Information Security Policy

Section 1 - Summary

(1) This Policy:

a. Defines Victoria University's (VU) high-level information security requirements based on the ISO 27001:2022 standard, National Institute of Standards and Technology (NIST) Cybersecurity Framework and other industry best practices, enabling the University to minimise information security risk and efficiently respond to incidents.
b. Ensures that University information security controls and governance comply with applicable state, federal and global laws governing information resources including legal and other compliance requirements. These include but are not limited to:
    i. Privacy Act 1988 (Cth);
    ii. Victoria University Act 2010 (Vic);
    iii. Requirements mentioned as part of VU Committees;
    iv. Tertiary Education Quality and Standards Agency Act 2011 (Cth) (TEQSA Act);
    v. Education Services for Overseas Students Act 2000 (Cth) (ESOS Act);
    vi. Higher Education Standards Framework (Threshold Standards) 2021;
    vii. Security of Critical Infrastructure Act 2018 (Cth);
    viii. University Foreign Interference Taskforce.
c. Provides the mandated set of minimum security and operational guidelines meeting the needs of VU, students and VU Community for connected, protected and trusted systems.
d. Further endeavours to engage all levels of VU to promote a cyber-aware, informed and proactive culture to protect VU's information and data assets.

Section 2 - HESF/ASQA/ESOS Alignment

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

(3) Standards for Registered Training Organisations (RTOs) 2015: Standard 8.

Section 3 - Scope

(4) This Policy applies to:

a. VU students, staff, controlled entities of VU, contractors and third-party service providers undertaking any activities that involve creating, accessing, using, storing, processing or transferring of the University's information.
b. Information assets that are owned and/or operated by VU and/or registered in any Domain Name System (DNS) domain owned by VU and any devices that are present on the University premises, but may not be owned or operated by the University.

c. Any information assets outsourced or hosted at external/third-party service providers, if that asset resides in a VU domain or appears to be owned by VU or stores VU information.

Section 4 - Definitions

(5) Account – A unique identity created for a person, machine or service that provides access to digital infrastructure and information assets.

(6) Business Continuity - Capability of the University to continue the delivery of services at predefined acceptable levels following a disruptive incident to minimise any reputational risk to the University.

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

(8) Cryptographic Key Management - Implementation of procedures and internal processes to manage and support approved encryption algorithms and protocols for the secure transmission of information.

(9) 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, removable media, third-party providers and storage amongst others.

(10) 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.

(11) 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.

Section 5 - Policy Statement

(12) This Policy supports VU's cyber security principles and objectives.

(13) VU's information assets must not be used, shared or stored in a manner that violates VU's policies and will be used and protected in compliance with this Policy, and other relevant policies including the:

a. IT Appropriate Use Policy
b. IT Asset Policy
c. Appropriate Workplace Behaviour Policy
d. Records Management Policy
e. Privacy Policy

Part A - Classification and Configuration of Information Assets

(14) Information assets are to be appropriately protected based on their classification and sensitivity in line with VU's Information and Asset Classification Framework.

(15) VU staff will be responsible for:

a. The classification of information assets in line with VU’s Information and Asset Classification Framework.
b. Handling VU information assets based on their classification in line with VU’s Information and Asset

Classification Framework.

(16) All systems at VU will be configured in line with University approved security configuration recommendations to minimise security risks.

Part B - Risk Management

(17) Information security risks will be managed in line with VU's Risk Management Policy and Procedure.

(18) Critical incidents are responded to in line with the Critical Incident, Emergency Planning and Business Continuity Policy and Procedure.

(19) Business Continuity response and planning are managed in accordance with the Business Resilience Framework and Policy.

(20) Third-party service providers are procured in line with Third Party Arrangements Policy and Purchasing Policy requirements.

(21) Third-party service providers that access, store, transmit or process VU's information assets will be subject to information security due diligence in line with VU's Ecosystem Security Assurance Framework.

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

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

Part C - Physical Access to Information Assets

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

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

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

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

Part D - Authentication and Access Management

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

(29) Access to information assets is authenticated against a central authentication system and authorisation is based on need to know and the principle of least privilege in line with the Information Security - User Access Management Procedure and the Information Security - User Authentication Procedure.

(30) Unauthorised use of accounts is prohibited, is a breach of university policy and may be subject to disciplinary and/or legal action.

Part E - Responsibilities

(31) All persons using or accessing VU's information assets are responsible for protecting information from unauthorised access.

(32) Users sending university related email communications both internally and externally must use authorised university email systems and applications using a university issued email address.

(33) All persons using or accessing VU's information assets will undergo background verification as per the Enrolments Procedure or Recruitment and Selection Policy.

(34) The University will provide training and awareness activities for students, staff, contractors and third-party service providers accessing or using VU's information assets.

(35) The Cyber Security Advisory Committee is responsible for ensuring that University information security controls comply with applicable state, federal and global laws governing information resources, including legal and other compliance requirements.

Part F - Cryptography Security

(36) A Cryptographic Key Management System is established and implemented.

(37) A list of approved cryptographic algorithms (ACA) and approved cryptographic protocols (ACP) for use at VU will be established.

Part G - Compliance

(38) 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.

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

(40) VU has the right to conduct audits on VU information systems including personal devices while connected to the University network to ensure compliance with University polices. Any exceptions to this Policy and associated Information Security procedures must be approved by the Chief Digital Officer and Executive Director Campus Services.

Part H - Breach of Policy

(41) Any actual or suspected breaches of this Policy should be reported immediately to the IT Customer Support Desk or line manager or other authority including operational risk and compliance representative.

(42) All breaches of this Policy will be treated seriously and may be subject to disciplinary action in accordance with the relevant enterprise agreement (for staff) or Student Misconduct Regulations 2019 (for students).

Section 6 - Procedures

(43) Information Security - Internet Filtering Procedure

(44) Information Security - IT Security Audit Authorities Procedure

(45) Information Security - User Access Management Procedure

(46) Information Security - Virus Protection Procedure

(47) Information Security - User Authentication Procedure

Status and Details

Status	Current
Effective Date	1st February 2024
Review Date	1st February 2027
Approval Authority	Vice-Chancellor
Approval Date	31st January 2024
Expiry Date	Not Applicable
Accountable Officer	Lisa Line Deputy Vice-Chancellor Enterprise and Digital Lisa.Line@vu.edu.au
Responsible Officer	Stuart Hildyard Chief Digital Officer and Executive Director Campus Services 9919 5576
Enquiries Contact	James Munro Associate Director, VU Cyber 0437216020