Information Security Policy

Governance Policy

1 Purpose

The purpose of this policy is to ensure that the University's information assets are secured to the appropriate degree. These information assets are of significant value to the University. If they are not available when needed or are improperly disclosed, the University could incur serious financial loss or loss of reputation. Additionally, New Zealand legislation requires that the University protect student and staff privacy.

Access to and sharing of knowledge are of high value to the University. Therefore, this policy is also intended to ensure that the appropriate degree of access to and sharing of information assets will occur, and that academic freedom is preserved.

2 Organisational Scope

This is a University-wide policy.

3 Definitions

For purposes of this policy, unless otherwise stated, the following definitions shall apply:

Information Asset: Information assets are data, information, knowledge, or expertise in any form. They may include financial, operational, or scientific information; student, staff or stakeholder related information; or strategies, processes, or research and development.

Information Owner: The information owner is generally the person responsible for the function, process or project that collects, processes or creates information.

Information Security: Assurance that the confidentiality, integrity and availability of information assets are maintained to the appropriate degree.

Information Security Officer: The person responsible for establishing, maintaining, and ensuring compliance with the University-wide information security standards, procedures and guidelines that support the Information Security Programme.

Confidentiality: The protection of sensitive or private information assets from unauthorised disclosure.

User: Anyone using any Victoria University of Wellington information system.

Integrity: The accuracy, completeness and validity of information. Integrity also means that an information asset has not been modified without authorisation.

Availability: The state of an information asset being accessible by those individuals or systems authorised to access it when needed.

Privacy: As defined in the Privacy Act 1993.

Threat: Anything that could adversely affect an information asset.

Vulnerability: A weakness or practice that may allow a threat to affect an asset.

Risk: The potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset.

Controls: Policies, procedures, practices, devices, configurations etc. designed to mitigate potential loss.

Risk Assessment: A systematic process for identifying the degree of risk to an asset. Assets are identified and their value assessed, threats are quantified, vulnerabilities are documented, potential consequences of a loss are described, and a determination of resulting risk and commensurate controls is produced.

4 Policy Content and Guidelines

4.1 Information Security Governance

(a) The Information Security and Risk Committee shall oversee an information security programme, which shall include information security strategy, principles, policy, objectives, and other relevant components.

(b) The programme shall include means of ensuring that stakeholders within the University are involved in decisions relating to information security.

(c) The programme shall include means for ensuring effective communication in support of information security.

(d) Management shall allocate sufficient resources and staff attention to adequately address information security.

4.2 Information Asset Classification and Management

(a) All University information assets shall be classified according to the University Information Classification Standard (see Appendix A).

(b) All University information assets shall have an identified information owner and shall be managed and handled in accordance with the classification standard and related standards, procedures and guidelines.

4.3 Roles and Responsibilities

4.3.1 Users

(a) Information security is every user’s responsibility, and it is the user’s obligation to understand their specific responsibilities for information security.

(b) Users are required to abide by the Acceptable Use Policy. Central service units, schools or faculties may have additional acceptable use policies for their own purposes.

4.3.2 University Management

(a) Managers are responsible for promoting security as a part of standard operating procedures.

(b) Managers are responsible for ensuring the prompt adjustment of appropriate system permissions when changes to a user's role or status occur.

4.3.3 Information Owner

(a) The information owner is responsible for:

(i) determining the value of the information;

(ii) classifying the information according to the classification standard;

(iii) deciding who can access the information;

(iv) ensuring that risk assessments for the information assets are performed;

(v) ensuring that appropriate controls are in place.

(b) These responsibilities may not be delegated by the information owner.

Note: The information owner may seek advice and assistance in carrying out these responsibilities.

4.3.4 Information Security Officer

(a) The Information Security Officer is responsible for establishing and maintaining University-wide information security standards, procedures and guidelines that support the Information Security Programme.

(b) The Information Security Officer is authorised to review any aspect of any University information system for the purposes of ensuring the security of University information assets.

(c) The Information Security Officer is responsible for providing advice and guidance to information owners when exercising their responsibilities.

4.4 Information Security and Risk Management

(a) Information security risks shall be managed consistently with classification levels, and according to information security standards.

(b) Risk shall be managed in accordance with the University's Risk Management Policy and the AS/NZS ISO/IEC 27001:2006 and 27002:2006 standards.

(c) Acceptable levels of risk shall be defined in terms of maximum acceptable loss, and reviewed and approved by senior management at least annually.

(d) Compliance with the information security programme and related policy, standards and procedures shall be verified through periodic internal and external reviews by information security specialists.

4.5 Access to Information Assets

(a) Physical and electronic access to University information assets shall be consistently controlled in a manner appropriate with the assets' classification, and access privileges of all users shall be defined based on their assigned roles and demonstrated need for access.

(b) Access privileges shall be granted only with appropriate authorisation by the information owner.

4.6 Information Security Awareness and Training

Information security awareness and training relevant to each person's role shall be provided to all University staff, students or other users. Periodic updated training shall also be provided.

4.7 Operation of Information Systems

(a) New information systems shall conform to information security standards before being installed into any production environment.

(b) Information security standards and requirements shall be included in product specifications during the procurement process.

(c) Information systems infrastructure and operating procedures shall be documented, managed and maintained so as to ensure conformance with information security standards.

(d) All third party service providers and agents with access to any University information asset shall comply with all regulatory, legal, and contractual requirements, including University statutes and policy documents.

(e) When changes are made to systems that may affect the security of information assets, risks shall be assessed, and the system must subsequently conform to information security standards.

4.8 Incident Management and Response

(a) An information systems disaster recovery plan shall be developed, maintained and tested in a manner that ensures the ability of the University to continue operations as required by the University business continuity plan.

(b) Security incident reporting and response procedures shall be developed and maintained by the Information Security Officer, and published and accessible as appropriate. Users shall be informed of procedures relevant to them.

4.9 Physical Security

The Information Security Policy applies to information assets regardless of their media (for example, printed records and paper forms as well as electronically saved documents).

4.10 Privacy Expectations

At any time and without prior notice, University management reserves the right to monitor, access, inspect or disclose any information stored on or transmitted through University information systems. The users' rights to privacy will be respected and disruption to the users' legitimate activities avoided where possible.

5 Legislative Compliance

The University is required to manage its policy documentation within a legislative framework. The legislation directing this policy is the:

Copyright Act 1994

Official Information Act 1982

Privacy Act 1993

Public Records Act 2005

6 References

Information Systems Statute

Risk Management Policy

Acceptable Use Policy (under development)[1]

Victoria University Information Security Policies, Standards, Procedures and Guidelines (under development)

AS/NZS ISO/IEC 27001:2006 Information Technology - Security Techniques - Information Security Management Systems - Requirements

AS/NZS ISO/IEC 27002:2006 Information Technology - Security Techniques - Code of Practice for Information Management

7 Appendices

Appendix A: Victoria University Information Classification Standard

8 Approval Agency

Vice-Chancellor

9 Approval Dates

This policy was originally approved on:	15 April 2009
This version was approved on:	15 April 2009
This version takes effect from:	15 April 2009
This policy will be reviewed by:	15 April 2012

10 Policy Sponsor

Director, Information Technology Services

11 Contact Person

The following person may be approached on a routine basis in relation to this policy:

Derek Nelson
Information Security Officer
Ext: 6257

[1] In the interim, refer to the Student Conduct Statute.