Information Security Policy

Section 1 - Background and Purpose

(1) The purpose of this document is to detail La Trobe University's policy and approach to managing Information Security, and inform students, employees, contractors, and other third parties of their responsibilities.

(2) The procedures in this document do not override the Use of Computer Facilities Statute 2009. At the discretion of the Chief Information Officer (CIO) the procedures in this document may be interpreted, subject to the provisions in the Use of Computer Facilities Statute 2009.

Section 2 - Scope

(3) Applies to:

a. All La Trobe University campuses and external locations.
b. All information, information systems and equipment used, owned, operated, processed, or kept in custody on behalf of or by La Trobe University.
c. Students, employees, contractors, and other third parties who in the course of their work or studies have access to the University's information, information systems and other facilities on the computer network.

Section 3 - Policy Statement

(4) All members of the La Trobe University community are responsible for the preservation of confidentiality integrity and availability of University information. They must:

a. comply with all legislative, regulatory and contractual requirements
b. follow incident management processes
c. abide by human resources and user access security procedures
d. follow communication and connectivity management processes
e. follow asset management and allocation processes
f. follow business continuity management practices
g. use approved acquisition, development and maintenance practices
h. follow physical and environmental security procedures
i. follow access control procedures
j. undertake security education, training and awareness
k. make themselves aware of the consequences of information security policy violations

(5) Under the Use of Computer Facilities Statute 2009 the CIO may issue determinations from time to time with prospective effect to determine authorised usage. The CIO is empowered to determine the levels of compliance to the practices contained in this policy and procedure.

Section 4 - Procedures

General

(6) These procedures are to assist members of the University community in maintaining and improving information security.

Compliance with Legislative, Regulatory and Contractual Requirements

Compliance with Legal Requirements

(7) All relevant statutory, regulatory, and contractual requirements and the organisation's approach to meet these requirements shall be explicitly defined, documented, and kept up to date for each information system and the organisation.

(8) Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

(9) Important records shall be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

(10) Data protection and privacy shall be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

(11) Users shall be deterred from using information processing facilities for unauthorised purposes.

(12) Cryptographic controls shall be used in compliance with all relevant agreements, laws, and regulations.

Compliance with Security Policies and Standards, and Technical Compliance

(13) Managers shall ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

(14) Information systems shall be regularly checked for compliance with security implementation standards.

Information Systems Audit Considerations

(15) Audit requirements and activities involving checks on operational systems shall be carefully planned and agreed to minimise the risk of disruptions to business processes

(16) Access to information systems audit tools shall be protected to prevent any possible misuse or compromise.

Information security incident management

Reporting Information Security Events And Weaknesses

(17) Information security events should be reported through appropriate management channels to Information Services as quickly as possible.

(18) All students, employees, contractors and third party users of information systems and services are required to note and report any observed or suspected security weaknesses in systems or services.

Management of Information Security Incidents and Improvements

(19) Management responsibilities and procedures shall be established to ensure a quick, effective, and orderly response to information security incidents.

(20) There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

(21) Where a follow-up action against a person or organisation after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Human resources and user access security

Prior to Engagement

(22) Security roles and responsibilities of students, employees, contractors and third party users shall be defined and documented.

(23) Background verification checks on all individual candidates for employment, contractors, students, and third party users shall be carried out where applicable in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

(24) As part of their enrolment or contractual obligation, students, employees, contractors and third party users shall agree and sign the terms and conditions of their enrolment or contract, which shall state their and the organisation's responsibilities for information security.

During Engagement

(25) Management shall require students, employees, contractors and third party users to apply security in accordance with established policies and procedures of the organisation.

(26) All students, employees of the organisation and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant.

(27) There shall be a formal disciplinary process for students and employees who have committed a security breach.

Termination or Change of Role

(28) Responsibilities for performing employment termination or change of role shall be clearly defined and assigned.

(29) All students, employees, contractors and third party users shall return all of the organisation's assets in their possession upon termination unless otherwise agreed with the University.

(30) The access rights of all students, employees, contractors and third party users to information and information processing facilities shall be removed upon termination or adjusted upon a role change.

Communications and Connectivity Management

Operational Procedures and Responsibilities

(31) Operating procedures shall be documented, maintained, and made available to all users who need them.

(32) Changes to information processing facilities and systems shall be controlled.

(33) Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional

modification or misuse of the organisation's assets.

(34) Development, test, and operational facilities shall be separated to reduce the risks of unauthorised access or changes to the operational system.

Third Party and Cloud Service Delivery Management

(35) It shall be ensured that the security controls, service definitions and delivery levels included in the third party service delivery agreement are implemented, operated, and maintained by the third party.

(36) The services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly.

(37) Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

System Planning and Acceptance

(38) The use of resources shall be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

(39) Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.

Protection Against Malicious and Mobile Code

(40) Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.

(41) Where the use of mobile code is authorised, the configuration should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code should be prevented from executing.

Back-Up

(42) Back-up copies of software and information necessary to achieve effective and efficient delivery of objectives and outcomes shall be taken and tested regularly in accordance with the agreed backup policy.

Network Security Management

(43) Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

(44) Security features, service levels, and management requirements of all network services shall be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

(45) Users of cloud and other external data services are required to subject any terms of use, conditions of service or any other agreement to the requirements of the University's Legal Process and Approval of Contracts Policy prior to accessing the service.

Media Handling

(46) There shall be procedures in place for the management of removable media.

(47) Media shall be disposed of securely and safely when no longer required, using formal procedures.

(48) Procedures for the handling and storage of information shall be established to protect this information from unauthorised disclosure or misuse.

(49) System documentation shall be protected against unauthorised access.

Exchange of Information

(50) Formal exchange procedures and controls shall be in place to protect the exchange of information through the use of all types of communication facilities.

(51) Agreements shall be established for the exchange of information and software between the organisation and external parties.

(52) Media containing information shall be protected against unauthorised access, misuse or corruption during transportation beyond an organisation's physical boundaries.

(53) Information involved in electronic messaging shall be appropriately protected.

(54) Policies and procedures shall be developed and implemented to protect information associated with the interconnection of business information systems.

Electronic Commerce Services

(55) Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification.

(56) Information involved in on-line transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.

(57) The integrity of information being made available on a publicly available system shall be protected to prevent unauthorised modification.

Monitoring

(58) Where practical, audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

(59) Procedures for monitoring use of information processing facilities shall be established and the results of the monitoring activities reviewed regularly.

(60) Logging facilities and log information shall be protected against tampering and unauthorised access.

(61) System administrator and system operator activities shall be logged wherever possible.

(62) Faults shall be logged, analysed, and appropriate action taken.

(63) The clocks of all relevant information processing systems within an organisation or security domain shall be synchronised with an agreed accurate time source.

Asset Management and Allocation

Responsibilities for Assets

(64) All assets shall be clearly identified and an inventory of all important assets drawn up and maintained.

(65) All information and assets associated with information processing facilities shall have a nominated owner.

(66) Rules for the acceptable use of information and assets associated with information processing facilities shall be identified, documented, and implemented.

Information Classification

(67) Information shall be classified in terms of its value, legal requirements, sensitivity, and criticality to the organisation.

(68) An appropriate set of procedures for information labelling and handling shall be developed and implemented in accordance with the classification scheme adopted by the organisation.

Business Continuity Management

Information Security Aspects of Business Continuity Management

(69) A managed process shall be developed and maintained for business continuity throughout the organisation that addresses the information security requirements needed for the organisation's business continuity.

(70) Events that can cause interruptions to business processes shall be identified, along with the probability and impact of such interruptions and their consequences for information security.

(71) Plans shall be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

(72) A single framework of business continuity plans shall be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

(73) Business continuity plans shall be tested and updated regularly to ensure that they are up to date and effective.

Information Systems Acquisition, Development and Maintenance

Security Requirements of Information Systems

(74) Statements of business requirements for new information systems, or enhancements to existing information systems shall specify the requirements for security controls.

Correct Processing in Applications

(75) Data input to applications shall be validated to ensure that this data is correct and appropriate.

(76) Validation checks shall be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

(77) Requirements for ensuring authenticity and protecting message integrity in applications shall be identified, and appropriate controls identified and implemented.

(78) Data output from an application shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

Cryptographic Controls

(79) Cryptographic controls for protection of information should be developed and implemented for sensitive information where practical.

(80) Key management shall be in place to support the organisation's use of cryptographic techniques.

Security of System Files

(81) There shall be procedures in place to control the installation of software on operational systems.

(82) Test data shall be selected carefully, and protected and controlled.

(83) Access to program source code shall be restricted.

Security in Development and Support Processes

(84) The implementation of changes shall be controlled by the use of formal change control procedures.

(85) When operating systems are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organisational operations or security.

(86) Modifications to software packages are discouraged, and limited to necessary changes, and all changes shall be strictly controlled.

(87) Opportunities for information leakage shall be prevented.

(88) Outsourced software development shall be supervised and monitored by the organisation.

Technical Vulnerability Management

(89) Timely information about technical vulnerabilities of information systems being used shall be obtained, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

Physical and Environmental Security

Secure Areas

(90) Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) shall be used to protect areas that contain information and information processing facilities.

(91) Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.

(92) Physical security for offices, rooms, and facilities should be designed and applied.

(93) Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster shall be designed and applied.

(94) Physical protection and guidelines for working in secure areas shall be designed and applied.

(95) Access points such as delivery and loading areas and other points where unauthorised persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorised access.

Equipment Security

(96) Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access.

(97) Important equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.

(98) Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage.

(99) Equipment shall be correctly maintained to ensure its continued availability and integrity.

(100) Security should be applied to off-site equipment taking into account the different risks of working outside University premises.

(101) All items of equipment containing storage media shall be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

(102) Equipment, information or software shall not be taken off-site without prior authorisation.

(103) University data on equipment not owned or leased by the University is still the responsibility of the member of the University, as specified in the Information Security Policy, this includes mobile devices such as iPhones, iPads, android devices, home PCs or other personal and cloud computing storage or services.

Access Control

Business Requirement for Access Control

(104) User access to Organization’s information systems shall be granted on the basis of the need-to-know principle. Users shall be given access only at the appropriate level required to perform their job functions for the business.

User Access Management

(105) There shall be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

(106) The allocation and use of privileges shall be restricted and controlled.

(107) The allocation of passwords shall be controlled through a formal management process.

(108) Users' access rights shall be subject to review at regular intervals.

User Responsibilities

(109) Users shall be required to follow good security practices in the selection and use of passwords.

(110) Users shall ensure that unattended equipment has appropriate protection.

(111) A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted where information of a sensitive nature is being handled.

Network Access Control

(112) Users shall only be provided with access to the services that they have been specifically authorised to use.

(113) Appropriate authentication methods shall be used to control access by remote users.

(114) Automatic equipment identification shall be considered as a means to authenticate connections from specific locations and equipment.

(115) Physical and logical access to diagnostic and configuration ports shall be controlled.

(116) Groups of information services, users, and information systems shall be segregated on networks.

(117) For shared networks, especially those extending across the organisation's boundaries, the capability of users to connect to the network shall be restricted, in line with the need to know principle and requirements of the business applications (see 9.1).

(118) Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the security of the business applications.

Operating System Access Control

(119) Access to operating systems shall be controlled by a secure log-on procedure.

(120) All users shall have a unique identifier (user ID) for their personal use only, and a suitable authentication technique shall be chosen to substantiate the claimed identity of a user.

(121) Systems for managing passwords shall be interactive and shall ensure quality passwords.

(122) The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

(123) Inactive sessions shall shut down after a defined period of inactivity.

(124) Restrictions on connection times shall be used to provide additional security for high-risk applications.

Application and Information Access Control

(125) Access to information and application system functions by users and support personnel shall be restricted in accordance with the need to know principle. Sensitive systems shall have a dedicated (isolated) computing environment.

Mobile Computing and Teleworking

(126) Appropriate security measures, such as the use of encryption for data in transit and at rest, shall be adopted to protect against the risks of using mobile computing and communication facilities.

(127) A policy, operational plans and procedures shall be developed and implemented for teleworking activities.

Security education, training and awareness

Security Education, Training and Awareness

(128) Information Security awareness training shall be included in the professional development plans of all personnel.

(129) The level of training required will be appropriate to the role of the individual in the University community.

Consequences of Information Security Policy Violations

Consequences For The University

(130) Violation of Security Policy and Procedures may result in Reputational, Financial, Regulatory/Legal, Business Performance or Stakeholder or Safety and Security risks or losses for the University and as a result are viewed very seriously.

Consequences for the Individual

(131) Breaches of the Information Security Policy may also constitute breaches of the Use of Computer Facilities

Statute 2009 or the Code of Conduct. The penalties for breaches of the statute are outlined in the statute itself. Breaches of the Code Of Conduct may also result in disciplinary action being taken.

Section 5 - Definitions

(132) For the purpose of this Policy and Procedure:

a. Android devices: The Android platform is Google Inc.'s open and free software stack that includes an operating system, middleware and also key applications for use on mobile devices, including smartphones.
b. Asset: anything that has value to the organisation.
    i. NOTE This definition is independent to that used by the Finance Division.
c. Cloud Computing: the use of computing resources that are delivered as a service over the network (typically the internet).
d. Control: means of managing risk, including policies, procedures, guidelines, practices or organisational structures, which can be of administrative, technical, management, or legal nature.
    i. NOTE Control is also used as a synonym for safeguard or countermeasure.
e. Equipment: an electronic device or media used to store, process or transmit information.
f. Guideline: a description that clarifies what should be done and how, to achieve the objectives set out in policies.
g. Home PC: any computer not owned or leased by the University and used by a member of the University community.
h. iPad: a tablet computer developed by Apple Inc.
i. iPhone: a smartphone developed by Apple Inc.
j. Information processing facilities: any information processing system, service or infrastructure, or the physical locations housing them.
k. Information security: preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, reliability and privacy can also be involved.
l. Information security event: an information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
m. Information security incident: an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
n. Information systems: any information processing system, service or infrastructure, or the physical locations housing them.
o. Mobile Code: mobile code (MMC) is any software program designed to move from computer to computer and network to network, in order to intentionally modify computer systems without the consent of the owner or operator. MMC includes viruses, Trojan horses, worms, script attacks and rogue internet code.
p. Policy: overall intention and direction as formally expressed by management.
q. Risk: combination of the probability of an event and its consequence.
r. Risk analysis: systematic use of information to identify sources and to estimate the risk.
s. Risk assessment: overall process of risk analysis and risk evaluation.
t. Risk evaluation: process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
u. Risk management: coordinated activities to direct and control an organisation with regard to risk.
    i. NOTE Risk management typically includes risk assessment, risk treatment, risk acceptance and risk communication.

v. Risk treatment: process of selection and implementation of measures to modify risk.
w. Third party: that person or body that is recognised as being independent of the parties involved, as concerns the issue in question.
x. Threat: a potential cause of an unwanted incident, which may result in harm to a system or organisation.
y. University: refers to La Trobe University.
z. University: La Trobe University
aa. Vulnerability: a weakness of an asset or group of assets that can be exploited by one or more threats.

Status and Details

Status	Current
Effective Date	1st November 2016
Review Date	9th March 2023
Approval Authority	Vice-Chancellor
Approval Date	27th October 2016
Expiry Date	Not Applicable
Responsible Policy Officer	Stuart Hildyard Chief Information Officer
Author	David Hird
Enquiries Contact	Information Services 03) 9479 1500