Policy Title: **Information Security and Information Technology**

Policy Owner: **Chief Information Officer**

Keywords: **Information, Security, Risk, Applications, Planning, Architecture, Management, ICT, Technology**

Policy Code: **PL265**

---

1. INTENT:

To provide clear boundaries, expectations and accountabilities for Information Security management and the provision and management of the University's Systems, Information Assets and Information and Communications Technology (ICT) environment.

2. ORGANISATIONAL SCOPE:

This policy applies to all Authorised Users of University Information Assets and ICT resources.

All Authorised Users who are connected to University networks or services must comply with this policy, irrespective of location or device ownership, including personally owned devices.

3. DEFINITIONS:

The University Glossary and the following definitions apply to this policy.

Term:	Definition:
Authorised Users	Any person who has been granted access to University Information Assets or any part of the University's ICT environment by a person authorised by the University to grant that access.
Business Reason	Teaching, research, academic, professional and business activities required by the University.
Information Assets	Information which has been collected within a system or other digital repository, and that has a value to the University.

Information and Communications Technology (ICT)	Any device, network, system, service, infrastructure, application, database or any physical and/or virtual location that stores, transports or processes University Information Assets.
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.
Information Systems	An Information System is any organised system for the collection, organisation, storage, and communication of information. An Information System may or may not be provided by the University but is provided to Authorised Users to assist in the delivery of University business.

4. POLICY CONTENT:

Governance and Strategic Oversight

4.1. The Chief Information Officer (CIO), working within the governance arrangements and structure of the University, is accountable for achieving strategic oversight of the University's ICT environment, including determining future direction and capability, determining security posture, authorising responses to identified emerging risks and ensuring the environment remains contemporary and aligns with the University's strategic objectives.

4.2. The CIO or their nominee(s) will ensure there are robust systems and processes in place within ICT related business areas and teams, to allow the effective and efficient delivery of all core services essential to the delivery of a quality ICT environment.

4.3. Permission to proceed must be obtained from the CIO or their nominee prior to undertaking any actions which have a direct impact on the University's ICT environment. This may include purchasing and/or installing or deploying software, subscriptions, applications, or other systems not previously endorsed or approved via the University's technology governance processes. Individual/s may be personally accountable for adverse outcomes arising from acting contrary to advice provided, or for acting without seeking prior advice.

4.4. Non-compliance with this policy by an Authorised User will be investigated and, subject to the applicable provisions of relevant legislation, statutes, rules, policies and industrial agreements, action may be taken, up to and including termination of a staff member's employment and cancellation of a student's enrolment.

Information Security and Risk

4.5. The University is committed to implementing effective Information Security to protect the confidentiality, integrity and availability of the University's Information Assets and ICT environment from identified risks and potential threats.

4.6. The University will, in alignment with the University's Risk Management Framework, identify, assess and mitigate Information Security risks to Information Assets and the University ICT environment.

4.7. The University logs Information Security event data across its ICT environment for audit, operational monitoring and security incident investigation purposes.

4.8. All Authorised Users are required to read, understand and comply with the University's Acceptable Use of Information Systems policy before being granted access to any Information Systems, Information Assets or the ICT environment.

Information Management

4.9. University information should be considered in the context of the University Information Management Principles which have been established to achieve a consistent and aligned understanding, use, and management of Information Assets.

4.10. University information must, as far as is reasonable and practicable, be current and accurate, and be stored on a University provided and protected Information System. Where the use of a personal device to access/store University information cannot be avoided, the device must be password protected and kept secure. Where information has been stored, as soon as reasonable and practicable, the information must be transferred to a University provided and protected system.

4.11. All members of the University Community with access to Information Assets are required to appropriately manage and protect ECU Information Assets and the ICT environment.

Procurement and Vendor Management

4.12. The CIO is responsible for ensuring commercial and contractual suitability for all agreements relating to the purchase of and delivery of software and services, and other contracts or formalised arrangements for the delivery of ICT products and/or services.

4.13. In addition to adhering to the University's Strategic Procurement policy and associated operational documents, and in order to ensure the University is provided with specialist advice and/or information pertaining to any identified concerns or risks, the CIO or their nominee shall be consulted from the initial stages of any procurement involving additions to, or expansions of, the ICT environment.

5. ACCOUNTABILITIES AND RESPONSIBILITIES:

The CIO is the policy owner and has overall responsibility for taking all reasonable steps to ensure this policy and its associated operational documents are achievable, understood and accessible by the persons falling within the scope of the policy.

All members of the University Community with access to the ICT environment, and/or ownership of Information Assets are responsible for taking all reasonable steps to understand this policy and proactively seek guidance should there be uncertainty around any aspect of its application.

6. RELATED DOCUMENTS:

Policies

Acceptable Use of Information Systems
Creation and Management of Contracts
Privacy
Integrated Risk Management
Records Management
Strategic Procurement
Statement on Academic Freedom and Freedom of Speech

Operational documents and resources

Information Principles
Risk Management Framework

7. CONTACT INFORMATION:

For queries relating to this document please contact:

Policy Owner	Chief Information Officer
All Enquiries contact:	Vito Forte
Telephone:	6304 3737
Email address:	v.forte@ecu.edu.au

8. APPROVAL HISTORY:

Policy approved by:	Vice Chancellor
Date policy first approved:	17 November 2015
Date last modified:	29 March 2021
Revision history:	• June 2017 (Reviewed and no revisions) • October 2018 (Reviewed and redefined complete document) • March 2021 The suite of ICT policies was reviewed with a focus on ensuring they were contemporary, reflective of the current environment and principle based. Within scope were the following: PL199 PL255 PL271 The review resulted in the development of an overarching Information Security and Information Technology policy which removed the need for multiple individual policies and allowed PL199, PL255 and PL271 to be rescinded.
Next revision due:	April 2024
HPCM file reference:	SUB/68337