Policy Title: Information Security

Policy Owner: **Chief Information Officer**

Keywords: **Information, Security, Continuity, Asset, Access, Communications, IT, Compliance**

Policy Code: **PL265 [it047]**

1. INTENT

This policy defines the information security requirements for the protection of all information held by Edith Cowan University. Maintaining the Confidentiality, Integrity and Availability of any information that is stored and processed by the University or has originated from within the University's electronic and hard copy systems is a requirement of all Authorised Users of ECU information and record management keeping systems.

It applies to information collected and/or stored by the University for the purposes of conducting business, in any format including electronic and hard copy.

This policy is supported by a suite of guidelines, standards and procedures that govern the implementation of controls to address the requirements of this policy.

2. ORGANISATIONAL SCOPE

Adherence to this policy is mandatory for all Authorised Users of ECU information and record management keeping systems.

3. DEFINITIONS

TERM	DEFINITION
Authorised Users	Any individual that uses University information systems or resources in the normal course of business, i.e. ECU students, staff, council members, contractors and other relevant individuals.
Availability	Ensuring that information is available to authorised individuals, entities, or processes.
Confidentiality	Ensuring that information is not made available or disclosed to unauthorised individuals or parties.

Information Asset	Information which has importance to the University in the achievement of its goals and objectives. The worth of an Information Asset can vary depending on its use within the University. An Information Asset can be physical, as in a document, or digital, in which case it can be in many different formats, such as, database tables, video files, audio files, etc. Examples of Information Assets, include, *inter alia*, research data, academic results, student personal information, financial information, professional advice and minutes. The worth of the information asset is expressed in its Information Classification label.
Information Asset Owners	The person(s) who are accountable and responsible for ensuring that specific Information Assets are appropriately handled and managed.
Information Classification	The process of assigning an appropriate level of protection to an information asset to indicate the scope of an information assets distribution and use. An Information Classification will determine an information asset's level of protection, its distribution and use both inside and outside of the University.
Information Processing Facilities	Any system, service, infrastructure, or any physical and/or virtual location that stores, transports or processes ECU information.
Integrity	Processes designed to maintain the accuracy and completeness of data and information throughout its life-cycle.
ISO27001	International standard for Information Security Management, providing a framework of policies and procedures including all legal, physical and technical controls involved in an organisation's information risk management.

4. POLICY CONTENT

ECU has information security and business continuity management policies, guidelines and processes in order to ensure organisational sustainability by providing good information governance. In this context, information security is delivered through the following:

4.1 General Principles

4.1.1 Information security and business continuity, within the context of their role, is accepted as being the responsibility of all Authorised Users of ECU information

4.1.2 Information security and business continuity roles and responsibilities will be clearly defined and disseminated.

4.1.3 Controls surrounding access to ECU Information Assets will be documented, and where appropriate, communicated to Authorised Users of ECU information and those parties accountable and responsible for the implementation of this policy.

4.1.4 All appropriate and relevant information security controls implemented at ECU will be based on the international standard for Information Security Management (ISO27001).

4.1.5 Risk identification and management in relation to information security will be based on ECU's Integrated Risk Management Policy.

4.1.6 An ongoing ECU information security program supports the fulfilment of information security responsibilities by all Authorised Users of ECU information. This will include information provision, process improvement, risk assessments and audits.

4.2 Access to ECU Information Assets

4.2.1 Access to Information Assets owned by or entrusted to the University will be controlled on the basis of a University requirement for such access. Access will be will provisioned by a combination of physical and electronic protective measures as well as an Information Classification system.

4.2.2 ECU will establish processes and procedures to mitigate the risks of unauthorised access, data and information breaches, damage and interference to the Information Processing Facilities that process ECU data and information.

4.3 Information Distribution and Protection

4.3.1 Information will be distributed or made available to Authorised Users on the basis of the user's role, the Information Asset Classification and a University requirement that necessitates the distribution of any Information Asset approved by the Information Asset Owner.

4.3.2 Protection of ECU Information Assets will be commensurate with the Information Asset Classification. Information protection measures will ensure the University's compliance with its contractual, regulatory and legislative requirements.

4.4 Information Security Resilience

4.4.1 The University will ensure that information security is embedded in ECU's Business Continuity Plans and in its information systems back up and disaster recovery plans. This shall, as appropriate, extend to data breach notifications.

4.4.2 ECU will ensure that that the plans referred to in 4.4.1 are regularly tested and audited that the results of such tests and audits are reported to Senior Management, and where appropriate, Council.

5. ACCOUNTABILITIES AND RESPONSIBILITIES

In relation to this policy, the following positions are responsible for the following:

5.1 Policy Owner

5.1.1 Overall accountability for the content of this Policy.

5.2 Information Asset Owners

5.2.1 Accountable for embedding this Information Security Policy, and its related controls, as part of their organisational structures and processes.

5.3 Manager, Information Security Management

5.3.1 Responsible for ensuring that a formal review and re-approval of this policy takes place at least annually, and after any significant change to the business or threat environment.

5.3.2 Responsible for facilitating ECU's Information Asset Owners in embedding information security into their organisational structures and processes.

5.4 Authorised Users

5.4.1 All Authorised Users are required to comply with the content of this policy, guidelines and processes and to seek guidance in the event on uncertainty as to its application.

6. RELATED DOCUMENTS:

This policy is supported by the following policies, guidelines, standards and procedures:

- Information Security Guideline
- Acceptable Use of Information Systems Policy
- Information Security Framework Standards
- Integrated Risk Management Policy
- Records Management Policy
- Business Continuity Management Policy

7. CONTACT INFORMATION

For queries relating to this document please contact:

Policy Owner	Chief Information Officer
All Enquiries Contact:	Manager, Information Security
Telephone:	08 6304 3590
Email address:	k.owens@ecu.edu.au

8. APPROVAL HISTORY

Policy Approved by:	Vice-Chancellor
Date Policy First Approved:	17 November 2015
Date last modified:	October 2018
Revision History:	June 2017 (Reviewed and No revisions) October 2018 (Reviewed and redefined complete document)
Next Revision Due:	October 2019
TRIM File Reference	SUB/68337

Guidelines for the Information Security Policy (PL265)

1. Student Responsibilities for Information Security

Any use of the University's information, information systems or IT hardware must be in accordance with University policy including but not limited to the ECU Copyright Policy, Social Media Policy, Privacy Policy, Acceptable Use of Information Systems Policy and the Information Security Policy;

1.1 When using any University provided digital resources or assets be aware of and act in accordance with the terms of use;

1.2 When copying and sharing digital and print resources this must be done in accordance with copyright laws, any known legal restrictions and ECU Copyright Policy;

1.3 Don't share or disclose your student access account and password information to another person or third party either electronically or physically;

1.4 Observing others in attempting to compromise information security or the misuse of information or information systems should be promptly reported to the IT Service Desk;

1.5 Any ECU information you have access to should only be used for the purpose for which it was provided;

1.6 When connecting a personal device to the University's network, you should ensure that no illegal or unlicensed software is installed and the devices firmware, operating system and anti-malware products are current;

1.7 The use of tools and applications explicitly for masking activities whilst using the University's computer resources or systems is not acceptable unless by approved exception;

1.8 The use or installation of illegal or unlicensed software on any of the University's computer resources or systems is not permitted;

1.9 For the purposes of compliance with legislation etc. and compliance with the policy and these guidelines be aware that all activity on the University network and the use of University systems and information may be monitored. Failure to adhere to the policy conditions, inadvertently or otherwise, may be considered an act of misconduct and action may be taken in accordance with relevant laws, ECU statutes, by-laws, rules, policies and procedures; and

1.10 These guidelines will be updated on a regular basis as the University advances its capability to manage Information Security.

2. Staff, Council Member, and Contractor and other Relevant Individuals responsibilities

Any use of the University's information, information systems or IT hardware must be in accordance with University policy including but not limited to the ECU Code of Conduct, Email Policy, Copyright Policy, Social Media Policy, Privacy Policy, Acceptable Use of Information Systems Policy and the Information Security Policy;

2.1 Completion of ECU's information security awareness and training as required by the University;

2.2 Access and use of University systems and information should be limited to that needed for fulfilling your role;

2.3 Must take reasonable precautions when sharing personal devices as this may provide unauthorised access to ECU information or systems;

2.4 Be aware of, and adhere to any restrictions of use on any University provided digital resources and assets used. For example, library resources, Blackboard resources, copyright, etc;

2.5 Not share or disclose your access account and password information to another person;

2.6 Promptly report to the IT Service Desk, any attempts by others seeking to compromise ECU IT security, or attempting to misuse ECU information or ECU information systems;

2.7 Any ECU information you have access to should only be used for the purpose for which it was collected;

2.8 Ensure that any University Information is stored on a University approved storage facility or information system;

2.9 Ensure that when connecting any personal device to the University's network that the firmware, operating system and anti-malware products are current;

2.10 Not load any illegal or unlicensed software on to any of the University's computer resources or your own personal digital equipment if it is connected to the University's network;

2.11 The use of tools and applications explicitly for masking activities whilst using the University's computer resources or systems is not acceptable unless by approved exception;

2.12 Ensure that University Information that you deal with is handled and protected in a manner consistent with its purpose and classification;

2.13 For the purposes of compliance with legislation etc. and compliance with the policy and these guidelines be aware that all activity on the University network and the use of University systems and information may be monitored. Failure to adhere to the policy conditions, inadvertently or otherwise, may be considered an act of misconduct and action may be taken in accordance with relevant laws, ECU statutes, by-laws, rules, policies and procedures; and

2.14 These guidelines will be updated on a regular basis as the University advances it's capability to manage Information Security.

3. ACCOUNTABILITIES AND RESPONSIBILITIES

In relation to this policy, the following positions are responsible for the following:

3.1 The Chief Information Officer has the responsibility to establish policy, guidelines and standards, for the management of university information including the identification of instances of non-compliance.

3.2 The Policy Owner has overall responsibility for the content of this policy and its operation in ECU.

3.3 ECU Students, Staff, Council Members and Contractors and other Relevant Individuals (any users of University computer systems and resources) are required to comply with the content of this policy and to seek guidance in the event of uncertainty as to its application.

4. RELATED DOCUMENTS:

This guideline is supported by the following:

- Information Security Policy
- Acceptable Use of Information Systems Policy
- Information Security Framework Standards
- ECU Code of Conduct
- ECU Email Policy
- ECU Copyright Policy
- Information Management Policy (draft)
- Integrated Risk Management Policy
- ECU Software Asset Policy
- ECU Privacy Policy
- ECU Records Management Policy
- ECU Social Media Policy

5. CONTACT INFORMATION

For queries relating to this document please contact:

Guideline Owner	Chief Information Officer
All Enquiries Contact:	Manager, Information Security
Telephone:	0448 798293
Email address:	k.stones@ecu.edu.au

6. APPROVAL HISTORY

Guideline Approved by:	
Date Guideline First Approved:	
Date last modified:	
Revision History:	
Next Revision Due:	
TRIM File Reference	