IT Security Policy

Section 1 - Purpose / Objectives

(1) This policy:

a. Documents an IT security framework for best operational practice, so that the University is able to minimize risk and respond to IT security risks incidents.
b. Ensures that University IT Security Controls and Governance meet legal and other compliance requirements.
c. Specifies appropriate physical security measures to be used to protect computer systems, personnel, and data and communications systems located in secure locations.
d. Provides the authority for members of Victoria University's IT Security and Assurance team to conduct a security audit on any system of the University.

Section 2 - Scope / Application

(2) This policy applies all students and staff of Victoria University and any person having legitimate business purpose on University property.

(3) This policy applies to all equipment or devices that are owned and/or operated by Victoria University and/or registered in any Domain Name System (DNS) domain owned by Victoria University and any devices that are present on the University premises, but may not be owned or operated by the University.

(4) This policy also covers any host device outsourced or hosted at external/third-party service providers, if that equipment resides in a Victoria University domain or appears to be owned by Victoria University.

Section 3 - Definitions

(5) Nil

Section 4 - Policy Statement

Information Security

(6) Victoria University's reputation is directly linked with the way it manages both information and information systems.

(7) Victoria University is critically dependent on information and information systems. If important information were disclosed to inappropriate persons, the University could suffer from the entire spectrum of risk consequences outlined in the University Risk Management Policy .

(8) Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information must be protected in a manner that is consistent with its

classification, no matter what stage it is at in the life cycle from origination to destruction.

(9) Staff wishing to telecommute must follow all appropriate rules, policies and regulations of the University regarding security and confidentiality of information, including computer data and files security.

(10) Every Victoria University community member who uses computers in the course of their regular job duties will be granted an e-mail address and related privileges. All Victoria University business communications sent by e-mail must be sent and received using this institutional e-mail address.

Change Management

(11) With the exception of emergency situations, all changes to Victoria University IT-based resources including enterprise systems, operating systems, equipment, networks and applications must follow appropriate Change Management processes, and be approved by the appropriate governance body and Information Technology Services.

Information Protection

(12) All equipment and devices owned and/or operated by Victoria University, which is directly accessible from external networks must comply with VU approved firewall and device security configuration guidelines.

(13) ITS may choose to isolate the University network from the rest of the Internet if no protection is available, and an attack is likely or imminent. ITS may isolate any contaminated portion of the University network from the rest of the University as it sees appropriate.

(14) An infected device may be disconnected from the University network until it is cleaned and poses no threat to the rest of the University. An infected device may also be required to be presented for inspection by ITS before reconnection to the University network is permitted.

Access Control

(15) Access to information that is not publicly available must be provided based on a need to know basis. Confidential information must be disclosed only to people who have a legitimate business need for the information. At the same time, access to information must not be restricted unduly.

(16) Victoria University community members are provided with Internet access to perform their duties related to their studies, their job, research or other academic development, but this access may be terminated at any time at the discretion of a community member's supervisor or College Dean.

(17) Physical access to controlled areas containing critical computing equipment is restricted to University staff and authorised visitors who need access as part of their job.

(18) VU equipment, networks and business systems must identify and authenticate VU users by an ITS approved authentication service. Approval via the IT Director must be obtained to use alternate authentication models.

(19) All Victoria University computers that store sensitive and restricted information and that are permanently or intermittently connected to computer networks must have a password-based access control system approved by the Information Technology Services department.

(20) All in-bound session connections to Victoria University computers from external networks must be protected with an approved access control system.

(21) All critical and sensitive information handling activities must take place in areas that are physically secured and protected against unauthorised access, interference, damage and to minimise equipment theft.

ITS Security Audits

(22) Victoria University has the right to conduct and will regularly conduct audits of staff as specified in IT Security Audit Authorities procedure.

(23) All community members who wish to use Victoria University multi-user computer systems must sign a compliance statement prior to being issued a staff or user ID. For staff this is part of their employment conditions. For students this is part of their enrolment form.

External Providers

(24) The responsibility for the security of equipment deployed by external service providers must be clarified in the contract with the service provider and include documentation of security contacts and escalation procedures.

(25) All outsourcing contracts between external providers and Victoria University for services and equipment must comply with the Contracts Policy and Procedures and will include reference to IT Security policies and procedures.

(26) Business Owners will monitor and review external provider services to ensure appropriate security controls are implemented and maintained as specified in the outsourcing contract.

Breach of Policy

(27) Breach of this policy by a staff member could result in a withdrawal of the staff member's access to the University email and computer network as well as other processes under the Enterprise Agreement.

Section 5 - Procedures

(28) IT Security - Information Security (Best Operational Practice) Procedure

(29) IT Security - Internet Filtering Procedure

(30) IT Security - IT Security Audit Authorities Procedure

(31) IT Security - Security Access to Controlled IT Areas Procedure

(32) IT Security - User Access Management Procedure

Section 6 - Guidelines

(33) Firewall Security Guidelines

(34) Device Security Guidelines

(35) IT Security - Virus Protection Procedure and Guidelines

Status and Details

Status	Historic
Effective Date	18th August 2015
Review Date	16th August 2019
Approval Authority	Vice-Chancellor
Approval Date	11th August 2015
Expiry Date	17th December 2019
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020 Information Technology Services