# Information Security Policy

# Section 1 - Summary

(1) This Policy:

a. Defines Victoria University's high-level information security requirements based on the ISO 27001:2013 standard, NIST Cybersecurity Framework and other industry best practices, enabling the University to minimize information security risk and efficiently respond to incidents.
b. Ensures that University information security controls and Governance meet legal and other compliance requirements.

# Section 2 - Accountability

### Key Decision-making powers under the Policy

| (Delegated) Power | Role |
|---|---|
| Executive Director, IT Services | Power to approve the use of alternative authentication models for all VU equipment, networks and business systems as per the Information Security - User Access Management Procedure.<br>Power to suspend user access for student accounts as per the Information Security - User Access Management Procedure and in accordance with the Student Misconduct Regulations 2019.<br>Power to approve the blocking of sites believed to be in contravention of legislation or University policies and values, as per the Information Security - Internet Filtering Procedure.<br>Power to approve Security Audits that involve access to confidential material, as per the Information Security - IT Security Audit Authorities Procedure. |

# Section 3 - HESF/ASQA/ESOS Alignment

(2) HESF: 2.1 Facilities and Infrastructure; 3.3 Learning Resources and Support; 7.3 Information Management.

# Section 4 - Scope

(3) This Policy applies to all Victoria University's students, employees, contractors and third-party service providers undertaking any activities that involve creating, accessing, using, storing, processing or transferring of University's information.

(4) This Policy applies to all information assets 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.

(5) This Policy also covers any information assets outsourced or hosted at external/third-party service providers, if that

asset resides in a Victoria University domain or appears to be owned by Victoria University.

# Section 5 - Definitions

(6) Information Security Risk – Cyber and information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information assets and consider impacts to the organisation (mission, functions, image, or reputation), individuals, other organisations, the State and the Nation.

(7) ICT Business Risk – Business risk associated with the adoption and use of technology. This includes cyber and information security risk.

(8) Business Owner – Individual with operational authority for specified information asset and responsibility for establishing controls for its protection.

(9) Information Custodian – Individual responsible for overseeing and implementing the necessary controls to protect the information assets, at the level classified by the Business Owner.

(10) Information Asset – Any information that is of value to the organisation. This term also includes the underlying supporting infrastructure such as business processes, hardware, networks, storage, applications, third-party providers and storage amongst others.

(11) Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

(12) Information Transfer – Any activity that involves transferring data from one application, system or end-point to another. Information transfers are considered, but not limited to email, file transfers and web traffic.

(13) Authentication Information / Credentials – Any form of authentication used to validate the identity of an individual. Common authentication information are: passwords, private keys, tickets, tokens, etc.

(14) Account – Accounts provide a way to identify and authenticate individuals to a system.

(15) Generic Accounts – Accounts that identify a function or a group of people.

(16) Keying Material – The data (e.g., keys and IVs) necessary to establish and maintain cryptographic keying relationships. In other words, secret keys of (unspecified) format, length and amount.

(17) Key Management Infrastructure or Cryptographic Key Management System – All parts – computer hardware, firmware, software, and other equipment and its documentation; facilities that house the equipment and related functions; and companion standards, policies, procedures, and doctrine that form the system that manages and supports the ordering and delivery of cryptographic material and related information products and services to users.

(18) SOE / MOE – Standard Operating Environment or Managed Operating Environment is a standard implementation of an operating system and its associated software.

(19) Business Continuity Plan – BCP prepares the University for planned and unplanned business disruptions so that in the event of a disruption, the University can move expeditiously from ‘Preparedness’ to ‘Response’ in order to maintain core business activities and to protect the interests of the University.

(20) Disaster Recovery Plan – DRP refers to the processes, policies and procedures relating to preparing for recovery or continuation of critical functions and services after a system failure, human provoked or natural disaster.

(21) Vulnerability – A flaw in security procedures, software, internal system controls, or implementation of an IS that

may affect the integrity, confidentiality, accountability, and/or availability of data or services. Vulnerabilities include flaws that may be deliberately exploited and those that may cause failure due to inadvertent human actions or natural disasters.

# Section 6 - Policy Statement

## Information Security Governance

(22) Adequate information security governance will be achieved to ensure that information assets are adequately protected based on their classification and sensitivity; risks are managed; compliance with regulatory, legislative and contractual requirements are achieved; and strategic business objectives are accomplished.

(23) A digital advisory committee (DAC) or equivalent will be established as the governance body responsible for ensuring that proper information security governance is established, maintained, monitored, improved and achieving its objectives.

(24) A business risk approach towards information security risk will be adopted. Victoria University should define an appropriate information security risk management framework in order to ensure risks are properly identified, analyzed, evaluated, tracked, managed and reported.

(25) Information security capabilities such as risk management and policy management will not be outsourced.

(26) For further information refer to the ICT risk and compliance standard.

## Human Resources Security

(27) Adequate human resources processes (e.g. recruitment, on-boarding, off-boarding and disciplinary) will be established to reduce the risk of insider threats and unauthorized disclosure of information.

(28) Employees, contractors or third-party service providers seeking access to Victoria University's information assets will have background verification checks carried out in accordance with University policies and procedures, relevant laws, regulations and ethics before being granted access.

(29) Students, employees, contractors and third-party service providers accessing or using Victoria University's information assets will be subject to awareness and education activities including topics such as policies, responsibilities, consequences of non-compliance, potential security threats and how to prevent them.

(30) Management will require students, employees, contractors and third-party service providers to apply information security in accordance with this Policy and supporting IT Security Standards.

(31) Work agreements and contracts with employees, contractors and third-party providers will during and after employment.

(32) For further information, refer to the human resources security standard.

## Asset Management Security

(33) Information assets will be adequately used and protected based on the information they store, process or transmit.

(34) All information assets will be identified, classified, labelled and recorded in a centralised inventory; be subject to periodic reviews to confirm their existence, adequacy of implemented controls and defined classifications.

(35) Appropriate individuals will be defined as Business Owners and Custodians. Business Owners will classify their information and ensure that adequate security controls are applied to protect it. Information Asset Custodians should implement security controls based on the classification of the assets and guidance from the Business Owners.

(36) Information assets will be securely removed, transferred, sanitized, destroyed and disposed of based on their classification and established procedures. All students, employees, contractors and third-party service providers will return Victoria University assets in their possession upon termination of their attendance, employment, contract or agreement.

(37) The use of removable media will be controlled based on the classification of the assets and guidance from the Business Owners.

(38) All Victoria University business communications sent by e-mail will be sent and received using the institutional e-mail address.

(39) For further information, refer to the following IT Security Standards: asset management standard, media sanitisation, destruction and disposal standard; product sanitisation, destruction and disposal standard; removable media security standard; and information asset classification standard.

## Access Control Security

(40) Adequate processes to provision, modify, revoke and revalidate user accounts will be established in order to reduce the risk of unauthorized access to information assets.

(41) Access to information assets will be authenticated based on a business need (need to know principle) and allocated the minimum required privileges (least privilege principle).

(42) Students, employees, contractors and third-party service providers accessing Victoria University's information assets will be uniquely identified. Use of generic user accounts will be strictly controlled.

(43) Unauthorized use of user accounts will be prevented by protecting authentication credentials and implementing technical controls.

(44) Authentication credentials will not be shared.

(45) All user account identification, authentication and authorisation activities will be logged and monitored.

(46) Temporary access to Victoria University's information assets will be restricted and supervised.

(47) For further information, refer to the following IT Security Standards: Access control standard, identification standard and authentication standard.

## Cryptography Security

(48) Keying material will be adequately managed and protected.

(49) Keying material suspected of being compromised will be:

a. Immediately reported to the ITS Service Desk.
b. Immediately revoked when they are suspected of being compromised

(50) A Cryptographic Key Management System will be established and implemented.

(51) A list of approved cryptographic algorithms (ACA) and approved cryptographic protocols (ACP) for use at Victoria

University will be established.

(52) For further information, refer to the following IT Security Standards: Cryptography standard, Key management standard, TLS and S/MIME security standard, SSH security standard and IPSec security standard.

## Physical and Environmental Security

(53) Access to physical areas hosting Victoria University's information assets will be controlled to ensure that only authorized employees, contractors and third-party services providers are allowed access.

(54) Information assets will be protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

(55) Information processing and communication facilities hosting Victoria University's information assets will be adequately protected and designed against natural, man-made disasters and malicious attacks.

(56) Keys or equivalent access mechanisms to server rooms, communications rooms and security containers or rooms will be appropriately secured and controlled.

(57) Operational procedures associated with information processing and communication facilities will be established.

(58) For further information, refer to the following IT Security Standards: Physical and environmental security standard and Cabling security standard.

## Operations Security

(59) Changes to production information assets will be controlled through a formal change and transition management process.

(60) Information asset resources will be monitored, tuned and projections made of future capacity requirements to ensure current and future performance is achieved.

(61) Tools and procedures covering the detection of potential cybersecurity incidents will be established, implemented and maintained.

(62) Information backups will be performed on applicable information assets, based on its classification and business availability and integrity requirements.

(63) Information asset events will be recorded, retained, archived, protected and correlated in order to detect, investigate and respond to security incidents. Logging and audit configurations will be defined and implemented in consideration of regulatory requirements and best practices.

(64) Managed Operating Environments (MOEs) will be defined, designed and implemented in such a way that a common, consistent and secure approach is obtained. All MOEs will prevent unauthorized software installation and configuration changes.

(65) MOEs and applications will be configured in a way to reduce the risk of cyber-attacks.

(66) Confidentiality, integrity and availability of database systems and their content will be maintained based on their classification.

(67) Information about technical vulnerabilities applicable to Victoria University's information assets will be obtained in a timely fashion, evaluated and managed to reduce the risk of cyber-attacks.

(68) Audit requirements and activities involving the verification of operational systems will be carefully planned and

agreed to minimize disruptions to business processes.

(69) For further information, refer to the following IT Security Standards: SOE security standard, vulnerability management Standard, security patch management standard, logging and auditing standard, information backup standard, database security standard, availability and capacity management standard, change and transition management standard, virtualisation security standard; ICT product security standard; and IoT security standard.

## Communications Security

(70) Networks will be designed, configured and operated in a secure manner to prevent cyber-attacks and minimise disruptions.

(71) Appropriate security controls will be implemented in order to minimise unauthorized access and the effects of disruptions on the network and online services. A defence-in-depth approach will be considered by implementing multiple layers of controls.

(72) Intrusion detection and prevention strategy will be developed, implemented and maintained in order for Victoria University to efficiently detect incidents and respond to cyber-attacks.

(73) Information asset transfers will be protected while at rest and in transit based on its classification. Transfer and non-disclosure agreements between Business Owners and the sending or receiving organizations should be established.

(74) Information assets will be configured in a way to reduce the risk of cyber-attacks.

(75) Network traffic, including data being imported to or exported from a Victoria University information asset, will be monitored for malicious content and breaches of the policy.

(76) Mobile devices and communication technologies will be controlled, secured and monitored.

(77) For further information, refer to the following IT Security Standards: network security standard, gateway security standard, information transfer security standard, content filtering security standard, email security standard, wireless security standard, web proxy security standard, mobile device security standard and communications systems and devices security standard.

## System Acquisition, Development and Maintenance Security

(78) Information security requirements will be included in projects delivering new information assets or enhancements to existing information assets.

(79) Software developers will adopt secure programming practices and principles when developing software.

(80) Development environments will be established and protected. The production environments will be logically or physically separated from the development ones.

(81) New information systems, upgrades and new versions will be subject to testing activities, including security testing, before implementing in production.

(82) Information in production environments including anonymized production data will not be used in testing or development environments unless the testing or development environments are secured to the same level as the production environment. The use of production information for testing or development purposes will be approved and risk accepted.

(83) For further information, refer to the following IT Security Standards: software security and development standard

and change and transition management standard.

## Supplier Relationships Security

(84) Third-party service providers will be procured following Victoria University's procurement policies and procedures.

(85) Victoria University's information assets will not be stored, processed or transferred outside of Australia.

(86) Third-party service providers that access, store, transmit or process Victoria University's information assets will be subject to thorough information security due diligence prior to entering in a contractual obligation.

(87) Controls associated with the protection of information assets entrusted to a third-party service provider as well as other requirements will be documented in contract provisions, a memorandum of understanding or equivalent formal agreement between parties.

(88) Relationships with third-party service providers will be adequately managed.

(89) Third-party service providers will be periodically reassessed for compliance, changes and risk monitoring purposes.

(90) For further information, refer to the ICT outsourcing standard.

## Information Security Incident Management

(91) An incident response plan (IRP) will be established and periodically tested. The IRP will consider common cyber-security incidents in order to ensure an efficient and orderly response to cyber-attacks.

(92) All cyber and information security incidents, such as unauthorized disclosure, access or deletion/destruction of information assets (including applications or network credentials), will be reported to Victoria University's ITS Services.

(93) For further information, refer to the incident response standard.

## Business Continuity and Resiliency

(94) A disaster recovery plan (DRP) will be established and periodically tested to ensure that core ICT services can be restored during a major extended disruption affecting Victoria University's primary processing facility (i.e. Data Centre) or other service providers facilities.

(95) Availability requirements will be established and agreed for core ICT services and implement the required controls to ensure those requirements are met.

(96) Business Owners will define for each of their assets (e.g. business applications) their availability requirements and a disaster recovery plan (DRP).

## Compliance

(97) Compliance with established policies and applicable legal and regulatory requirements will be proactively monitored and achieved. This includes intellectual property rights, protection of records, software licenses, privacy and cryptographic controls.

(98) Compliance monitoring activities will be enhanced with independent reviews and automated processes.

(99) Non-compliances to Policy will be identified, analysed, evaluated, tracked, managed and reported.

(100) Victoria University has the right to conduct audits on any system at Victoria University as specified in the

Information Security - IT Security Audit Authorities Procedure.

(101) Breach of this Policy could result in a withdrawal of access to the University email and computer network as well as possible disciplinary action under the Victoria University Enterprise Agreement 2019 and Appropriate Workplace Behaviour Policy.

(102) Any actual or suspected breaches of this Policy should be reported immediately to your line manager or other authority including operational risk and compliance representative.

(103) Although compliance with this Policy is mandatory, exemptions may be permitted under extraordinary circumstances where full compliance is not possible.

# Section 7 - Procedures

(104) Information Security - Internet Filtering Procedure

(105) Information Security - IT Security Audit Authorities Procedure

(106) Information Security - User Access Management Procedure

(107) Information Security - Virus Protection Procedure

## Status and Details

| | |
|---|---|
| **Status** | Historic |
| **Effective Date** | 18th December 2019 |
| **Review Date** | 18th December 2022 |
| **Approval Authority** | Vice-Chancellor |
| **Approval Date** | 18th December 2019 |
| **Expiry Date** | 31st January 2024 |
| **Accountable Officer** | Lisa Line<br>Deputy Vice-Chancellor Enterprise and Digital<br>Lisa.Line@vu.edu.au |
| **Responsible Officer** | Stuart Hildyard<br>Chief Digital Officer and Executive Director Campus Services<br>9919 5576 |
| **Enquiries Contact** | James Munro<br>Associate Director, VU Cyber<br>0437216020 |