IT Security - Information Security (Best Operational Practice) Procedure

Section 1 - Purpose / Objectives

(1) The purpose of this procedure is to protect Victoria University (VU) information and information systems by providing the University community with a framework for best operational practice so that the University is able to minimise risk and respond quickly to any security risks that may occur.

(2) A member of the University community that interacts with VU systems is defined as one of three types of users:

a. Business Owners
b. Custodians
c. End users

(3) This procedure clarifies the responsibilities of each of these users and the steps they must take to help protect VU information and information systems.

Section 2 - Scope / Application

(4) This procedure applies to all students, staff and contractors employed or engaged by VU.

(5) This procedure applies to all information handled by computers and network systems owned by or administered by VU; and all operating systems, computer form factors, and application systems.

(6) This procedure excludes the security of information handled exclusively via voice and paper.

Section 3 - Definitions

(7) Nil

Section 4 - Policy Statement

(8) Nil

Section 5 - Procedures

Roles/Responsibilities

Roles	Responsibility
(9) Business Owner (Management)	a. Designate the relevant sensitivity classification in accordance with relevant Records Management procedures. b. Designate the appropriate level of criticality. c. Define which users will be granted access d. Approve requests for various ways in which the information will be utilised.
(10) Custodian (IT staff and local administrators)	a. Safeguard the information, including implementing access control systems to prevent inappropriate disclosure. b. Make backups so that critical information will not be lost; as guided by the Business Owner. c. Implement, operate, and maintain the security measures defined by Business Owners.
(11) User (End user of a system)	a. Comply with all VU policies, procedures and standards related to information security. b. Contact the relevant Custodian or Business Owner with any questions about the appropriate handling of a specific type of information. c. Whenever information is maintained only on a personal computer, the User is also a Custodian (see Custodian for responsibilities).

Procedures

(12) All members of the University that are defined as a user of a VU system must follow these guidelines to protect VU information and information systems.

Consistent Handling of VU Information

(13) VU information as well as information that has been entrusted to VU must be protected in a manner relevant to its sensitivity and criticality regardless of what stage it is at in the life cycle from origination to destruction.

(14) 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.

(15) Reference [AS/NZS ISO/IEC 27002:2006, 6.1.3, 7.2.1].

Disclosure of VU Information

(16) Information in the possession of, or under the control of VU must be disclosed only to people who have a legitimate business need for the information.

(17) Community members must not withhold access to information when the Business Owner of the information instructs that it be shared.

(18) The privileges granted to all users must be periodically reviewed by Business Owners and Custodians to ensure that only those with a current need to know presently have access.

(19) Reference [AS/NZS ISO/IEC 27002:2006, 11.2.2].

Unique User ID

(20) Each community member accessing multi-user information systems must have a unique user ID and a private password.

(21) User IDs must be employed to restrict system privileges based on job duties, project responsibilities, and other business activities.

(22) Each University community member is personally responsible for the usage of his or her user ID and password.

(23) Staff User IDs are to be based on employee number.

(24) Student User IDs are to be based on student number.

(25) User IDs for other members of the University community are to be based on their Non-VU Staff card ID.

(26) The person issued with an information system account, identified by their unique user ID, is wholly responsible and accountable for all actions performed with that account.

(27) Reference [AS/NZS ISO/IEC 27002:2006, 11.2.1].

Anonymous access to VU systems

(28) Users are prohibited from logging into any VU system or network anonymously. An example of anonymous access includes the use of 'guest' user IDs.

(29) Exceptions include electronic bulletin boards, Internet sites, intranet sites, and other systems where all regular users are intended to be anonymous.

(30) When users employ system commands that permit them to change active user IDs to gain certain privileges, they must have initially logged on employing user IDs that clearly indicated their identity.

(31) Reference [AS/NZS ISO/IEC 27002:2006 11.2.1].

User Account Security

(32) Keep passwords confidential.

(33) Avoid keeping a paper record of passwords unless this can be stored securely.

(34) Change passwords whenever there is any indication of a possible system or password compromise.

(35) Select quality passwords with a minimum length of eight characters (more are better) which are:

a. easy to remember;
b. not based on anything somebody else could easily guess or obtain using person-related information e.g. names, telephone numbers, and dates of birth etc.;
c. contain at least one lower-case letter, upper-case letter and digit. Optionally a special character should be included;
d. not a derivative of a previous password.

(36) Staff are required to change passwords at least every 60 days.

(37) Students are required to change passwords at least every 180 days.

(38) The system retains 12 previously used passwords, therefore do not reuse passwords.

(39) User requested password changes should be limited to 1 per day.

(40) Change temporary password at the first log-on.

(41) Do not include passwords in any automated log-on process, e.g. stored in a macro or function key.

(42) Do not share individual passwords.

(43) User accounts will become locked and access prevented after 50 invalid log-in attempts. Users will be required to contact Service Desk if their account is locked out and have their password reset.

(44) Reference [AS/NZS ISO/IEC 27002:2006, 11.3.1].

Password Storage

(45) Do not store passwords in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorised persons might discover them.

(46) Passwords must not be written down in some readily decipherable form and left in a place where unauthorised persons might discover them.

(47) Information systems that do store passwords should only store one way cryptographically hashed representation, salted if available.

(48) Reference [AS/NZS ISO/IEC 27002:2006 11.3.1].

Sharing Passwords

(49) Sharing passwords is prohibited.

(50) If users need to share computer-resident data, they must use electronic mail, groupware databases, public directories on local area network servers, manual removable storage exchange and other mechanisms.

(51) System administrators and other technical information systems staff must never ask a worker to reveal their personal password.

(52) The only time a password should be known by another is when it is issued. These temporary passwords must be changed the first time that the authorised user accesses the system.

(53) If a user believes that his or her user ID and password are being used by someone else, the user must immediately notify the Custodian and/or Business Owner for the information system.

(54) Reference [AS/NZS ISO/IEC 27002:2006 11.3.1].

Resetting Passwords

(55) The University may reset passwords and personal identification numbers (PIN) where, in its view, the interests of the University or the staff member so require; for example:

a. the staff member has forgotten his or her password/PIN;
b. or is unavailable to identify his or her password/PIN when required so as to enable the processing of urgent University business;
c. or is on a prolonged absence from the University.

(56) Staff members will be informed that their password/PIN has been reset, and are required to change it again to ensure individual account a security.

Compliance Statement

(57) All community members who wish to use VU multi-user computer systems must sign a compliance statement prior to being issued a staff or user ID.

(58) Staff do this as part of their employment conditions and Students sign on their enrolment form.

(59) Reference [AS/NZS ISO/IEC 27002:2006 8.2.2].

Physical Security to control access to information

(60) Access to every office, computer machine room, and other VU work area containing sensitive or restricted information must be physically restricted to authorised people.

(61) Electronic media (e.g. CDs, diskettes, removable hard disks and USB key must be locked in suitable security storage when not in use.

(62) Staff should lock their computers when leaving their desk, using the automatic screensaver lockout as a fall-back position.

(63) Reference [AS/NZS ISO/IEC 27002:2006 9.1.2, 9.1.3 & 11.3.3].

Connecting to the Internal Network

(64) All VU computers that store and/or process sensitive and restricted information must have a password-based access control system approved by the Information Technology (IT) department.

(65) All other types of computers and devices must employ an automatic lock out feature such as the screen saver passwords that are provided with operating systems, so that after a period of no activity the screen will go blank until the correct password is again entered.

(66) Reference [AS/NZS ISO/IEC 27002:2006 11.3.2, 11.5.5].

Connecting to the External Network

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

(68) When using VU computers, VU users must not establish connections with external networks including Internet service providers or VPN services unless these connections have been approved by the IT department.

(69) All methods of given people or organisations remote access to VU resources must be approved by IT. This includes, but is not limited to, VPN's, remote management/access web services and modems.

(70) Reference [AS/NZS ISO/IEC 27002:2006, 11.4.2 & 11.4.6].

Telecommuting and Information Security

(71) 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 file security.

(72) The staff member must apply approved safeguards to protect records from unauthorised disclosure or damage.

(73) Periodic checking of mail while on the road, or from home is not considered telecommuting, but does require that staff follow the same security precautions.

(74) Reference [AS/NZS ISO/IEC 27002:2006 11.7.1 & 11.7.2].

Access to the Internet

(75) VU community members are provided with Internet access to perform their duties related to their job, research or other academic development.

(76) Internet access may be terminated at any time at the discretion of a community member's supervisor or other relevant University Authority.

(77) Limited personal use is allowed but Internet access is monitored to ensure that community members are not visiting sites that are deemed "objectionable" or "unsuitable for minors", in order to comply with Australian state and federal legislation; and also to ensure that they continue to be in compliance with University policies and procedures.

(78) Community members must take special care to ensure that they do not represent VU on Internet discussion groups and in other public forums unless they have previously received senior management authorisation to act in this capacity.

(79) Community members must not place VU material on any publicly-accessible computer system such as the Internet unless the posting has been approved by the Business Owner.

(80) Sensitive and restricted information, including passwords and credit card numbers, must not be sent across the Internet unless this information is in encrypted form.

(81) Reference [AS/NZS ISO/IEC 27002:2006 8.1.3, 15.1.6].

Electronic Mail (e-mail) Communications

(82) All VU business communications sent by email must be sent and received using the official VU email address.

(83) A personal Internet service provider email account or any other electronic mail address must not be used for VU related business unless a community member obtains senior management approval.

(84) Unsolicited and unauthorised global or commercial email transmissions are prohibited.

(85) All VU community members must refrain from sending credit card numbers, passwords, or other sensitive and restricted information that might be intercepted.

(86) See IT Appropriate Use Policy .

Computer Security Components

(87) All personal computer users must keep the current versions of approved virus screening software enabled on their computers (see http://intranet.vu.edu.au/its/Antivirus/)

(88) Users must not abort automatic software processes that update software, virus signatures or security settings.

(89) University community members must not bypass or turn off security features that could prevent the proper and secure operation of computers at VU.

(90) Reference [AS/NZS ISO/IEC 27002:2006 10.4.1].

Computer Virus Eradication

(91) If University community members suspect infection by a computer virus, they must immediately stop using the involved computer and contact the IT Service Desk.

(92) Removable storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated.

(93) An infected computer must be immediately isolated from internal networks.

(94) Users must not attempt to eradicate viruses themselves.

(95) Qualified VU staff or consultants must complete computer virus eradication tasks in a manner that minimises both data destruction and system downtime.

(96) If there is any doubt that the virus has or can be eradicated the infected system should wiped and reimaged.

(97) Reference [AS/NZS ISO/IEC 27002:2006 10.4.1].

Downloading Software

(98) VU computers and networks must not run software that comes from sources other than VU departments, knowledgeable and trusted user groups, well-known systems security authorities, or established computer, network, or commercial software vendors.

(99) Any doubts about the legality of the license should be checked by the University's Legal Services Department.

(100) Reference [AS/NZS ISO/IEC 27002:2006 15.1.2].

Formal change control process

(101) All computer and communications systems used for production processing must employ a documented change control process that is used to ensure that only authorised changes are made.

(102) This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures.

(103) This applies to personal computers running production systems and larger multi-user systems.

(104) All changes to VU information systems (including desktops, servers and networks) must only be performed by persons authorised by IT.

(105) Reference [AS/NZS ISO/IEC 27002:2006, 10.1.2 & 12.5.3].

Systems Development Conventions

(106) All production software development and software maintenance activities performed by in-house staff must adhere to IT policies, standards, procedures, and other systems development conventions.

(107) Systems development conventions include proper testing, training, and documentation.

(108) All software developed by in-house staff intended to process restricted or sensitive information must have a formal written specification.

(109) Specifications must include discussion of security risks and controls including access control systems and contingency plans.

(110) Specifications must be part of an agreement between the Business Owner and the system developer.

(111) Reference [AS/NZS ISO/IEC 27002:2006, 12.1.1].

Software Licenses

(112) VU management must make appropriate arrangements with software vendors for additional licensed copies, if and when additional copies are needed for business activities.

(113) All software purchased must be reported to the IT Service Desk so that the University can centrally ensure we are appropriately licensed for all software in use.

(114) Reference [AS/NZS ISO/IEC 27002:2006, 15.1.2].

Unauthorised copying of Software

(115) Users must not copy software provided by VU to any storage media, transfer such software to another computer, or disclose such software to outside parties without advance permission from their IT.

(116) Ordinary backup copies are an authorised exception to this policy.

(117) Reference [AS/NZS ISO/IEC 27002:2006, 15.1.2].

Backups Responsibility

(118) Users must regularly back up the information on their personal work computers.

(119) For multi-user computer and communication systems, a Custodian is responsible for making periodic backups.

(120) All backups containing restricted or sensitive information must be stored at an approved off-site location with either physical access controls or encryption.

(121) A contingency plan must be prepared for all applications that handle critical production information.

(122) It is the responsibility of the Business Owner to ensure that a contingency plan is adequately developed, regularly updated, and periodically tested.

(123) Reference [AS/NZS ISO/IEC 27002:2006, 10.5.1].

Theft Protection

(124) All VU computer and network equipment must be physically secured with anti-theft devices if located in an open office or open area e.g. a laboratory.

(125) Servers and other multi-user systems must be located in an ITS approved server housing facility.

(126) Portable computers must be secured with locking cables, placed in locking cabinets, or secured by other locking systems when in an open office environment but not in active use.

(127) Computer and network gear may not be removed from VU offices unless the involved person has obtained permission from their manager.

(128) Personal electronic devices such as iPads, mobile phones and PDAs are not subject to these requirements.

(129) Reference [AS/NZS ISO/IEC 27002:2006, 9.2.1].

Disclosure of Security Information

(130) Information about security measures for VU computer and network systems is confidential and must not be released to people who are not authorised users of the involved systems unless approved by the Director of IT Operations.

(131) Public disclosure of electronic mail addresses for reasonable business needs is permissible.

(132) Reference [AS/NZS ISO/IEC 27002:2006, 6.1.5].

IT Audit of Information Systems

(133) VU management reserves the right to monitor, inspect, or search at any time all VU information systems.

(134) Inspections may take place with or without the consent, presence, or knowledge of the involved community

members.

(135) The information systems subject to such examination include, but are not limited to, electronic mail, system files, personal computer hard drive files, voice mail files, printer spool files, phone usage, fax machine output, desk drawers, and storage areas.

(136) Because VU computers and networks are provided for business and academic purposes only, community members must have no expectation of privacy associated with the information they store in or send through these information systems.

(137) VU management retains the right to remove from its information systems any material it views as offensive or potentially illegal.

(138) Further guidance on this matter can be found in the procedure for ITS Security Audit Authorities.

(139) Reference [AS/NZS ISO/IEC 27002:2006, 10.10.2].

Personal Use of VU Information Systems

(140) VU information systems are intended to be used for business and academic purposes only.

(141) Incidental personal use is permissible if the user does not consume more than a trivial amount of resources that could otherwise be used for business or academic purposes, does not interfere with normal operations or productivity, and does not interfere with any business activity.

(142) Personal use that does not fall into these three categories requires the advance permission of a department manager.

(143) Use of VU information systems for chain letters, charitable solicitations, political campaign material, religious work, transmission of objectionable material is prohibited.

Revoking System Privileges

(144) VU management reserves the right to revoke the system privileges of any user at any time.

(145) Conduct that interferes with the normal and proper operation of VU information systems, which adversely affects the ability of others to use these information systems, or is harmful or offensive to others is not permitted.

Tools that may compromise Security

(146) Unless specifically authorised by the IT department, VU community members must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security.

(147) Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

(148) Without this type of approval, community members are prohibited from using any hardware or software that monitors the traffic on a network or the activity on a computer.

(149) Reference [AS/NZS ISO/IEC 27002:2006, 10.4.1].

Prohibited Activities

(150) Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the Acting Director of IT Operations.

(151) Incidents involving unapproved system hacking, passwords guessing, file decryption, bootleg software copying, or similar unauthorised attempts to compromise security measures may be unlawful, and will be considered serious violations of VU internal policy.

(152) Short-cuts bypassing systems security measures, and pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

(153) Reference [AS/NZS ISO/IEC 27002:2006, 8.1.3].

Mandatory Reporting

(154) All suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardise VU information or VU information systems must be immediately reported to IT Service Desk.

(155) Information may be given anonymously.

(156) Reference [AS/NZS ISO/IEC 27002:2006 13.1.1, 13.1.2].

Section 6 - Guidelines

(157) Nil

Status and Details

Status	Historic
Effective Date	15th July 2015
Review Date	15th March 2018
Approval Authority	Vice-Chancellor
Approval Date	15th July 2015
Expiry Date	20th November 2016
Responsible Officer	Stuart Hildyard Chief Digital Officer and Executive Director Campus Services 9919 5576
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020