Waikato systems must be monitored and information security events must be recorded. System monitoring must be used to check the effectiveness of controls adopted and to verify conformity to this standards framework. Additionally, the University of Waikato operator logs and fault logging must be used to ensure system problems are identified.

6.11.1 Assessment Trails

- Ensure logging and assessment trails for security events are enabled and unique to each system's Restricted Data environment and consistent with the Information Security Policy and standards.
- The following (at least) must be recorded for all system components for each security event:
    - User identification;
    - Type of event;

  - Date and time;
  - Success or failure indication;
  - Origination of event;
  - Identity or name of affected data, system component or resource.

- Assessment trail files for security events must be promptly backed up to a centralised log server or difficult to alter media.
- Assessment trail history must be retained for at least one year (with a minimum of three months online availability).
- Alerts from IPS and file integrity monitoring systems must be enabled.

6.11.2 Monitoring System Use

- The University Of Waikato must establish a process for linking all access (especially privileged account access) to system components containing Restricted Data to an individual user.
- Automated assessment trails must be implemented for all system components to reconstruct the following events:
  - All individual user accesses to Restricted Data;
  - All actions taken by any individual with a privileged account;
  - Access to all assessment trails;
  - Invalid logical access attempts to Restricted Data;
  - Use of identification and authentication mechanisms;
  - Initialisation of the assessment logs
  - Creation and deletion of system-level objects.
- The University of Waikato must develop operational security procedures that include log reviews for all system components used with Restricted Data.
- Log reviews must include those servers that perform security functions (i.e.: IPS, AAA servers).
- Network IPS, systems must be used to monitor all network traffic to/from systems with Restricted Data and alert staff to suspected compromises.
- All IPS engines must be kept up-to-date.
- The University Of Waikato must assign to an individual or team the responsibility for:
  - Monitoring and analysing security alerts and information
  - Monitoring and controlling all Restricted Data access.

6.11.3 Protection of Log Information

- Direct public access must be prohibited between external networks and any system logs.

- Assessment trails must be secured so they cannot be altered.
- Viewing of assessment trails must be limited to those with a job-related need.
- Assessment trail files must be protected from unauthorised modification.

6.11.4 Clock Synchronisation

- All critical system clocks and times must be synchronised.

7. Access Control

7.1 Business Requirement for Access Control

The purpose is to control access to the University of Waikato's data, systems - and business processes - on the basis of business and Information Security requirements.

7.1.1 Access Control Standards

- Access to computing resources and sensitive information must be limited to only those individuals whose job requires such access.
- A mechanism must be established for systems with multiple users that restricts access based on a user's 'need to know' and is set to 'deny all' unless specifically allowed.
- Strict control must be maintained over the accessibility of media that contains Restricted Data.
- Access controls, limitations, and restrictions for Restricted Data systems must be reviewed annually to assure the ability to adequately identify and to stop any unauthorised access attempts.
- The University Of Waikato must develop usage policies for critical employee-facing technologies that define the proper use of these technologies for all staff, including explicit management approval for use of the technology.
- The University of Waikato should automatically disconnect sessions or lock workstations and terminals after a specific period of inactivity.
- The University Of Waikato must assign to an individual or team the duty of monitoring and control of each system utilising Restricted Data.
- The University Of Waikato must maintain a register which lists the systems with owners and responsibilities.
- Each entity's (i.e. merchant, service provider, or other entity) hosted environment and data must be protected to ensure each entity only has access to its own Restricted Data environment.

7.2 User Access Management

To ensure authorised user access - and to prevent unauthorised access to the University of Waikato's data and systems - formal standards must be put in place to control the allocation of access rights to the University of Waikato data, systems and services.

7.2.1 User Registration

- The University Of Waikato must ensure proper user authentication and password management for users and administrators on all system components as follows:
    - Control and monitor the addition, deletion, and modification of user IDs, credentials, and other identifier objects;
    - Immediately revoke access for any terminated users;
    - Revoke access for leaving users within 1 working day after their last day of work;

  - Disable inactive user accounts (at least) every 180 days;
  - Communicate password procedures and policies to all users who have access to Restricted Data.
  - Do not use group, shared, or generic accounts and passwords for access to Restricted Data.

- The University Of Waikato must establish a process for linking all access to systems that hold Restricted Data to each individual user.
- The University Of Waikato must assign to an individual or team the responsibility for administering user accounts, including additions, deletions, and modifications.
- First-time passwords must be set to a unique value for each user - and must change immediately after the first use.

7.2.2 Privilege Management

7.2.2.1 Scope of Privileges

- The University Of Waikato must ensure that user privileges are limited to those required for a particular role.
- Privileged access to computing resources and restricted and private data must be limited to those individuals whose job requires such access only.

7.2.2.2 Privilege Requests

- All requests for additional privileges must be formally recorded and include a valid justification.
- The University Of Waikato must review all privilege requests and ensure that they are authorised by the appropriate system risk owner before implementation.
- Granted requests for privileges must be retained for a minimum of 7 years, or for as long as the restricted data is retained in regards to the privilege granted.

7.2.2.3 Reviewing User Privileges

- The University Of Waikato must review user privileges to restricted information systems on an annual basis.
- As part of this review, all accounts should be scrutinised to ensure that:
  - Justification remains valid.
  - The University Of Waikato security policies, standards and procedures have been complied with.
  - Access remains proportionate and appropriate.
- Any account or group found to no longer meet these criteria must have their privilege access disabled and removed after a period of no more than 90 days.

7.2.2.4 Monitoring of Privileged Activity

- The University Of Waikato must ensure that all accounts with privileged user account access to restricted systems are subject to monitoring and that all activity and user sessions can be recreated where possible.
- All accounts that access Restricted Data should be identified as high risk and must be subjected to monitoring.

7.2.3 User Password Management

7.2.3.1 Password Complexity Requirements

- The University Of Waikato must enforce password complexity requirements for all accounts on all systems. Where systems use a login that is separate to the user's network account login, access to be able to log into the system must be controlled by the privileges assigned to the network account login and the system's login password complexity must either meet the University's password complexity requirements or as near as the system's functionality provides.
- The University Of Waikato password complexity requirement must include at a minimum password length of seven characters, consisting of at least two of the following character sets:
    - Lowercase characters (a-z)
    - Uppercase characters (A-Z)
    - Digits (0-9)
    - Punctuation and special characters.
    - To encourage strong passwords the University of Waikato is to consider the use of password setting/changing routines that provide feedback to the user as to the password's strength.
    - To encourage strong passwords the University of Waikato is to consider a shorter password expiry timeframe (ie 30 days) for weaker passwords and a longer expiry timeframe (ie 180 days) for strong passwords – 90 day expiry being the norm for medium strength passwords.
- Where systems cannot be configured to enforce complexity requirements, access to be able to log into the system must be controlled by the privileges assigned to the network account login and the systems login password complexity must either meet the University's password complexity requirements or as near as the system's functionality provides.

7.2.3.2 Password Change and Reuse

- The University Of Waikato must prevent the following activities during network account - and where possible, per system - password change and reset:
    - Password reuse across multiple accounts
    - Password reuse within 6 password changes
    - Use of sequential passwords
    - Use of predictable passwords
- The University Of Waikato must ensure that passwords for all accounts on all systems and devices, where possible, are changed at least every 180 days.

- Wherever possible, the University Of Waikato must prevent system users from changing their password more than once a day.
- The University Of Waikato must force the system user to change an expired password on initial logon or if reset.

7.2.3.3 Password Reset Procedures

- The University Of Waikato must ensure that system users provide sufficient evidence to verify their identity when requesting a password reset.
- Identity verification must be completed using information pre-registered in the UARM system (to be replaced with IdM Project's "UniAccess" tool).

7.2.4 Review of User Access Rights

7.2.4.1 Suspension of Access

- The University Of Waikato must suspend user accounts in the following circumstances
  - Three failed login attempts
  - Suspected malicious activity
  - Suspected inappropriate behaviour
- In the case of failed logins, accounts must only be automatically unlocked after 30 minutes.
- In the case of malicious or inappropriate behaviour, suspended accounts must be unlocked by an authorised systems administrator.
- The University Of Waikato must record all account suspensions and investigate all repeated account lockouts.

7.2.4.2 Changing Roles

- The University Of Waikato must ensure that upon changing role within the organisation, any user accounts, access permissions or group memberships granted to the user are reviewed and removed where no longer required.
- This must be applied to employees, contractors and sub-contractors.
- This must be applied to temporary and permanent role changes.
- Where a user had access to systems or devices that do not use centralised authentication, all devices must checked and relevant accounts removed.
- Any shared passwords known by or accessed by the user must be changed immediately.

7.2.4.3 Leaving the Organisation

- The University Of Waikato must ensure that upon leaving the organisation, all accounts for a user are disabled.
- This must be applied to employees, contractors and sub-contractors.
- Any shared passwords known by or accessed by the user must be changed immediately.

7.2.4.4 Inactive Accounts

- The University Of Waikato must conduct monthly reviews of all user and system accounts and identify all accounts that have been inactive for 180 days or more.
- Accounts that have been inactive for 180 days must be disabled.

7.2.4.5 Disabled Accounts

- The University Of Waikato must conduct monthly reviews of all user and system accounts and identify all accounts that have been disabled for 180 days or more.
- Accounts that have been disabled for 180 days or more must be terminated.

7.2.4.6 Account Termination

- The University Of Waikato must ensure that all terminated accounts are subjected to the following configuration changes:
  - Accounts are set to expired.
  - Accounts are removed from all Active Directory groups.
  - Accounts have logon hours set to 0 hours per day.
  - Accounts are moved to the Active Directory "Deletions" organisational unit (OU).
- The University Of Waikato must ensure that a record is made regarding the Active Directory groups the user was in prior to termination.

Note: This standard has been defined as such to compensate for the lack of reusable account names and email addresses in other products used within the University Of Waikato.

7.2.4.7 Shared, Generic and Device Accounts

- No shared accounts of any description are permitted on The University of Waikato systems, applications or devices that contain Restricted Data.
- All default administration, guest or generic accounts must be disabled or deleted prior to system deployment.
- All default vendor passwords and user names must be changed prior to system deployment.

7.3 User Responsibilities

For effective Information Security and to prevent unauthorised user access - and compromise or theft of the University of Waikato data and systems - the co-operation of authorised University of Waikato users is essential.

7.3.1 Password Use

- First-time passwords must be set a random unique value for each user - and must change immediately after the first use.
- User passwords must be changed (at least) every 180 days.

- The use of Strong passwords is expected. To encourage strong passwords the University of Waikato to consider the use of password setting/changing routines that provide feedback to the user as to the password's strength and set a shorter password expiry timeframe (ie 30 days) for weaker passwords and a longer expiry timeframe (ie 180 days) for strong passwords - 90 day expiry being the norm for medium strength passwords.

7.3.2 Unattended User Equipment

- If a session has been idle for more than 30 minutes - users must be forced to re-enter the password to re-activate the terminal.
- All University of Waikato staff should report any equipment that does not comply with this standard.

7.4 Network Access Control

To prevent unauthorised access to the University of Waikato networked services - access to both internal and external networked services must be controlled.

7.4.1 Network Connection Control

- Direct public access must be restricted between external networks and any system component that stores Restricted Data.
- Internal network access must be restricted depending on the user and device credentials, with access granted based on user access permissions and the device’s security profile.

7.4.2 Network Routing Control

- Inbound and outbound traffic must be restricted to that which is necessary for the restricted data environment only - with all other inbound and outbound traffic not being allowed.

7.5 Operating System Access Control

To prevent unauthorised access to the University of Waikato operating systems, security facilities must be used to restrict access to operating systems to authorised users.

7.5.1 Systems Configuration and Monitoring

7.5.1.1 Authentication Methods

- The University Of Waikato must monitor developments in authentication technologies to ensure that this standard and any associated procedures are kept up to date with current security good practice.

7.5.1.2 Device Configuration

- Vendor-supplied default passwords must be changed prior to installing a system on the University of Waikato’s network.
- Where available, all system components must be configured to use centralised authentication systems.

7.5.1.3 Password Storage

- The University Of Waikato must not store passwords in plain text on any system or device.
- All passwords must be encrypted during transmission and storage on all system components.

7.6 Mobile Computing and Teleworking

To ensure the University of Waikato Information security when using mobile computing and teleworking facilities the protection required must be commensurate with the risks these specific ways of working cause.

7.6.1 Provision of Devices

7.6.1.1 Use of Personal Devices

- Device maintenance and security for personal mobile computing and communication devices (including but not limited to laptops, tablets and mobile phones) remains the responsibility of the asset owner.
- The University of Waikato must inform all users of personal devices of their security obligations concerning mobile computing devices.
- Personal devices must only connect to The University of Waikato networks designated for such usage. These include mobile device and guest networks only.
- The University of Waikato must prevent personal and unknown mobile computing devices from connecting to all other University of Waikato systems with Restricted Data.

7.6.1.2 Use of University of Waikato Devices

- Personal firewalls and anti-virus must be installed on all of the University of Waikato issued laptop computers and mobile computing devices.
- All of the University of Waikato mobile computing devices must be registered as per the University of Waikato mobile device management policy.
- The user will be responsible for the secure storage and management of mobile computing device.
- The University of Waikato must conduct an audit of all of the University of Waikato provided mobile computing devices on an annual basis. This audit must:

    Physically verify the device and its condition

    Identify any damage or modifications since issue

    Verify device registration details

    Verify the allocated user remains unchanged

- The University of Waikato issued mobile computing devices must be returned upon leaving the organisation (including all issued peripherals and storage media).

7.6.2 Liability, Storage and Insurance

7.6.2.1 Insurance

- The University of Waikato does not insure privately owned devices used for University Waikato business.

7.6.3 Device Usage

7.6.3.1 Data Storage

- Restricted Data stored on University of Waikato owned mobile devices, must be file or disk encrypted.
- The University of Waikato should ensure that Restricted Data is only stored on mobile devices for the duration it is needed. Extended storage on such devices must be discouraged.

7.6.3.2 Network Usage

- When connecting with a mobile device on campus, University of Waikato staff and students must only connect to designated networks for mobile devices (including tethering).
- The University of Waikato must ensure that personal or unknown devices are prevented from connecting to the secure internal University of Waikato networks.

7.6.4 Remote Access Governance and Management

7.6.4.1 Authorisation

- Remote access authorisations should be reviewed annually.

7.6.4.2 Logging and Monitoring

- All remote access activity must be logged and monitored in line with the University of Waikato Vulnerability Management standard (see section 8.5).

7.6.5 Configuration and Operation

7.6.5.1 Authentication

- Strong authentication must be used for remote access to the network by staff, and authorised third parties.
- Where exceptions to this item are required (such as guest and mobile wireless networks), these networks must be segregated from core University of Waikato data storage systems and networks.
- Remote access must not be permitted using system administration accounts, or accounts with system administration privileges.

7.6.5.2 Device and Systems Configuration

- The University of Waikato should strongly encourage that remote devices employ anti-virus and firewall software.

7.6.5.3 Data Access and Storage

- The University of Waikato must ensure that Restricted Data is only stored remotely for the duration it is needed.

8. Information Systems Acquisition, Development and Maintenance

8.1 Systems Security Requirements

The design and implementation of the University of Waikato systems can be crucial for information security. Security requirements must therefore be identified and agreed prior to the development and/or implementation of the University of Waikato systems.

8.1.1 Operating Standards

8.1.1.1 Development of Operational Standards

- The University Of Waikato must develop daily operational security procedures that are consistent with the requirements of this Information Security standard.
- All information systems must be managed in accordance with industry best practice
- Documented Standard Operating Procedures must be prepared for all those system activities associated with information processing and communication facilities. Therefore the following must be considered:
  - System start-up and close-down;
  - Backups;
  - Equipment maintenance;
  - Media handling;
  - System version;
  - Application versions;
  - Secure area working.

8.1.1.2 Responsibility and Accountability

- Departmental ICT Managers are responsible for ensuring the development, maintenance, updating and implementation of any Standard Operating Procedures (SOPs).

8.1.2 Operating procedures

These should be peer reviewed as part of the UOW Change Management Process.

8.1.2.1 Change Management and Definition of Process

- The implementation of changes to systems with Restricted Data must be controlled by the use of formal Change Management procedures.
- The UOW Change Management Process must be followed for all Restricted Data system and software configuration changes - these procedures must include:
  - the testing of operational functionality; and
  - have passed an internal security review conducted by the change implementer's peer.
- The University Of Waikato Change Management procedures must be documented and peer reviewed in order to protect the integrity, availability and confidentiality of the University of Waikato's information systems.
- Formal management responsibilities and procedures must be in place to ensure satisfactory control of all changes to equipment, software or procedures.
- The Manager, ICT Infrastructure (CAB chairperson) must approve all changes that impact the security of The University of Waikato Restricted Data information and systems.

8.1.2.2 Control Items

- The following Change Management control items must be considered:
  - Identification and recording of all significant changes;
  - Planning and testing of changes;
  - Assessment of the potential information security impacts of such changes;
  - Approval procedure for proposed changes;
  - Communication of change details to all relevant persons including third parties; and
  - Rollback procedures (including processes and responsibilities for aborting and recovering from unsuccessful changes and unforeseen events).
- Any change procedure must also include:
  - Maintaining a record of agreed authorisation levels;
  - Ensuring changes are submitted by authorised users only;
  - Reviewing relevant controls and integrity procedures to ensure they will not be compromised by the changes;
  - Identifying all software, information, database entities, and hardware that require amendment;
  - Obtaining approval for detailed proposals before work commences;
  - Ensuring authorised users accept changes prior to implementation;
  - Ensuring that the system documentation set is updated on the completion of each change;
  - Ensuring old documentation is archived or disposed of;

- Maintaining version control for all software updates;
- Maintaining an audit trail of all change requests;
- Ensuring that operating documentation - and any user procedures - are changed as necessary to remain appropriate; and
- Ensuring that the implementation of changes takes place at the right time - and minimise the impact on core University operations.

8.1.2.3 Audit and Logging

- When changes are made, an audit log containing all relevant information must be retained for a minimum of 7 years.

8.1.2.4 Emergency Change Management

- The procedures should define the appropriate actions to be followed before and after any emergency changes are implemented.
- These procedures must ensure existing security and control procedures:
  - Are not compromised;
  - That support personnel are only given access to those parts of the system necessary for their work; and
  - That agreement and approval for any change is obtained within 1 working day.

8.1.2.5 Change Implementation and Rollback

- All change requests must include a rollback procedure or process to be activated in case of unforeseen change consequence or impact.

8.1.3 Separation of Development, Test and Production Facilities

8.1.3.1 Provision and Configuration of Environments

- The University Of Waikato should have separate development/test, and production environments.
- The University Of Waikato must ensure that test and production environments are configured to ensure that testing can be conducted in a replica of the production environment.
- Production systems must be configured such that no compilation, development or alteration of production applications can be conducted.

8.1.3.2 Test Data

- Live production data is not to be used for testing or development.
- Development and test databases derived from production data must have the same level of security controls as the production databases.

8.1.3.3 Release Management

- The University Of Waikato must have a documented release management process that governs the transition of systems and data between test, development and production facilities.
- This document must comply with the UOW Change Management Process.

8.1.3.4 Preparation for Release

- All test data and accounts must be removed before production systems become active.

8.2 Third Party Service Delivery Management

8.2.1 Agreements

8.2.1.1 Implementation Standards

- The University Of Waikato must ensure that all outsourced systems development and implementation providers are held to The University of Waikato security standards.
- These requirements must be included in all service agreements.

8.2.2 Monitoring and Review of Third Party Services

8.2.2.1 Right to Audit

- The University Of Waikato must ensure that the 'right to audit' (a periodic review of the service provider's security controls) is included in every commercial service agreement.
- The 'right to audit' must extend to a minimum of the following activities:
  - Penetration Testing (checking that the service provider does periodic testing);
  - Vulnerability Assessment (checking that the service provider assesses and addresses vulnerabilities on an ongoing basis);
  - Configuration Review (checking that the service provider's security controls are still appropriate and reviewing any changes that have been made);
  - Information Security Audit (checking that the service provider does regular audits); and
  - Physical Review (Premises, Data centres - if there have been changes).

8.2.2.2 Service Levels and Information Security

- The University Of Waikato must review the service levels provided by external providers on at least annual basis to ensure that all obligations have been met.
- The University Of Waikato must include information security objectives in external provider service level reviews.
- The University Of Waikato must reserve the right to amend, terminate or otherwise renegotiate all agreements with external parties based on reviews.

8.2.2.3 Remediation Costs

- The University Of Waikato must ensure that all outsource providers are held liable for the cost of remediation activities incurred as a result of failure to implement systems to The University of Waikato security standards.
- This obligation must be documented in commercial agreements.

8.3 System Planning, Design, Development and Acceptance

8.3.1 Capacity Management

8.3.1.1 Media Access and Storage

- The University Of Waikato must maintain strict control over the storage and accessibility of media that contains Restricted Data in accordance with The University of Waikato Media Handling standard (see section 6.7).

8.3.2 Systems Design

8.3.2.1 Requirements Analysis and Specification

- Software applications must be developed based on industry best practices, such as OWASP, and incorporate information security throughout the software development life cycle.

8.3.2.2 Defensive Design

- Web applications must be developed based on secure coding guidelines (OWASP).
- The University Of Waikato must ensure all web-facing applications are protected against known attacks by applying either of the following methods:
  - All custom application code must be peer reviewed for common vulnerabilities; and
  - Installing an application layer firewall in front of web-facing applications.

8.3.3 System Development and Systems Acceptance

8.3.3.1 Code Review

- All custom code must be reviewed prior to release to production or customers in order to identify any potential coding vulnerability.
  - All code that is customer facing, should be peer reviewed for security vulnerabilities; and
  - All code should be reviewed for best practice development guidelines.

8.3.3.2 Standards

- All developed web applications must be based on secure coding guidelines to ensure common coding vulnerabilities are prevented.

- All web applications should use Open Web Applications Security Project (OWASP) best practice guidelines.
- All web applications that will be handling financial data and transactions, must conform to PCI DSS guidelines for PCI DSS compliance (refer to PCI DSS compliance manual for guidelines).
- Web application penetration testing must be completed on new external facing applications before production release and upon each subsequent major release.
- Internal and external network vulnerability scans must be completed at least quarterly - and after any significant network changes;
- Penetration testing must be completed at least annually - and after any significant infrastructure or application upgrade or modification;

8.4 Cryptographic Controls

To protect the confidentiality, authenticity or integrity of the University of Waikato data by cryptographic means a standard must be developed on the use of cryptographic controls.

8.4.1 Use of Cryptographic Controls

8.4.1.1 For wireless environments:

- Enable Wi-Fi Protected Access technology for encryption and authentication, and update when WPA2-capable and updating is possible;
- WI-Fi passwords, where used, should be a complex password that includes capitals and lower case letters, numbers and characters with the minimum length of 8 characters;
- WI-Fi passwords, where used, must be changed annually;
- Wireless vendor defaults must be changed (including - but not limited to - default SSID, passwords, and SNMP community strings)

8.4.1.2 Disk and Database Encryption

- If disk (rather than file- or column-level database) encryption is used, logical access must be managed independently of native operating system access control.
    - All data classified CONFIDENTIAL and above must be encrypted in storage and in transfer (SSL); and
    - All data classified CONFIDENTIAL and above must be encrypted in physical transit.
- Decryption keys must not be tied to user accounts.

8.4.2 Cryptographic Key Management

8.4.2.1 Key Storage

- The University Of Waikato must provide details of how the key(s) will be electronically and physically stored and transferred to different sites.
    - Keys must not be stored on the same media as the encrypted data; and
    - All cryptographic keys should be stored in an encrypted state.

- The University Of Waikato must protect encryption keys used for the encryption of restricted data against both disclosure and misuse (see data classification guide for data classification reference).
- A backup of cryptographic keys should be kept offsite in an encrypted state.

8.4.2.2 Key Access

- Access to keys must be restricted to the fewest number of custodians necessary.
  - All allowed user access to cryptographic keys should be approved by the Manager, ICT Infrastructure.
  - Cryptographic key management access should assigned by the Systems Engineer (Security).
  - Encryption keys must be stored securely in the fewest possible locations and forms.

8.4.2.3 Key Management Processes and Procedures

- The University Of Waikato must provide a description of the process of the:
  - Generation of strong keys;
  - Secure key distribution of keys;
  - Periodic key changes;
  - Destruction of old keys;
  - Prevention of unauthorised substitution of keys; and
  - Revocation of old or invalid keys.
- The University Of Waikato must describe how the key(s) are to be used, include the following:
  - When encryption and decryption occurs;
  - What classification of data is to be encrypted and decrypted (see classification guide for assistance); and
  - The keys and algorithms are to be used in these transformations.
- The University Of Waikato's cryptographic key management users must provide details on how keys will be distributed electronically or physically.
- The University Of Waikato require key management users to accept their key-custodian responsibilities.
- Cryptographic keys must be protected against disclosure and misuse by restricting the number of cryptographic key management users and by storing keys securely in as few locations and forms as possible.
- Encryption keys shall be disclosed only when required for exchange or by law.
- Keys shall be distributed out of band to data transmission.
- The University Of Waikato must use best practice security countermeasures that will be used to protect the key(s) from compromise.

- The University Of Waikato must provide a description of how the key(s) will be sourced. This may be via another agency or may be key(s) generation processes or equipment. It may be required to provide details of the initial key generation or seeding.

8.4.2.4 Key Management Incident Response

- The University Of Waikato must fully document Key Management Incident Response procedures for:
  - The event that a key may have been compromised; and
  - The replacement of known or suspected compromised keys.
- In the event that a cryptographic key has been compromised The University Of Waikato staff must:
  - Escalate the event to the Systems Engineer (Security).
  - Provide reporting of the compromise to the Manager, ICT Infrastructure.

8.5 Security of System Files

To ensure the security of the University of Waikato's system files, access to such system files and program source code must be controlled - and projects and support activities conducted in a secure manner.

8.5.1 Control of Production Software

- The UOW Change Management Process must be followed for all production Restricted Data system and software configuration changes, including the testing of full operational functionality.

8.6 Security in Development and Support Processes

To maintain the security of the University of Waikato application system software and information, project and support environments must be strictly controlled.

8.6.1 Technical Review of Applications after Operating System Changes

- Internal and external system vulnerability scans must be run after any significant Operating System changes.

8.7 Vulnerability Management

To reduce risks resulting from the exploitation of published vulnerabilities – the University of Waikato must implement vulnerability management in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

8.7.1 Vulnerability Awareness

8.7.1.1 Attack Surface Awareness

- The University Of Waikato must maintain a record of system components in use across The University of Waikato systems.
- This record should include:
  - Operating Systems (including versions)
  - Software packages and installed components
  - Libraries, development frameworks and application components
- The University Of Waikato must use this record to focus vulnerability awareness activities including:
  - Patching and system updates
  - Systems configuration and hardening
  - Technology upgrades
  - Installation of defensive security measures
  - Systems monitoring
  - Education and Training

8.7.1.2 Vulnerability Awareness

- The University Of Waikato must maintain a high level of vulnerability awareness.
- Vulnerability awareness should be maintained through:
  - Active membership of industry and community groups
  - Integration with vulnerability information sources
  - Attendance of relevant conferences and training courses

8.7.1.3 Vulnerability Severity Classification

- The University Of Waikato must ensure that all vulnerabilities are assigned a severity value relevant to the potential impact on the confidentiality, integrity and availability of The University of Waikato systems.
- Vulnerability severity classifications must be recorded.
- Vulnerability severity classifications must be used to prioritise the remediation of security issues.

CVSS2	LEVEL	DESCRIPTION
9 – 10	Critical	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.
7 - 8.9	High	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
4 - 6.9	Medium	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
0.1 - 3.9	Low	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
0	Info	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.

Table 1 – Vulnerability Severity Rankings http://nvd.nist.gov/cvss.cfm

8.7.1.4 Dissemination of Vulnerability Information

- The University Of Waikato must assign responsibility for the dissemination of vulnerability information to all relevant technical area and systems risk owners.

8.7.2 Systems Development and Vulnerability Assessment

8.7.2.1 Application Development

- Software applications must be based on industry best practices and incorporate information security throughout the software development life cycle.
- Custom code must be peer reviewed prior to release to production or customers in order to identify any potential coding vulnerability.
- All web applications must be developed based on secure coding guidelines to prevent common coding vulnerabilities.

8.7.2.2 Vulnerability Scanning

- The University Of Waikato must establish a process to identify newly discovered security vulnerabilities, and standards must be updated to address these.
- The University Of Waikato must ensure all web-facing applications are protected against known attacks by running internal and external network vulnerability scans:
  - Prior to initial system use
  - Every 6 months
  - After any significant change in the network

8.7.3 Patching

8.7.3.1 Identification of Systems for Patching

- The University Of Waikato must maintain a record (monitor and reporting tool) of all systems and technologies that require the application of security patches.
- The University Of Waikato must ensure that this record is updated regularly.

8.7.3.2 Assessment and Testing of Patches

- Prior to installation, systems patches should be tested.
- Any issues identified during testing that may affect other faculties/divisions must be reported to the Systems Engineer (Security).
- Where testing results in the decision not to install one or more security patches, this must be recorded in the Patch Register.

8.7.3.3 Lack of Patch Availability and End of Life

- The University Of Waikato should assess the security risk of using software or IT equipment when a cessation date for support is announced or when the product is no longer supported by the developer.
- Where known vulnerabilities cannot be patched, or security patches are not available, The University Of Waikato should either implement:
  - Vulnerability Resolution Techniques:
    - Disable the functionality associated with the vulnerability though product configuration
    - Ask the vendor for an alternative method of managing the vulnerability
    - Move to a different product with a more responsive vendor, or
    - Engage a software developer to correct the software
  - Exploit Prevention Controls:
    - Apply external input sanitisation (if an input triggers the exploit)
    - Apply filtering or verification on the software output (if the exploit relates to an information disclosure)
    - Apply additional access controls that prevent access to the vulnerability, or
    - Configure firewall rules to limit access to the vulnerable software
  - Containment Controls:
    - Apply firewall rules limiting outward traffic that is likely in the event of an exploitation
    - Apply mandatory access control preventing the execution of exploitation code,
    - Set file system permissions preventing exploitation code from being written to disk

- Detection Tools:
  - Deploy an IPS
  - Monitor logging alerts, or
  - Use other mechanisms as appropriate for the detection of exploits using the known vulnerability.

8.7.3.4 Routine Patching

- Routine patches (including security and functional patches) must be applied to all systems and components within 3 months of release, or prior to the start of the next major semester, whichever is later.

8.7.3.5 Critical Patching

- Critical patches must be applied to all systems and components within 30 days of release.

8.7.3.6 Change Control

- All Restricted Data systems patching must be conducted in conjunction with the UOW Change Management Process.

8.7.3.7 Rollback

- The University Of Waikato must ensure that rollback mechanisms are in place for all Restricted Data system changes including patching.
- The University Of Waikato must be able to rollback systems and components to a previous stable configuration upon an issue arising from patching activities.

8.7.4 Systems Configuration and Build

8.7.4.1 Configuration Standards and Processes

- Configuration standards must be developed for all system components which must address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
- All unnecessary and insecure services, protocols and functionality must be disabled (e.g. scripts, drivers, features, subsystems, file systems, and unnecessary web servers).
- System security parameters must be configured to prevent misuse.

8.7.4.2 Automated builds and images

- To simplify the process of configuring multiple hosts or systems, The University of Waikato should use automated build scripts, or in the case of virtualised systems templates, snapshots and images.

8.7.4.3 Separation of Purpose

- The University Of Waikato should ensure where practical that systems are implemented with only one primary function per server or virtual system component.

8.7.5 Mobile and Malicious Code

8.7.5.1 Anti-Virus

- Anti-virus software must be deployed on all systems.
- The University Of Waikato must ensure that anti-virus programs are capable of detecting, removing, and protecting against other forms of malicious software - including spyware and adware.
- All anti-virus mechanisms must remain current, actively running, and capable of generating assessment logs.
- The University Of Waikato must ensure that all anti-virus applications are updated daily.

8.7.6 Control of Technical Vulnerabilities

- Configuration standards must be developed for all system components (see glossary) which must address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.
- All unnecessary and insecure services, protocols and functionality must be disabled (e.g.: scripts, drivers, features, subsystems, file systems, and unnecessary web servers).
- System security parameters must be configured to prevent misuse.
- The University Of Waikato must establish a process to identify newly discovered security vulnerabilities, and standards must be updated to address these.
- Software applications must be based on industry best practices and incorporate information security throughout the software development life cycle.

9. Information Security Incident Management

9.1 Reporting Information Security Events and Weaknesses

To ensure Information security events and weaknesses associated with the University Of Waikato's data and systems are communicated in a manner allowing timely corrective action to be taken - formal event reporting and escalation standards must be in place.

9.1.1 Reporting Information Security Events and Weaknesses

- Implement an incident response plan, and ensure this plan outlines users' roles and responsibilities.

9.2 Management of Information Security Incidents and Improvements

To ensure a consistent and effective approach is applied to the management of the University of Waikato Information security incidents, responsibilities and standards must be in place to handle Information security events and weaknesses effectively once they have been reported.

9.2.1 Responsibilities and Standards

- The University Of Waikato must assign to an individual or team the responsibility for documenting and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.
- An incident response plan must be implemented - and executed in the event of a system compromise.
- Ensure this plan addresses (as a minimum as defined in the DR and BCP plan):
  - Specific incident response procedures, business recovery and continuity procedures;
  - Data backup processes;
  - Roles and responsibilities
  - Communication and contact strategies.
- The plan must be tested (at least) biennially.

9.2.2 Learning from Information Security Incidents

- The University Of Waikato must develop process to modify and evolve the incident response plan according to lessons learned - and to incorporate industry developments.

9.2.3 Collection of Evidence

- The University Of Waikato must enable processes to provide for timely forensic investigation in the event of a compromise.

10. Business Continuity Management

10.1 Information Security Aspects of Business Continuity Management

In the event of system disruption or compromise, it is essential that plans are in place to restore key system and data stores and resume business operations. This business continuity plan should include those activities and considerations necessary to protect sensitive University of Waikato information during this process.

Business Continuity Management for the University is a responsibility of the Assistant Vice Chancellor - Student and Information Services (AVC-SIS). Refer to the University's Critical Event and Business Continuity Policy and the Business Continuity website for further information.

10.1.1 ICT Disaster Recovery

ICT Disaster Recovery (DR) planning is a responsibility of the Director of ITS. Refer to the ITS maintained ICT DR Plan in the ITSD BCP folder in Google Drive. Similarly, Faculties and Divisions who administer their own ICT systems may also have ICT DR Plans stored within their Faculty/Division folder in the University's BCP folder in Google Drive.

11. Compliance

11.1 Compliance with New Zealand or Australian Legal Requirements

To avoid breaching any New Zealand law, statutory, regulatory or contractual obligations - and any Information security requirements - the design, operation, use, and management of the University of Waikato's systems may be subject to statutory, regulatory, and contractual security requirements.

11.1.1 Identification of Applicable New Zealand Legislation

11.1.1.1 Documentation of Requirements

- The University of Waikato must clearly document all information security requirements leveraged upon the organisation through legislation and regulation.
- The University of Waikato must assign management responsibility for these requirements to the Director of ITS.
- Management of these requirements should involve representatives from technical, legal and managerial domains.
- The University of Waikato must ensure that changes to legislative and regulatory information security requirements are followed and any impact on The University of Waikato documented and escalated to the Director of ITS.

11.1.1.2 Information Security Policy, Standards and Procedures

- The University of Waikato must publish, maintain, and disseminate an Information Security Policy.
- The University of Waikato Information Security Policy, Standards and Procedures must ensure that all legislative and regulatory information security requirements are addressed.

11.1.1.3 Review of Policy

- The Information Security Policy must be reviewed at planned and scheduled intervals (at least annually), or if significant changes occur to any relevant systems.
- This policy review must take into account any identified threats and vulnerabilities, and must result in a formal risk assessment being undertaken.

11.1.1.4 Review of Standards and Procedures

- The University of Waikato information security standards and procedures must be reviewed at planned and scheduled intervals (at least annually), or if significant changes occur to any relevant systems.
- Changes to standards and procedures must be subject to The University of Waikato change control process.
- Document versioning should be used to track changes in Standards and Procedures.

11.1.1.5 Third Party Service Providers

- All processors and service providers must maintain and implement policies and procedures to manage connected entities.

11.1.2 Protection of Records

- Restricted data storage must be kept to a minimum.
- The University Of Waikato must develop a data retention and disposal policy.
- Restricted data must not be kept subsequent to authorisation (even if encrypted):
- Visitor logs must be retained for a minimum of three months (unless otherwise restricted by law).
- Assessment trail history must be kept for at least one year - with a minimum of three months online availability.

11.1.3 Prevention of Misuse of Information Processing Facilities

- The University Of Waikato must disable all unnecessary and insecure services and protocols.
- System security parameters must be configured to prevent misuse.

11.2 Compliance with the Information Security Policy, Framework and Standards, and Technical Compliance

To ensure the compliance of all systems with the Policy, this framework, and all relevant standards and procedures - the security of the University of Waikato systems must be regularly reviewed.

11.2.1 Compliance with the Information Security Policy, Framework, Standards and Procedures

- The University Of Waikato must publish, maintain, and disseminate an Information Security Policy.
- The Information Security Policy, framework and standards must be reviewed at planned and scheduled intervals (at least annually), or if significant changes occur to any relevant systems.
- This policy review must take into account any identified threats and vulnerabilities, and must result in a formal risk assessment being undertaken.
- All processors and service providers must maintain and implement policies and procedures to manage connected entities.

11.2.2 Technical Compliance Checking

11.2.2.1 Creation of a Testing Schedule

- The University of Waikato must review security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorised access attempts.
- This annual schedule must be supplemented by additional scheduled testing and review on significant systems change or deployment.

11.2.2.2 Vulnerability Scanning

- The results of all vulnerability scans must be reviewed.

11.2.2.3 Penetration Testing

- Penetration tests must be performed at least annually and after any significant infrastructure or application upgrade or modification.
- Penetration testing must be conducted by a competent penetration tester.
- If penetration testing is conducted by a member of The University of Waikato staff, they must be sufficiently removed from the design, implementation and operational support of the system under test. This will allow the testing to be objective.

11.2.2.4 Information Systems Audit

- All of The University of Waikato information security processes should be subject to audit to ensure compliance across the organisation and suitability for purpose.

11.2.2.5 Classification of Results

- All security testing should result in a list of identified issues.
- Each identified issue must be assessed to determine the following:
  - Impact on The University of Waikato systems
  - The Risk posed
  - Remediation requirements
  - Remediation cost
- This process must be completed in accordance with The University of Waikato Vulnerability Management standard.

11.2.2.6 Remediation and Escalation

- All identified issues must be remediated or escalated to the Director of ITS.
- Escalated issues must be included in The University of Waikato risk register.
- Upon remediation, all issues must be retested to ensure that they have been resolved and no additional security vulnerabilities were introduced as part of the remediation process.
- This process must be completed in accordance with The University of Waikato Vulnerability Management standard.

Appendix A: Information Security Responsibilities Matrix

	Controls\Clauses		ITS	Division\Faculty	Management
1	Information Security Policy	Document	S		P
		Ownership			P
		Review	P	S	S
2	The Organization of security	Information Security Co-ordination	P	S	
		Information Security activities	P	S	
		On-going Information Security Activities	P	S	
		Information Security Risk Management	P		
		Authorisation Process for Information Processing Systems	P	S	
		Contractual Requirements	P	S	S
		Incidents and Contact with External Authorities	P		S
		Review of Information Security	P	S	S
		Service Delivery (external parties)	P	S	
		Establish Firewall Configuration Standards	P		
3	Asset Management	Asset Inventory	P	S	
		Securing the Asset Lifecycle	P	S	
		Acceptable Use of Assets	S	S	P
		Information labelling and Classification	P	S	S
4	Human Resources Security	Roles and Responsibilities		S(HR)	P
		Background Screening and Checking		P(HR)	
		Terms and Conditions of Employment		P(HR)	S
		Management Responsibilities			P
		Information Security Awareness, Education, and Training	P	S	
		Termination Responsibilities	S	P	
		Removal of Access Rights	P	S	

	Controls\Clauses		ITS	Division\Faculty	Management
5	Physical and Environmental Security	Physical Security Perimeters	P	S (FMD)	
		Physical Entry Controls	P	S (FMD)	
		Physical Security Obligations and Incidents	P	S (FMD)	
		Secure Systems Configuration and Defence	P	S	
		Security of Equipment On-Premises	P	S	
		Equipment Maintenance	P	P	
		Security of Equipment Off-Premises	P	P	
6	Communications and Operations Management	Documented Operating Standards	P	S	
		Change Control Management	P	S	
		Separation of Development, Test and Production Facilities	P	P	
		Monitoring and Review of Third Party Services	P	P	
		Capacity Management	P	P	
		System Acceptance	P	P	
		Controls against Malicious Code	P	P	
		Information Backups	P	P	
		Network Controls	P	S	
		Management of Media	P	P	
		Media Handling	P	P	
		Disposal of Media	P	P	
		Information Handling Standards	P	P	
		Exchange Agreements	P	P	
		Physical Media in Transit	P	P	
		Electronic Messaging	P	P	
		E-Commerce and On-Line Transactions	P	P	
		Assessment Trails	P	S	
		Monitoring System Use	P	S	
		Protection of Log Information	P	S	
		Clock Synchronisation	P	S	

	Controls\Clauses		ITS	Division\Faculty	Management
7	Access Control	Access Control Standards	P	S	
		User Registration	P	P	
		Privilege Management	P	P	
		User Password Management	P		
		Review of User Access Rights	P	S	
		Unattended User Equipment	P	S	
		Network Connection Control	P		
		Network Routing Control	P		
		Systems Configuration and Monitoring	P	P	
		Provision of Devices (Mobility)	P	P	
		Liability, Storage and Insurance (Mobility)	P	P	
		Device Usage (Mobility)	P	S	
		Remote Access Governance and Management	P		
		Configuration and Operation (Mobility)	P	S	
8	Information Systems Acquisition, Development and Maintenance	Operating Standards	P	P	
		Change Control Management	P	S	
		Separation of Development, Test and Production Facilities	P	P	
		Third Party Agreements	P	P	
		Monitoring and Review of Third Party Services	P	P	
		Capacity Management	P	S	
		Systems Design	P	P	
		System Development	P	P	
		System Acceptance	P	P	
		Use of Cryptographic Controls	P	S	
		Cryptographic Key Management	P	P	
		Technical Review of Applications after Operating System Changes	P	P	
		Vulnerability Awareness	P	S	
		Systems Development and Vulnerability Assessment	P	P	
		Patching	P	P	

	Controls\Clauses		ITS	Division\Faculty	Management
		Systems Configuration and Build	P	P	
		Mobile and Malicious Code	P	P	
		Control of Technical Vulnerabilities	P	P	
9	Information Security Incident Management	Reporting Information Security Events and Weaknesses	P	S	
		Responsibilities and Standards	P	S	
		Learning from Information Security Incidents	P	S	
		Collection of Evidence	P	S	
10	Business Continuity Management	Information Security Aspects of Business Continuity	P	S	P
		ICT Disaster Recovery	P	S	
11	Compliance	Identification of Applicable New Zealand Legislation	S		P
		Protection of Records	P	S	
		Prevention of Misuse of Information Processing Facilities	P	S	
		Compliance with the Information Security Policy, Framework, Standards and Procedures	P		
		Technical Compliance Checking	P	S	

Legend:
P = Primary Responsibility
S= Secondary Responsibility

Appendix B: Glossary and Definitions

For the purposes of this document, the following terms and definitions apply.

NOTE 1: A term in a definition or note which is defined elsewhere in this clause is indicated by boldface followed by its entry number in parentheses. Such a boldface term can be replaced in the definition by its complete definition. For example:

attack is defined as "attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an **asset**";

asset is defined as "any item that has value to the organisation".

If the term "**asset**" is replaced by its definition:

attack then becomes "attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of any item that has value to the organisation".

access control
means to ensure that access to **assets** is authorized and restricted based on business and security requirements

accountability
assignment of actions and decisions to an entity

analytical model
algorithm or calculation combining one or more **base** and/or **derived measures** with associated decision

asset
anything that has value to the organisation

NOTE: There are many types of assets, including:

information;
software, such as a computer program;
physical, such as computer;
services;
people, and their qualifications, skills, and experience; and
intangibles, such as reputation and image.

attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an **asset**

attribute
property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means

audit scope
extent and boundaries of an audit

authentication
provision of assurance that a claimed characteristic of an entity is correct

authenticity
property that an entity is what it claims to be

availability
property of being accessible and usable upon demand by an authorized entity

base measure
measure defined in terms of an **attribute** and the method for quantifying it

NOTE: A base measure is functionally independent of other measures.

business continuity
procedures and/or **processes** for ensuring continued business operations

confidential data
a generalized term that typically represents data classified as **restricted**, according to the data classification scheme defined in this standard. This term is often used interchangeably with **sensitive data**.

confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or **processes**

conformity
fulfilment of a requirement

NOTE: The term "conformance" is synonymous but deprecated.

consequence
outcome of an **event** affecting objectives

NOTE 1: An event can lead to a range of consequences.

NOTE 2: A consequence can be certain or uncertain and in the context of information security is usually negative.

NOTE 3: Consequences can be expressed qualitatively or quantitatively.

NOTE 4: Initial consequences can escalate through knock-on effects.

control
means of managing **risk**, including **policies**, **procedures**, **guidelines**, practices or organisational structures, which can be of administrative, technical, management, or legal nature

NOTE 1: Controls for information security include any process, policy, procedure, guideline, practice or organisational structure, which can be administrative, technical, management, or legal in nature which modify information security risk.

NOTE 2: Controls may not always exert the intended or assumed modifying effect.

NOTE 3: Control is also used as a synonym for safeguard or countermeasure.

control objective
statement describing what is to be achieved as a result of implementing **controls**

corrective action
action to eliminate the cause of a detected **non-conformity** or other undesirable situation

critical employee-facing technologies
the PCI (Payment Card Industry) Data Security Standard (DSS) defines these to include, but not limited to, "remote access, wireless network, removable electronic media, laptops, handheld devices, email and Internet". So, basically any technology an employee, or contractor, uses to access restricted data.

data
institutional data, or University information **asset**

NOTE: Within the context of ISO/IEC 27004:2009 data is defined as a collection of values assigned to **base measures**, **derived measures** and/or **indicators**.

data custodian
a senior-level employee of the University who oversees the lifecycle of one or more sets of **institutional data**. See the University's Corporate Data Management Policy for more information.

decision criteria
thresholds, targets, or patterns used to determine the need for action or further investigation, or to describe the level of confidence in a given result

derived measure
measure that is defined as a function of two or more values of **base measures**

effectiveness
extent to which planned activities are realized and planned results achieved

efficiency
relationship between the results achieved and the resources used

elevated privileges
defined as roles or permissions that – if misused or compromised – could allow a person to exploit the University systems for his or her own gain or illicit purpose .

event
occurrence or change of a particular set of circumstances

NOTE 1: An event can be one or more occurrences, and can have several causes.

NOTE 2: An event can consist of something not happening.

NOTE 3: An event can sometimes be referred to as an "incident" or "accident".

external context
external environment in which the organisation seeks to achieve its objectives

NOTE: External context can include:

the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;

key drivers and trends having impact on the objectives of the organisation; and

relationships with, and perceptions and values of, external stakeholders.

guideline
description that clarifies what should be done and how, to achieve the objectives set out in **policies**

idle session
No user inputs such as key strokes, mouse movements and clicks etc. for a certain period of time.

indicator
measure that provides an estimate or evaluation of specified **attributes** derived from an **analytical model** with respect to defined **information needs**

information need
insight necessary to manage objectives, goals, risks and problems

information processing facilities
any information processing system, service or infrastructure, or the physical locations housing them

information security
preservation of **confidentiality, integrity** and **availability** of information

NOTE: In addition, other properties, such as **authenticity, accountability, non-repudiation** and **reliability** can also be involved.

information security event
identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant

information security incident
single or a series of unwanted or unexpected **information security events** that have a significant probability of compromising business operations and threatening **information security**

information security incident management
processes for detecting, reporting, assessing, responding to, dealing with, and learning from **information security incidents**

information security management system
ISMS
part of the overall **management system** based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve **information security**

NOTE: The management system includes organisational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

information system
application, service, information technology asset, or any other information handling component

institutional data
all **data** owned or licensed by the University

integrity
property of protecting the accuracy and completeness of **assets**

internal context
internal environment in which the organisation seeks to achieve its objectives

NOTE: Internal context can include:

governance, organisational structure, roles and accountabilities;

policies, objectives, and the strategies that are in place to achieve them;

the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);

information systems, information flows and decision-making processes both formal and informal);

relationships with, and perceptions and values of, internal stakeholders;

the organisation's culture;

standards, guidelines and models adopted by the organisation; and

form and extent of contractual relationships.

ISMS project
structured activities undertaken by an organisation to implement an **ISMS**

level of risk
magnitude of a **risk** expressed in terms of the combination of **consequences** and their **likelihood**

likelihood
chance of something happening

management
coordinated activities to direct and control an organisation

management system
framework of **guidelines, policies, procedures, processes** and associated resources aimed at ensuring an organisation meets its objectives

measure
variable to which a value is assigned as the result of **measurement**

NOTE: The term "measures" is used to refer collectively to base measures, derived measures, and indicators.

measurement
process of obtaining information about the **effectiveness** of **ISMS** and **controls** using a **measurement method,** a **measurement function,** an **analytical model** and **decision criteria**

measurement function
algorithm or calculation performed to combine two or more **base measures**

measurement method
logical sequence of operations, described generically, used in quantifying an **attribute** with respect to a specified **scale**

NOTE: The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished:

subjective: quantification involving human judgment;

objective: quantification based on numerical rules**.**

measurement results
one or more **indicators** and their associated interpretations that address an **information need**

non-conformity
non-fulfilment of a requirement

non-public information
any information that is classified as **private** or **restricted** Information according to the data classification scheme defined in this document

non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

object
item characterized through the **measurement** of its **attributes**

off-site mobile device
university owned mobile devices including, but not restricted to, mobile phones, smartphones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers, and other portable Internet connected devices.

policy
overall intention and direction as formally expressed by **management**

preventive action
action to eliminate the cause of a potential **non-conformity** or other undesirable potential situation

private data
data should be classified as **private data** when the unauthorized disclosure, alteration or destruction of that **data** could result in a moderate level of **risk** to the University or its affiliates. By default, all **institutional data** that is not explicitly classified as **restricted data** or **public data** should be treated as **private data**. A reasonable level of security **control**s should be applied to **private data.**

procedure
specified way to carry out an activity or a **process**

process
set of interrelated or interacting activities which transforms inputs into outputs

public cloud
as opposed to 'private cloud', the **public cloud** is where cloud service providers make resources and services available to the general public. The public shared service model means that data is collocated with the data of other public users and is thus generally less secure. Security is reliant on the controls implemented by the public cloud service provider.

public data
data should be classified as **public data** when the unauthorized disclosure, alteration or destruction of that **data** would result in little or no **risk** to the University and its affiliates. Examples of **public data** include press releases, course information and research publications. While little or no **control**s are required to protect the **confidentiality** of **public data**, some level of **control** is required to prevent unauthorized modification or destruction of **public data**.

record
document stating results achieved or providing evidence of activities performed

reliability
property of consistent intended behaviour and results

removable media
media or devices that is readable and/or writable by the end user and are able to be moved from computer to computer without physical modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players, smartphones, tablets and PDAs; portable hard drives (including USB hard drives and hard drive-based MP3 players); optical disks such as CD and DVD disks; backup tapes and floppy disks.

residual risk
risk remaining after **risk treatment**

NOTE 1: Residual risk can contain unidentified risk.

NOTE 2: Residual risk can also be known as "retained risk".

restricted data
data should be classified as **restricted data** when the unauthorized disclosure, alteration or destruction of that **data** could cause a significant level of **risk** to the University or its affiliates. Examples of **restricted data** include **data** protected by government privacy regulations and **data** protected by **confidentiality** agreements. The highest level of security **control**s should be applied to **restricted data**.

review
activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives

review object
specific item being reviewed

review objective
statement describing what is to be achieved as a result of a review

risk
effect of uncertainty on objectives

NOTE 1: An effect is a deviation from the expected — positive and/or negative.

NOTE 2: Objectives can have different aspects (such as financial, health and safety, information security, and environmental goals) and can apply at different levels such as strategic, organisation-wide, project, product and process).

NOTE 3: Risk is often characterized by reference to potential **events** and **consequences** or a combination of these.

NOTE 4: Information security risk is often expressed in terms of a combination of the consequences of an information security event and the associated **likelihood** of occurrence.

NOTE 5: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 6: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation.

risk acceptance
decision to accept a **risk**

risk analysis
process to comprehend the nature of **risk** and to determine the **level of risk**

NOTE 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

NOTE 2: Risk analysis includes risk estimation.

risk assessment
overall **process** of **risk identification, risk analysis** and **risk evaluation**

risk communication and consultation
continual and iterative processes that an organisation conducts to provide, share or obtain information, and to engage in dialogue with **stakeholders** regarding the management of **risk**

NOTE 1: The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk.

NOTE 2 Consultation is a two-way process of informed communication between an organisation and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is:

a process which impacts on a decision through influence rather than power; and

an input to decision making, not joint decision making.

risk criteria
terms of reference against which the significance of **risk** is evaluated

NOTE 1 Risk criteria are based on organisational objectives, and external and internal context.

NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.

risk evaluation
process of comparing the results of **risk analysis** with **risk criteria** to determine whether the **risk** and/or its magnitude is acceptable or tolerable

NOTE Risk evaluation assists in the decision about risk treatment.

risk identification
process of finding, recognizing and describing **risks**

NOTE 1 Risk identification involves the identification of risk sources, events, their causes and their potential consequences.

NOTE 2 Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.

risk management
coordinated activities to direct and control an organisation with regard to **risk**

risk management process
systematic application of management **policies procedures** and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing **risk ,**

NOTE ISO/IEC 27005 uses the term 'process' to describe risk management overall. The elements within the risk management process are termed 'activities'

risk treatment
process to modify **risk**

NOTE 1: Risk treatment can involve:

avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;

taking or increasing risk in order to pursue an opportunity;

removing the risk source;

changing the likelihood;

changing the consequences;

sharing the risk with another party or parties (including contracts and risk financing); and

retaining the risk by informed choice.

NOTE 2: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction".

NOTE 3: Risk treatment can create new risks or modify existing risks.

scale
ordered set of values, continuous or discrete, or a set of categories to which the **attribute** is mapped

NOTE: The type of scale depends on the nature of the relationship between values on the scale. Four types of scale are commonly defined:

nominal: the measurement values are categorical;

ordinal: the measurement values are rankings;

interval: the measurement values have equal distances corresponding to equal quantities of the attribute;

ratio: the measurement values have equal distances corresponding to equal quantities of the attribute, where the value of zero corresponds to none of the attribute.

These are just examples of the types of scale.

security implementation standard
document specifying authorized ways for realizing security

sensitive data
a generalized term that typically represents **data** classified as **restricted**, according to the data classification scheme defined in this document. This term is often used interchangeably with **confidential data**

service provider
any **third party** who provides services under contract to the University

stakeholder
person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity

statement of applicability
documented statement describing the **control objectives** and **controls** that are relevant and applicable to the organisation's **ISMS**

system components
any devices (such as servers, routers, switches, wireless Access Points, storage, etc.) other than end user devices

third party
person or body that is recognized as being independent of the parties involved, as concerns the issue in question

threat
potential cause of an unwanted incident, which may result in harm to a system or organisation

unit of measurement
particular quantity, defined and adopted by convention, with which other quantities of the same kind are compared in order to express their magnitude relative to that quantity

validation
confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

verification
confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

NOTE: This could also be called compliance testing.

vulnerability
weakness of an **asset** or **control** that can be exploited by one or more **threats**