Cyber Security Procedures

To be read in conjunction with the Information and Records Management and Security Policy

1 Purpose

These Procedures should be read in conjunction with the University's Information and Records Management and Security Policy.

The University's Information Assets are of significant value to the University. If they are insecure, lost, inaccessible, improperly disclosed or changed, the University could incur financial or reputational loss. We are required by legislation to protect student and staff Privacy, University records, data, and copyrights and in some cases are contractually bound to protect University information in specific ways.

These Procedures acknowledge that access to and sharing of knowledge is of high value to the University and ensures sharing of Information Assets can occur and academic freedom is preserved.

2 Organisational Scope

These are University-wide Procedures.

3 Definitions

Availability	The state of an Information Asset being accessible by those individuals or systems authorised to access it when needed.
Administrative Systems	Software and hardware maintained by a unit or collection of units on behalf of the entire University, are focused toward the collective needs of units across campus, and directly serves a core function of the University.
Cloud Computing	This refers to information services that are provided from a service company based on the Internet. Typically, these services are purchased to replace or augment corporate information services. These services are defined as software, platform or infrastructure.
Controls	Policies, procedures, practices, devices, configurations etc. designed to mitigate potential loss.
Confidentiality	The protection of sensitive or private Information Assets from unauthorised disclosure.
Information Security Classification	Determines the confidentiality of the material contained within a document or system.

	The information classification of a document may change throughout its lifecycle, however the information classification of data contained in a business information system is less likely to change throughout its lifecycle.
Information Security Classification - Confidential	Sensitive information, which, if disclosed inappropriately, could cause significant harm to the reputation of the University or individuals, or expose the University to liability. This includes all private data and sensitive information about University staff and or students. Confidential information should be accessible to authenticated users only, who have explicit approval from their Manager to access this information.
Information Security Classification - Internal Use Only	Information which, if disclosed inappropriately, could harm the reputation of the University or individuals or cause embarrassment. Staff or students may suffer inconvenience. Accessible to authenticated users only.
Information Security Classification – Public	Information developed for public use, by the University and needs no classification label. Disclosure of this information will not cause harm to the University or members of the University Community. Accessible to the public.
Information	Information, whether in its original form or otherwise, including (but not exclusively) documents, a signature, a seal, text, images, sound, speech, or data compiled, recorded or stored in in any format (paper, electronic files, databases, texts, social media etc)
Information Asset	Includes data, information, knowledge, or expertise in any form. May include financial, operational, or scientific information; student, staff or stakeholder related information; or strategies, processes, or research and development.
Information Integrity	The accuracy, completeness and validity of information. Information Integrity also means that an Information Asset has not been modified without authorisation.
Information Owner	A University employee who has the accountability for information of a specific type.
Information Security	Assurance that the sensitivity, Information Integrity and Availability of Information Assets are maintained to the appropriate degree.
Information Security Incident	Attempted or actual unauthorised access, use, disclosure, modification or destruction of Information, Information Assets or interference with Information Systems or operations.
Information Systems	Any computer system, telephone or peripherals owned or administered by the University, together with any associated electronic or mobile data storage systems; and any communication devices, wired or wireless network intended for the transfer of information, whether on University campuses or to which Users have access through University facilities, including the Internet.
Privileged Account	Administrator rights, otherwise known as administrator access, admin rights or privileged access, allow a User to have permissions to install, uninstall software and change configuration settings. Administration rights can be delegated to Users on a single machine, a group of machines, domain or enterprise wide. This includes accounts with the name of admin, administrator, root or prefixed with ADM.
Risk	The potential that a given Threat will exploit vulnerabilities to cause loss or damage to any University information or technology asset.
Risk Assessment	A systematic process for identifying the degree of Risk to an Information or Technology 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.
Security Manager	The person delegated by the Director, Digital Solutions, who is responsible for establishing, maintaining, and ensuring compliance with the Information and Records Management and Security Policy, and Procedures that support the Information Security Programme.
Threat	Anything that could adversely affect an Information Asset.
User	Anyone using any University information system.
Vulnerability	A weakness or practice that may allow a Threat to affect an Information Asset.

4 Procedures

4.1 Information Security Governance and Risk Management

a. The Information Security Programme will be overseen by the Audit and Risk Committee. The Programme will include an information security strategy, principles, policies, objectives, and other relevant components.

b. The Programme will:

i. Ensure that stakeholders within the University are involved in decisions relating to information security.

ii. Ensure effective communication in support of information security.

iii. Be verified through periodic internal and external reviews by information security specialists to ensure compliance with the Information Security Programme and industry best practices.

iv. Information security Risks will be managed consistently with information security classification levels, and according to Cyber Security Procedures.

v. Ensure Risk will be managed in accordance with the University's Risk Management Policy and the AS/NZS ISO/IEC 27001:2013 and 27002:2013 Procedures.

vi. Define acceptable levels of Risk in terms of maximum acceptable loss which are reviewed and approved by the Information Security and Risk Committee at least annually.

vii. Provide Information security awareness and training to all University staff, students or other Users. Periodic additional training will also be provided.

4.2 Roles and Responsibilities

4.2.1 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 must abide by all University policies, procedures, including the Acceptable Use of Information Systems Statute.

c. Access rights to University Information Systems must only be used for official University purposes.

d. Users are required to complete annual Security Awareness eLearning.

e. Users must report all information security incidents to the Digital Solutions Service Desk (extn 5050).

f. Users must keep confidential information in either paper or electronic format secure at all times.

4.2.2 Management

a. Managers are responsible for promoting information and records security as a part of standard operating procedures.

b. Managers must regularly review staff compliance with the Information Management Policy and the security Procedures.

c. Managers must include security requirements in vendor agreements and regularly review vendor security compliance.

d. Managers must ensure the prompt adjustment of appropriate system permissions when changes to a User's role or status occur.

4.2.3 Information Owner

a. The Information Owner is responsible for and must:

i. Determine the value of the information;

ii. Classify the information according to the Information Classification Scheme;

iii. Decide who can access the information;

iv. Ensure that Risk Assessments for the Information Assets are performed;

v. Ensure that appropriate Controls are in place.

b. Information and Records Owners must consult the University Security Manager regarding the management of University records and information related to University branded websites and confidential information.

4.2.4 The University Security Manager

a. Is responsible for establishing and maintaining the University Information Security Programme.

b. Is responsible for establishing, maintaining, and ensuring compliance with the University-wide Information and Records Management and Security Policy all procedures that support the Information Security Programme.

c. Manages the University Information Security Programme in accordance with AS/NZS ISO/IEC 27001:2013, 27002:2013 Procedures.

d. Is authorised to review any aspect of any University information system for the purposes of ensuring the security of University Information Assets.

e. Will maintain these Procedures and provide advice on relevant procedures and guidelines overseen by other units within the University.

f. Will create an annual information security plan defining information security objectives.

4.3 Remote Work

a. Information and Records with an Information Security Classification of "Confidential" and "Internal Use" may be accessed and processed on personal home computers or devices provided that:

i. Access is restricted so that only the staff member can access the information;

ii. If stored for more than one day, the information will be encrypted.

iii. All personal devices must have in-support operating systems, updated patches, antivirus software and be physically secured from theft or unapproved access.

iv. The information is wiped from the device as soon as is practically possible, including all downloaded files.

b. All remote access to the University must be through the Digital Solutions provided VPN and must make use of Multifactor Authentication (MFA). Exceptions must be approved by the Digital Solutions Security Team.

4.4 Access Control and User Account Management

a. Physical and electronic access to University Information Assets will be consistently controlled in a manner appropriate with the assets' Information Security Classification, and access privileges of all Users will be defined based on their assigned roles and demonstrated need for access.

b. Access privileges will be granted only with appropriate authorisation by the Information Owner.

c. Access to University systems or devices will be controlled, at a minimum, through the use of a uniquely owned credential with password or PIN, or as determined by the University Security Manager.

d. All devices with access to University "Confidential" and "Internal Use" information, must be secured with at least a four digit access PIN, or as determined by the University Security Manager and must be kept physically secured at all times on and off University premises.

e. Information with an Information Security Classification of "Confidential" must be protected at all times and must not be:

i. Stored unencrypted;

ii. Transported unencrypted; or

iii. Processed (accessed) on public systems, including Internet Cafes or Libraries.

(a) Information with an Information Security Classification of "Internal Use" should be protected at all times and should not be:

i. Stored unencrypted;

ii. Transported unencrypted; or

iii. Processed (accessed) on public systems, including Internet Cafes or Libraries.

4.4.1 User accounts

a. Accounts must adhere to the Digital Solutions Access Control Guideline.

b. Users must not share authentication credentials e.g. passwords or PINs.

c. Privileged Accounts must not be used for the installation of software for personal reasons.

d. Internet browsing and email access must not be performed with Privileged Accounts.

e. Users will only be provided with access to the network and network services that they have been specifically authorised to use.

f. Personal computers or devices brought to the University will only use the University's Bring Your Own Device network.

g. Staff with access to confidential information must not disclose this information unless authorised to do so.

h. Users must be verified for credential access (password changes), access, update or change to confidential information.

i. Staff accounts for all systems must have the following requirements:

   i. Password history- 10
   ii. Maximum password age- 0
   iii. Minimum password age- 0
   iv. Minimum length- 10
   v. Lockout duration- 15min
   vi. Lockout threshold- 10 invalid attempts

j. Student accounts for all systems must have the following requirements:

   i. Password history- 10
   ii. Maximum password age- 0
   iii. Minimum password age- 0
   iv. Minimum length- 8
   v. Lockout duration- 15min
   vi. Lockout threshold- 10 invalid attempts

k. Administrative accounts

   i. Password history- 10
   ii. Maximum password age- 90 days
   iii. Minimum password age- 0
   iv. Minimum length- 14
   v. Lockout duration- 15min
   vi. Lockout threshold- 10 invalid attempts

4.5 University devices

a. Administrative accounts are to be provisioned for local device access. Normal accounts are not to be Local Administrators.

b. Staff are not to be local administrators of their University devices unless approved by Digital Solutions Security.

c. Staff devices must be set to have password protected lock screens automatically applied after 5 minutes of inactivity.

d. Only current, supported and patched versions of software may be installed onto University devices. Exceptions must be approved by the Digital Solutions Security Team.

e. Out of support Operating systems are not allowed onto the production networks such as, Staff, Students etc. They must be placed into an appropriate network zone such as Research, labs or BYOD as directed by the Security Team.

4.6 Physical and environmental security

a. These Cyber Security Procedures apply to Information Assets regardless of their media (for example, printed records and paper forms as well as electronic documents).

b. All University provided devices must be kept physically secured at all times on and off University premises.

c. Servers storing or processing "Confidential" or Internal Use" information must reside in a Victoria University datacentre or preapproved cloud provider.

d. All employees must keep secure, paper and electronic confidential information. Loss of any Information Asset must be reported to the Digital Solutions Service desk.

e. Staff must lock their computer screen when leaving it at all times to prevent unauthorised access.

4.7 Operations security

a. New Administrative Systems must conform to Cyber Security Procedures before being installed into any production environment.

b. Cyber Security Procedures and requirements must be included in product specifications during the procurement process.

c. Information Systems infrastructure and operating procedures must be documented, managed and maintained so as to conform to Cyber Security Procedures.

d. When changes are made to systems that may affect the security of information assets, Risks must be assessed, and the system must subsequently conform to Cyber Security Procedures.

4.8 Vulnerability management

a. Computers and devices must be mitigated, usually through patching, from critical vulnerabilities within 20 business days using vendor or CVSS provided vulnerability ratings. Information owners should use the Digital Solutions Patching Standard.

4.8.1 Timeframes for deployment

Patches released by vendors shall be installed within the below timeframes. All timeframes begin on the vendor's day of the patch release. Vendor recommended security severity shall be used for security timeframe requirements.

a. Feature patches shall be deployed on an as needed basis, at the request of the Information System Owner or provided in service pack updates.

b. Service Packs shall be deployed within six calendar months

c. Security patches shall be deployed –

i. For core business systems

a) Severity Critical and Important/High – 100% within ten business days

b) Severity Moderate – 100% within one calendar month

a. For all other systems

a) Severity Critical and Important/High – 80% within ten business days

b) Severity Moderate – 80% within one calendar month

4.9 System acquisition

4.9.1 Cloud and Internet Services

The University provides facilities for secure transmission, processing and storage of data and information, however it is recognised that there may be instances where staff need to use services in non-University-owned facilities.

a. These services include, but are not limited to:

ii. The New Zealand Government Cloud Programme which offers storage or services on a pay-per-use or subscription basis.

iii. Platform or Software as a Service (PaaS/SaaS) applications which store data in non-University-Owned facilities for example Project Management software, Customer Management Software, Patient Management software, Task Software, Reader Software, iCloud

iv. Infrastructure as a Service (IaaS) environments such as Azure, AWS or Google.

b. Use of Cloud and Internet services must be in compliance with all other University policies and procedures and relevant legislation. It is the responsibility of University staff using such services to ensure that they are aware of, and are fully compliant with all relevant policies, procedures and legislation.

c. All use of Cloud and Internet services, in relation to information classifications: Confidential or Internal Use Only information, must be approved, prior to use, by the Director of Digital Solutions. To ensure proper management, the Director of Digital Solutions will use the University Cloud and Internet Services Guideline.

4.10 Incident Management

a. Information Security incident reporting and response procedures are maintained by the Security Manager.

b. Information Security Incidents must be reported to the Digital Solutions Service Desk (extn. 5050).

c. An information systems disaster recovery plan will 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.

4.11 Monitoring and Access

At any time as authorised by the Director, Digital Solutions appropriate people may monitor, access, inspect or disclose any information stored on or transmitted through University information systems to authorised parties.

5 References

Information and Records Management and Security Policy

Acceptable Use of Information Systems Statute

Risk Management Policy

Student Conduct Statute

AS/NZS ISO/IEC 27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements

AS/NZS ISO/IEC 27002:2013 Information Technology - Security Techniques - Code of Practice for Information Management

6 Document Management and control

Approver	Vice-Chancellor
Approval Date	03.06.2021
Effective Date	03.06.2021
Last Modified	03.06.2021
Review Date	June 2024
Sponsor	Director, Digital Solutions
Contact Person	Architecture and Security Manager, Digital Solutions