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 computers and communication devices owned or operated by the University and any communications devices that are present on the University premises, but may not be owned or operated by the University.

Section 3 - Definitions

(4) Nil

Section 4 - Policy Statement

Information Security

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

(6) 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 .

(7) 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.

(8) 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.

(9) With the exception of emergency situations, all changes to Victoria University computer networks must be documented in the ITS Change Management system prior to implementation, and be approved by Information Technology Services.

(10) 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.

(11) 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.

(12) 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.

Security Access to Controlled Areas in IT

(13) 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.

(14) 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.

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

(16) 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

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

(18) 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.

(19) 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

(20) See Associated Information tab.

Section 6 - Guidelines

(21) Nil

Status and Details

Status	Historic
Effective Date	6th September 2014
Review Date	6th May 2017
Approval Authority	Vice-Chancellor
Approval Date	6th September 2014
Expiry Date	15th April 2015
Responsible Officer	Tara Dharnikota Chief Information Security Officer Tara.Dharnikota@vu.edu.au
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020

This policy document may be varied, withdrawn or replaced at any time. Printed copies, or part thereof, are regarded as uncontrolled and should not be relied upon as the current version. It is the responsibility of the individual reading this document to always refer to Victoria University's Policy Library for the latest version.