Information Security Management System

Governance Framework

Section 1 - Purpose

(1) The University of Wollongong (UOW or the University) has established an Information Security Management System (ISMS) aligned to the ISO/IEC 27001:2022 information security standard and have established a set of information security objectives.

(2) This Framework details the governance structure and, roles and responsibilities required for the University to manage its information security risks relating to the provision of technology, through its commitment to developing, implementing and continually improving its ISMS.

(3) In support of this framework, the University develops, publishes, and continually improves policies, procedures and local protocols to support compliance to, and operation of the ISMS.

Section 2 – Application and Scope

(4) The scope of the ISMS includes:

a. *All users, including students, staff, suppliers and affiliates of the University.*

b. *All IT resources that are used to support the academic, administrative and research processes of the University.*

c. *All academic, research and administrative functions of the University.*

d. *All domestic Australian and international campuses and offices.*

(5) The University operates under three separate entities, with the University as the main controlling entity. These entities are:

a. **UOW:** UOW operates nine domestic campuses, with the main campus being in Wollongong, NSW. Below is a list of all campuses in Australia:

- UOW Main Campus, Wollongong NSW
- UOW Innovation Campus, North Wollongong NSW
- UOW Eurobodalla, Batemans Bay NSW
- UOW Bega Valley, Bega NSW
- UOW Shoalhaven, Nowra NSW
- UOW Southern Highlands, Moss Vale NSW
- UOW Sutherland, Loftus NSW
- UOW Liverpool, Liverpool NSW
- UOW Sydney CBD, Sydney NSW

UOW is governed by the University Council.

b. **UOW Global Enterprises:** UOW Global Enterprises (UOWGE) is a subsidiary group of the University of Wollongong and is aligned to the University's strategic objectives of international student growth

   Established in 1988, UOWGE owns and operates:

   - University of Wollongong in Dubai (UOWD)
   - UOW College Australia (UOWCA)
   - UOW College Hong Kong (UOWCHK)
   - UOW Malaysia (UOWM)
   - University of Wollongong India (UOWI)

   UOWGE is governed by its own Board of Directors.

c. **UOW Pulse Ltd:** UOW Pulse is a not-for-profit organisation, with proceeds from everything purchased on campus going straight back into enriching student life on campus.

   UOW Pulse is governed by its own Board of Directors.

Section 3 – Interested Parties

(6) The ISMS scope has considered the following interested parties and their requirements:

Interested Party	Requirements
Staff, Students, Suppliers and Affiliates	• Assurance that the University is invested in the management of its information security and trust in the University's information assets for the protection of personal information and intellectual property.
University Executive	• Assurance that information security practices are meeting the University's business objectives, regulatory requirements and the maintenance of the University's reputation.
Researchers	• Assurance that the University is invested in the management of its information security and trust in the University's information assets for the protection of their research data and the sensitive information of research participants. • Assurance that risk management practices will not have an adverse impact on project timelines and agility.
Regulators	• Assurance that the University is meeting its regulatory requirements, Including all due diligence and due care, regarding the protection of information and privacy. • Expectations to report notifiable incidents as required by the relevant legislation.
Donors and Alumni	• Assurance that the University is invested in the management of its information security and trust in the University's information assets for the protection of personal information and intellectual property.
Council Risk, Audit Compliance Committee	• Information security practices align with risk management practices in place and adhered to. • Assurance information security controls are effective and adhered to.

	• Information security legal, regulatory and compliance obligations are adhered to.

Section 4 – Internal and External Issues Considerations

(7) The University has considered the following internal and external issues which may impact its ability to achieve ISMS objectives:

a. Internal:

- Availability and capacity constraints of key resources and expertise to manage and support the ISMS.
- Potential cultural resistance to change across some areas of the business and a tendency to fall back to ad-hoc processes.
- Balancing the need for timely and appropriate availability of information against requirements for confidentiality.
- Availability of sufficient funding and resources to achieve information security objectives.
- Complexity of the University organisational structure and governance bodies.

b. External:

- The rate of technological, legal and regulatory changes with respect to information security.
- Changes in the political environment, legislation, and regulations may impact funding and University operations.
- Shifts in the geopolitical landscape and foreign interference can significantly influence decisions regarding the procurement of technology and the management of associated supply chains.
- Modern slavery poses a significant external risk when acquiring services from providers that do not comply with modern slavery obligations
- The increasing possibility of extreme weather events that may impact the availability of the University's information assets or people in delivering services to customers.

(8) The University's ISMS risk management approach and strategies have considered these issues to mitigate the risks associated with these identified issues.

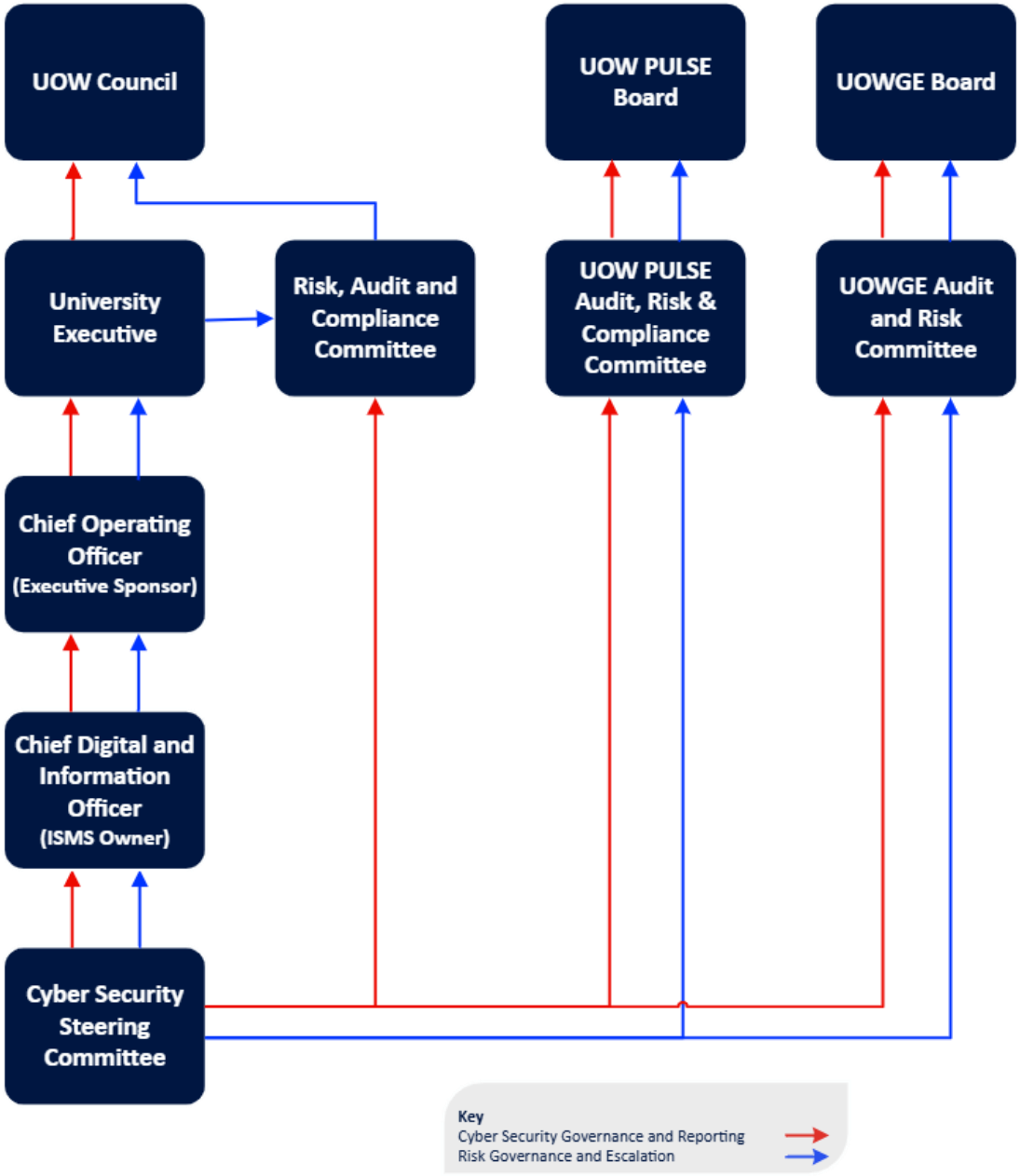
Section 5 - ISMS Governance

(9) The University's ISMS recognises that information security is everyone's responsibility. The implementation of the ISMS is overseen by the RACC and Cyber Security Steering Committee. The University's Chief Information and Digital Officer (CIDO) is the ISMS Owner.

(10) The CIDO is responsible for the operational effectiveness of the ISMS and for reporting issues relating to information security and the ISMS directly to the University Executive, Risk, Audit and Compliance Committee (RACC), PULSE Audit, Risk & Compliance Committee and UOWGE Audit and Risk Committee. This ensures a common understanding of the security issues, incidents and risks and provides a coordinated, planning body focused on information security.

a. The figure below shows the various governing bodies of the University influencing and managing activities the ISMS is dependent upon or may be dependent on the ISMS.

ISMS Governance Structure



Section 6 - Roles and Responsibilities

(11) The following table outlines the key roles and responsibilities required for the ongoing management and operation of the University ISMS together with the expected competencies and authorities.

Role	Responsibility	Competency and Authority
University Council	Highest authority across the University, with final approving authority for all departments and processes.	**Competency:** • Understand reports from University Executive, RACC and other reporting lines from the University departments. **Authority:** • Assign final authorities. • Approve policies. • Making final decisions on high level strategic, operational and financial actions across the University.

Role	Responsibility	Competency and Authority
University Executive	Top Management is defined as all members of the University Executive (UE). The responsibilities of the UE within the ISMS are to: • Provide oversight of the ISMS Owner to ensure the ISMS achieves the intended outcomes; and • Monitor and review significant security risks.	**Competency:** • Strong understanding of the University and strategic objectives. **Authority:** • Authority to assign resources.
Vice-President (VP) Operations	Senior Executive sponsoring the ISMS. The responsibilities of the VP Operations within the ISMS are to: • Champion an effective and sustainable approach to managing information security risks throughout the University's ISMS; and • Ensure appropriate organisational commitment to information security activities related to the ISMS scope.	**Competency:** • Strong understanding of the University and strategic objectives. **Authority:** • Authority to approve ISMS procedures. • Authority to assign resources.
Risk, Audit and Compliance Committee (RACC)	The Risk, Audit and Compliance Committee assists the Council in fulfilling its corporate governance and independent oversight responsibilities. With respect to the ISMS, the responsibilities for the Council are to: • Ensure the ISMS risk management practices are aligned to the University's broader risk management practices. • Reviewing cyber risk exposure for the University, ensuring cybersecurity risks are identified, managed and reviewed in a timely and appropriate manner. • Overseeing the University of Wollongong's cybersecurity framework across all domestic and international campuses. • Provide oversight of the Cyber Security Steering Committee (**CSSC**) and the ISMS governance function.	**Competency:** • Strong understanding of the University and strategic objectives. **Authority:** • Authority to audit and review ISMS governance and risk management processes.
Cyber Security Steering Committee (CSSC)	The role of the Cyber Security Steering Committee is to provide the operations functions of the ISMS. The CSSC is responsible for the following: • Respond to the direction of the ISMS Owner, RACC and UE; • Manage the implementation of the ISMS; • Update and endorse ISMS documentation including policies and procedures; • Oversee risk management activities within the context of the ISMS; • Promote this framework and ensure employees, contractors and interested parties are aware of it; • Regularly review information security risks and adequacy of controls; • Monitor changes to services or deliverables for interested parties and reassess any associated risks for such changes; • Review outcomes from information security incidents and associated corrective actions and improvements; • Review security weaknesses and facilitate improvements; and	**Competency:** • Strong understanding of ISMS concepts and requirements. **Authority:** • Authority to endorse core ISMS documents. • Authority to provide the respective business units with advice to implement security controls.

Role	Responsibility	Competency and Authority
	• Ensure audit and assurance activities are carried out as per a defined schedule. Membership of this group is defined within the CSSC Terms of Reference	
ISMS Owner	The Chief Information and Digital Officer shall act as the owner of the ISMS. The ISMS Owner is ultimately responsible for the successful operation of the ISMS and for the following activities: • Ensure the ISMS is aligned to ISO 27001; • Provide information security program visibility and report on the effectiveness of the ISMS to UE and RACC; • Facilitate provision of sufficient resources and training to ensure effective ISMS implementation; • Monitor the effectiveness of the ISMS; • Highlight major information security incidents to the RACC and UE; • Report audit findings and corrective actions to the RACC and UE • Review and approve the CSSC recommendations on major security incidents, risks and risk treatment plans, adequacy of response and controls, security audits, and corrective actions and improvements taken.	**Competency:** • Strong understanding of ISMS concepts and requirements. • Strong understanding of the organisation and strategic objectives. **Authority:** • Authority to approve local ISMS protocols. • Authority to approve local IMTS procedures. • Authority to assign resources.
ISMS Coordinator	The CISO will act as the ISMS Coordinator. The ISMS Coordinator is responsible for the overall coordination of ISMS activities, including: • Maintain ISMS documentation; • ISMS continuous improvement activities; • Coordinate risk assessments; • Ensure the activities documented in the Security Calendar are scheduled, updated and performed; • Monitor the progress on agreed activities; • Escalate any issues, as necessary, to the ISMS Owner; • Highlight major information security incidents to the CSSC; • Respond to the direction of the ISMS Owner, CSSC; • Coordinate with external security vendors and specialists as necessary for expert advice; and • Coordinate reporting on various aspects of the ISMS.	**Competency:** • Strong working understanding of ISO 27001. • ISO 27001 Implementer training (desirable). **Authority:** • Nil.
Staff	All University staff using and managing the University's ISMS (employees, contractors, suppliers and other third parties) are responsible for the following activities: • Comply with the ISMS together with any supporting policies, standards and procedures; • Comply with all established security controls; • Report security breaches and take necessary corrective actions; and	**Competency:** • Basic understanding of the ISMS's requirements. • Awareness and understanding of information security requirements, including framework and acceptable use policies. **Authority:** • Nil.

Role	Responsibility	Competency and Authority
	• Use information assets only as authorised and intended by the business owner.	
Risk Owners	Risk owners are responsible for managing risk within their area of responsibility, including: • Ensure risks within the scope of the ISMS are appropriately documented within the Protecht ISMS Risk Register; • Review and approve risks as required by the Risk Management Framework; and • Ensure that risk treatments are identified, and appropriately implemented, and residual risk is accepted, where required.	**Competency:** • Basic understanding of the ISMS. **Authority:** • Authority to approve and accept risks.
ISMS Internal Auditor	The role of the ISMS Internal Auditor is to conduct systematic and periodic checks to ensure the effective implementation and operations of the ISMS in compliance with the ISO 27001 standard. Any opportunities for improvement or areas of nonconformity are to be reported to the CSSC and the ISMS Owner.	**Competency:** • ISO/IEC 27001 Lead Auditor. **Authority:** • Nil. Must be sufficiently independent from the design and deployment of the controls within the ISMS to provide impartiality and objectivity.
UOWGE Audit and Risk Committee	The UOWGE Audit and Risk Committee assists the UOWGE Board in fulfilling its corporate governance and independent oversight responsibilities. With respect to the ISMS, the responsibilities for the Board are to: • Ensure the ISMS risk management practices are aligned to the organisation's broader risk management practices. Provide oversight of the CSSC and the ISMS governance function.	**Competency:** • Strong understanding of the UOWGE and strategic objectives. **Authority:** Authority to audit and review ISMS governance and risk management processes.
UOWGE Board	Highest authority in UOWGE, with final approving authority for all UOW Global Enterprises entities, departments and processes.	**Competency:** • Understand reports from UOWGE Audit and Risk Committee and other reporting lines. **Authority:** • Assign final authorities for UOWGE. • Approve UOWGE alignment with the University's ISMS policies. Making final decisions on high level strategic, operational and financial actions across UOWGE.
UOW Pulse Audit, Risk & Compliance Committee	The UOW Pulse Audit, Risk & Compliance Committee assists the UOW Pulse Board in fulfilling its corporate governance and independent oversight responsibilities. With respect to the ISMS, the responsibilities for the Board are to: • Ensure the ISMS risk management practices are aligned to the organisation's broader risk management practices. Provide oversight of the CSSC and the ISMS governance function.	**Competency:** • Strong understanding of the UOW Pulse and strategic objectives. **Authority:** Authority to audit and review ISMS governance and risk management processes.
UOW Pulse Board	Highest authority in UOW Pulse, with final approving authority for all UOW Pulse, departments and processes.	**Competency:** • Understand reports from UOW Pulse Audit, Risk & Compliance

Role	Responsibility	Competency and Authority
		Committee and other reporting lines. **Authority:** • Assign final authorities for UOW Pulse. • Approve UOW Pulse alignment with the University's ISMS policies. Making final decisions on high level strategic, operational and financial actions across UOW Pulse.

Section 7 - Legal, Regulatory and Contractual Obligations Management

(12) Services in scope of the University's ISMS are delivered within the following relevant Australian legal and regulatory frameworks with respect to our specific compliance requirements:

a. State Records Act 1998 (NSW)
b. Defence Industry Security Program (DISP)
c. Australian Privacy Act 1988
d. Australian Copyright Act 1968
e. Australian Criminal Code Act 1995
f. Australian Fair Work Act 2009
g. Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015
h. Privacy and Personal Information Protection Act 1998 (NSW)
i. Health Records and Information Privacy Act 2002 (NSW)
j. Museums of History NSW Act 2022 (NSW)
k. Security of Critical Infrastructure (SOCI) Act
l. Public Interest Disclosure Act 2013
m. Corporations Act
n. Taxation Administration Act
o. Government Information Public Access (GIPA) Act 2009
p. Higher Education Standards Framework (Threshold Standards) 2021
q. DTCA (where a breach involving sensitive defence related information)
r. Australian Children's Education and Care Quality Authority (ACECQA)
s. Children and Young Persons (Care and Protection) Act 1998 (NSW)
t. Education and Care Services National Regulations
u. Tertiary Education Quality and Standards Agency (TEQSA)
v. Data Sharing (Government Sector) Act 2015 No 60
w. Work Health and Safety Act 2011 (NSW)
x. Work Health and Safety Regulation 2017 (NSW)

(13) Additionally, The Australian Code for the Responsible Conduct of Research 2018, whilst not specifically required, the University's ISMS seeks to align with the regulatory requirements of our partners to best service our partners and contractual requirements.

Section 8 – ISMS Effectiveness and Improvement

Monitoring and Measuring

(14) The University will monitor the performance and effectiveness of the ISMS against the information security objectives and documented ISMS measures and metrics.

Continual Improvement

(15) The University will seek continuous improvement of the ISMS by ensuring:

a. identified nonconformities are recorded in the University's ISMS Actions Register (in Protecht);
b. major security incidents (i.e. those that require post-incident review) and the associated corrective actions are recorded in the University's ISMS Actions Register (in Protecht);
c. suggested improvements to the information asset are captured in the University's ISMS Actions Register (in Protecht); and
d. activities in the ISMS Security Calendar (in Protecht) are executed in a timely manner.

Changes to the ISMS

(16) Planned changes to the ISMS will be initially discussed as part of the management review process. Actions relating to these changes will be documented in the ISMS Actions Register (in Protecht) and managed by the CSSC as part of normal ISMS operations.

Section 9 – Management Review

(17) The CSSC will review the ISMS at each of their regular meetings. In addition, the ISMS Owner will facilitate at least one annual management review of the operations of the ISMS as outlined in the ISMS Security Calendar. This review will assess the effectiveness and practicality of the ISMS and its ability to meet organisational objectives. The management review will also consider the suitability and effectiveness of the existing policies and procedures. Outcomes from the review will be tasked to the relevant personnel and documented in the ISMS Actions Register (in Protecht) for tracking and management.

(18) Input into the annual review will include:

a. the effects on the University's ISMS of any changes to the ISO/IEC 27001:2022 standard and relevant legislation;
b. the effects of planned business changes on the ISMS;
c. status of actions from previous management reviews;
d. changes in external and internal issues that are relevant to the ISMS;
e. Changes in the needs and expectations of interested parties;
f. Trends in non-conformities and corrective actions;
g. Trends in monitoring and measurements of results;
h. Trends in audit results;
i. Trends in fulfilment of information security objectives;
j. Feedback from interested parties;
k. Results of risk assessment and status of risk treatment plan;
l. Opportunities for continual improvement;
m. Observations or recommendations following incidents;
n. Results of the education and awareness program; and
o. Review of the adequacy of resources to maintaining the ISMS and information security.

Section 10 – Reference Documentation

(19) This framework document should be read in conjunction with the following supporting documentation:

a. ISO/IEC 27001:2022 Information Security Management Standard; and
b. The University's ISMS policies and local protocols:

- Information Security Policy
- Acceptable Use of IT Resources Policy
- Backup and Archiving Local Protocol
- Encryption and Key Management Local Protocol
- Identity and Access Management Local Protocol
- Information Asset Management Local Protocol
- Information Asset Security Classification Local Protocol
- Log Management and Monitoring Local Protocol
- Malicious Code Local Protocol
- Mobile Devices and Teleworking Local Protocol
- Network Infrastructure and Configuration Local Protocol
- Patch and Vulnerability Management Local Protocol
- Physical Security Local Protocol
- Secure Deletion and Disposal Local Protocol
- Secure Development Local Protocol
- Security Assurance Local Protocol
- Supplier Security Local Protocol

Section 11 – Amendments

(20) This framework document can be amended at any time at the sole discretion of the ISMS Owner.

(21) To ensure that ISMS local protocols remain updated and contemporary, changes will be made from time to time. All relevant members will be advised of and communicated with about any change in a timely manner.

Section 12 – Definitions

Word/Term	Definition (with examples if required)
Acceptance Testing/User Acceptance Testing (UAT)	When a developed information asset (IT system or application) has been confirmed to meet its intended requirements. These requirements may be specific features its end users have requested.
ACSC	Australian Cyber Security Centre
Administrative/Privileged Account	Accounts that have been granted administrative access to an information asset (IT system) or application to perform functions that ordinary users cannot. Examples of these functions include managing system settings, defining role-based access, configurations and security.
Affiliate	Includes people holding University of Wollongong Honorary Awards as conferred by the University Council, including the awards of Emeritus Professor, Honorary Doctor and University Fellow; people appointed in accordance with the University's Appointment of Visiting and Honorary Academics Policy; and people engaged by the University as agency staff, contractors, volunteers and work experience students.
Antivirus	A program that removes malicious code from information assets.
Application Allowlisting/Application	A setting configuration that only allows a specific, pre-approved list of

Word/Term	Definition (with examples if required)
Whitelisting	programs/files to be executed/downloaded to The University's information assets.
Application Blocklisting/Application Blacklisting	A setting configuration that prevents specific programs/files being executed/downloaded to the University's information assets.
Archive	An item, record or asset required to be maintained for record-keeping purposes but not required for day-to-day University operations.
Assurance Activity Scope	The boundaries, both physical and logical, within which the assurance activity will take place. For example, an assurance activity may only verify the IT department of a campus, a specific set of buildings or a specific number of employees.
Assurance Activity Program	The schedule, processes and rules governing the assurance activity being undertaken.
Audit Features	The ability for an information asset to track who did what and when, within that information asset.
Audit Log	Files containing records of actions or occurrences completed by other information assets or files.
Authentication	A process or technology, either manual or automated, that ensures the person accessing an asset is authorised to do so.
Backup	A copy of data or files which can be restored into an information asset when the original data has been lost.
Bandwidth	The capacity limit for a certain amount of data to be passed through or across a network without that network being overloaded.
Biometric	Using the user's genetic features as a method of authentication. For example, their retina or fingerprint.
Business Continuity	The processes and information assets required to maintain the University's core services to its stakeholders.
Business Owner	An individual within the University who is nominated to assume responsibility for an information asset and is authorised to make business decisions with regard to the information asset.
Center of Internet Security (CIS)	CIS is a set of benchmarks and configurations for information asset (IT system) configurations/settings that organisations can align towards, to reduce the chance of a cyber attack.
Closed-Circuit Television (CCTV)	Information asset (camera system) that films continuously or over a period, used to monitor areas for security, crime prevention and safety.
Cloud	Information asset (computing service) by which information is stored virtually by accessing the internet, rather than through traditional local physical storage.
Command and Control Server	An external IT system, computer or website that can create or infect other IT systems with malicious software, such as rootkits.
Computer Surveillance	Surveillance, including by means of software or other equipment that monitors or records the information input or output, or other use, of a computer (including, but not limited to, local or hard drive, public network, internet and email and other electronic technologies).
Content Filtering	A setting configuration that looks for specific material, codes or patterns in downloaded programs/files and blocks them from execution if detected.
Contract/Agreement	Legally binding document establishing the minimum requirements to which both parties of the contract must adhere.
Control	Any measure or action that modifies or regulates risk.
Corrective Actions	Actions to remediate nonconformances.
Crisis	An emergency or series of incidents that seriously threatens the University's people, assets, continuity (>72hrs), the environment, its long-term prospects and/or reputation and requires strategic management of consequences.
Cryptographic Key/Key	The method of decrypting data to change it back from illegible text to legible data (to the authorised individual). Keys are usually in the form of a computer file.
Cyber Security	The practice of defending computing devices, networks and stored data from unauthorised access, use, disclosure, disruption, modification, or destruction.
Data Governance	A collection of policies, practices, and data ownership to ensure data's quality, adherence to regulatory and corporate requirements, and overall

Word/Term	Definition (with examples if required)
	efficient management.
Data Leak Prevention/Data Loss Prevention (DLP)	A set of tools and processes to detect, prevent and manage the unauthorised access, transmission or leakage of sensitive data. "Data loss" and "data leak" are related and used interchangeably. Data loss refers to the unwanted removal of sensitive data either due to a system error or malicious means. Data leak refers to the unauthorised exposure of sensitive data. Examples of DLP are Network DLP, Endpoint DLP or Cloud DLP.
Data Masking	Replacing real, live production data with fake data or obfuscating the data so it is illegible to unauthorised observers.
Deletion	Removing data/information from an information asset (device/IT system), while keeping its physical integrity intact, potentially for future re-use, selling or donating.
Development Environment	The initial environment of the development lifecycle. Initial development stages of the information asset (IT system) take place in this environment, such as the coding that covers the overall framework or architecture of the developed product.
Device/End User Device/Endpoint Device	A laptop, desktop computer, mobile phone or other device that is used to access the University's information assets.
Disposal/Destruction	Destroying a physical information asset; removing it from the ownership of the University entirely. Examples include drilling or magnetic degaussing.
Domain Name System (DNS)	The component of the internet standard protocol by which an IP address is converted into a readable domain.
Driver	Software for allowing your device to run a specific software. For example, to ensure headphones run sound from a computer, the appropriate sound driver must be installed.
Dynamic-Link Library (DLL)	An executable code for use in Microsoft IT systems.
Encryption	The act of obfuscating information or information assets to make it undecipherable to unauthorised users.
Email Account	An email account issued to a user to use whilst employed at or enrolled at the University.
Emergency	An event or series of events that arises from internal or external sources, requires an immediate response, poses risk to life, property, or continuity of operations (>1day) and/or requires strategic management of consequences.
Encryption	The act of obfuscating information or information assets to make it undecipherable to unauthorised users.
Enterprise Storage	Storage provided through IMTS that is protected from data loss; whether that storage be on premise or cloud based.
Event	A change or occurrence to the University's information assets.
External Assurance Activity	A verification of people, processes and technology against a chosen set of criteria; conducted by assessors external to the University.
Fallback	The "Plan B" that is to occur if significant issues occur during the development process. This may be in the form of a previous system version or configuration, or this may be pivoting to an entirely different development process.
File Integrity Monitoring (FIM)	A process that validates the integrity of operating system and application software files, to help detect if a cyber attack has occurred.
Firewall	An information asset (network security device), whether an application or virtual, that protects information assets and networks by applying specific rules and filtering traffic using those rules.
Firmware	The software components of a device that manages its base, low level hardware.
Formatting	Deleting the file system and index on a device or system but keeping its data intact (though inaccessible to most methods and access).
Governance	For the purposes of this Framework, governance mean the rules outlining which individual, role or group can approve what actions or documents throughout the University.
Group Policy	Settings and configurations that apply universally to all the University's devices of that type and classification.

Word/Term	Definition (with examples if required)
Hardware Token	A physical token that works like a key for a laptop/device by allowing one to access sensitive data that is only meant for them.
Hash/Hashing (Cryptography)	A one-way process to secure information using an algorithm to transform input data of any size into a value of fixed length, that is a string of nondescript text that cannot be reversed or decoded. Hashing is commonly used for integrity checks and validation checks.
HTTPS	Hypertext Transfer Protocol Secure (HTTPS) is a secure version of HTTP that encrypts data between a browser and a website. It allows users to use a website without unauthorised parties eavesdropping.
IMTS	Information Management & Technology Services at the University of Wollongong.
Incident	An information security event which may impact the confidentiality, integrity or availability of an information asset.
Information	Any digital or physical raw, processed, organised, presented or structured data created, stored or used by the University.
Information Asset	Any information, process or technology used to deliver business objectives or services. An information asset is, but not limited to: i. a physical device such as a laptop; ii. a physical server; iii. virtual server; iv. a cloud system; v. a database; vi. an application; vii. a file. For the purposes of this framework, information assets are the University's: a. Computing facilities; b. Collaboration hardware and software; c. Artificial intelligence capabilities; and d. Communications facilities. (Examples include, but are not limited to, telephones, facsimiles, mobile telephones, computers, tablets, printers, photocopiers, other devices, email, internet access, network infrastructure, web services and cloud services.)
Internal Assurance Activity	A self-driven verification of people, processes and technology against a chosen set of criteria; conducted by the University's staff separate to the implementation of the security controls or an external party on behalf of the University.
Internet-Facing Application/System/Information Asset	An application/system/information asset that is accessible from a non-University network or non-University approved VPN.
Internet-Facing Server	Servers that are directly accessible from the Internet, including those sitting behind a perimeter firewall. A server is considered internet-facing if it: • Has a public IP address or is accessible via a VIP • Accepts incoming requests from the internet (even if a firewall is in place) Examples include web server, email servers and public APIs.
Internet Protocol (IP)	The method through which devices and networks connect to the internet and other devices.
Internet Protocol (IP) Address	The virtual address of a sever, device or network. Every information asset (IT system) connected to the internet has its own unique IP address through which other information asset (IT systems and networks) can identify it.

Word/Term	Definition (with examples if required)
Intrusion Detection System (IDS)	A tool or program which monitors network traffic and information asset (IT system) activity for malware or policy violations.
Intrusion Prevention System (IPS)	A tool or program which automatically blocks certain types of traffic/malware. The specific type of blocked traffic depends on the rules configured by that program's administrators.
Information Technology (IT) Resources	The University's information and information assets.
Key Certificate/SSL Certificate	The padlock icon on a website ensuring traffic between that website and its used is secure.
Key Encryption Key	A key used to decrypt an encryption key, primarily used for added security in case the original key was compromised.
Log	Tracked record of an information asset (IT system), process, application or action completed through an information asset.
Logging	An information asset's (IT system) ability to record actions taken by or within it.
Macro	Keyboard shortcut that can potentially be used to run harmful applications, scripts or lead users to malicious websites.
Malware	Malicious software. Viruses are a type of malware.
Metadata	Data that provides details about an asset or its attributes. Metadata may be stored in a separate location or within the properties of the asset itself.
Mobile Application Management	Information asset (IT system/platform) that allows individuals to access organisational data using their own personal devices (e.g., laptops or mobile phones). It achieves this by isolating the access the user has to a compact, siloed compartment on their device, rather than across the entire device.
Mobile Device Management	Information asset (IT system/platform) allows the remote control and configuration of a University managed mobile device (such as a laptop or mobile phone).
Monitoring	An information asset (IT system or person) watching an information asset (IT system) for anomalous activity.
Multi-Factor Authentication (MFA)	An additional form of authentication to the user's main access (such as their password). For example, Microsoft Authenticator on the phone.
Network Edge	The connection or interface between a device or local network and the internet.
Network Time Protocol (NTP)	Allows an information asset (IT system) to be configured against the correct time zone of the region that the information asset (IT system) is physically located within. When a user travels to a different part of the country, the network time protocol ensures the correct time is shown on their device.
Non-disclosure Agreement (NDA)	An agreement that an individual or party will not divulge information to unauthorised parties.
Operating System	The central software that manages and connects a device's hardware and software systems. Examples include Windows, Android, macOS and Linux.
Patch	A technical/software update to an information asset (IT system), usually actioned to prevent a vulnerability being exploited. Patches can also be applied for improving an information asset's (IT system) features of look.
Partial Deletion	The process to selectively removing specific information from a dataset while retaining other related parts. This is often used to address data retention needs, comply with regulations like Australian Privacy Principles, or anonymizing data for specific purposes.
Personally Owned Device/Bring Your Own Device (BYOD)	Any technology device that was purchased by a user and not issued the University.
Plaintext	Data/information displayed as written, without encryption.
Port	A method of connection. A port can be either physical, allowing connections to a device or server, or it can be virtual. Virtual ports are virtual methods through which internet-based connections can occur. Examples of common ports are NTP, FTP, HTTP and HTTPS.
Port Number	The virtual "doorway" through which an information asset (IT system) enters and leaves through another information asset (IT system). If certain ports are blocked, certain applications cannot be used.

Word/Term	Definition (with examples if required)
Power User Account	An account with elevated privileges that are required by a user to perform their business function. Power Users are restricted to front-end functions of the information asset (IT system or application).
Principle of Least Privilege	A framework for managing access control, stating that each user is only be given the minimum access rights required for them to perform their job functions.
Privileged Account	An account that have been granted administrative access to an information asset (IT system or application) to perform functions that standard users cannot. Examples of these functions include managing system settings, defining role-based access, configurations, and security.
Production	Information asset (IT environment) used in the day-to-day operations of the University.
Proxy Log	An action where a user accesses the internet or otherwise touches the network edge.
Remote/Teleworking	Accessing the University's information assets or performing work on behalf of the University while not physically present on the University's controlled sites or campuses.
Resilience/Redundancy	The ability for information asset (IT system), entity or process to continue operating in the event of an incident or disaster.
Restore	The process of bringing a backup back to operation.
Rogue Access Point	A network connectivity entryway which was placed by an individual with malicious intent. Typically, these are placed for the purpose of users connecting to them believing they have been placed by the University.
Security Information and Event Management (SIEM)	A centralised information asset (IT system) that analyses the activity of groups of systems and alerts the IT team if it detects unusual activity on an information asset (IT system or application).
Self-Service Password Reset	When a user can reset their own password directly through an information asset (IT system), without assistance from a different person. This is almost always in the form of a "Reset Password" or "Forgot My Password" button at the login page.
Server	A server may be any of the following: • A physical or virtual server running in a University data centre offering a web application component. • A building controller device that is accessed over the network by a management server. • A virtual server instance running in a public cloud that is operated by or for the University.
Service Account	A privileged account that is the virtual identity of an information asset (IT system), used for controlling other applications or background processes.
Service Level Agreement (SLA)	A contract or agreement specifying the minimum levels of service provided by the supplier to the University. These may include uptime, incident resolution timelines and customer response timelines.
Short Message Service (SMS)	Text message to a mobile phone.
Shoulder Surfing	The act of monitoring the contents of another person's device screen or device inputs.
Signature (Digital)	The unique identifying feature or code of a file or traffic.
Single Sign-On (SSO)	"Linking" access from a user's device across multiple information assets (IT systems), for that user to only need to authenticate once rather than multiple times in the same timeframe.
Staff	All people employed by the University including conjoint appointments, whether on continuing, permanent, fixed term, casual or cadet or traineeship basis.
Staging	A test environment that is meant to be as close as possible to its live production counterpart but is still segregated for containment and security purposes.
Standard/Non-privileged User Account	A basic account, provided to a regular University staff, student or affiliate.
Standard Operating Environment (SOE)	The standard configuration settings of that information asset. These may include security settings, end user settings, application settings.

Word/Term	Definition (with examples if required)
Storage Media	Physical device that stores, or can store, data. Examples include removable hard drives, USBs, servers or laptops.
Student	A person enrolled to study or registered for a course at the University. It also includes former students of the University, students on an approved period of leave of absence or students who have been suspended from the University
Supplier/Third Party/Vendor	Any legal entity or contractor provider, legally distinct from the University, which provides services to the University.
Supply Chain	Parties which a third party may be reliant on to provide services to the University.
Technical Owner	The individual responsible for maintaining an information asset (IT system or application), throughout its lifecycle including updates, availability, security and any relevant compliance.
Threat	The source of an event which may lead to a vulnerability being exploited.
Traffic	Virtual information/data passing through an information asset (IT system) or network.
Uniform Resource Locator (URL)	Virtual address location of a website. Every website has their own unique URL. Allows users to reach a website by typing that website's URL into their internet browser's address bar.
Uninterruptible Power Supply (UPS)	A machine/power source that allows the running of an information asset (IT system) when its main source of power is down.
University	University of Wollongong and controlled entities.
University Network	The network infrastructure used by the University including all network services on main campus and satellite campuses with trusted access to the University's services. The connections can be physical (e.g. cables) or remote/wireless.
User	A person assigned a user account by the University or a person who is otherwise authorised to use the University's IT resources.
User Account	An identity assigned to a user, with an associated username, for the purpose of accessing IT resources that require authentication by the user. Also referred to as account throughout this document.
Utility Program	Any information asset (IT system) that can control or bypass other information assets (IT systems).
Virtual Private Network (VPN)	An authenticating "tunnel" which adds an extra layer of security when working remotely.
Vulnerability	Any flaw in an information asset (IT system) which can be exploited, either intentionally or unintentionally, leading to any kind of loss to the University.
Wipe/Wiping	Deleting or overwriting all information on an information asset (device or IT system). This can be actioned through technical tools or traditional physical destruction. This is considered the most secure form of data destruction.