Policy Title: Information Security

Policy Owner: **Chief Information Officer**

Keywords: **Security, Asset, Access, Communications, 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, processed and/or transmitted at the University is a requirement of all ECU students, staff, council members, contractors and other Relevant Individuals.

This policy applies to information 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 ECU students, staff, council members, contractors and other Relevant Individuals.

3. DEFINITIONS

TERM	DEFINITION
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, entities, or processes.
Incident Response	An organised approach to addressing and managing the aftermath of a security breach or attack
Information Asset	Information which has value to the University. The value of an Information Asset can vary depending on its business use. 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. For example, a student's unit result or a corporate document.
Information Processing Facilities	Any system, service, infrastructure, or any physical location that houses information.
Integrity	Maintaining and assuring the accuracy and completeness of data over its entire life-cycle.
Relevant Individuals	Any individual that uses the University information systems or resources in the normal course of business.

4. POLICY CONTENT

ECU must maintain an information security framework, including policies, guidelines and processes in order to assure good governance and delivered through the following:

4.1 Roles and Responsibilities

4.1.1 Information security roles and responsibilities that are clearly defined and disseminated.

4.1.2 Awareness and fulfilment of their information security responsibilities by all ECU students, staff, Council Members, contractors and other Relevant Individuals responsibilities.

4.2 Access

4.2.1 Restrict access to Information Assets owned by or entrusted to the University to those with a business need for such access.

4.2.2 Adequate protection against unauthorised access, damage and interference to the University's Information Processing Facilities.

4.3 Protection

4.3.1 Protection of Information Assets to assure the Confidentiality, Integrity and Availability of information, through appropriate use of controls, determined by risk assessment and classification.

4.3.2 Securing, protecting and managing Information Assets to comply with contractual, regulatory and legislative requirements.

4.4 Managing

4.4.1 Managing information security incidents in a consistent and effective way that is tested regularly.

4.4.2 Embedding information security continuity in all the University's business continuity management plans.

5. ACCOUNTABILITIES AND RESPONSIBILITIES

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

5.1 Policy Owner

5.1.1 The policy owner has overall responsibility for the content of this policy and its operation in ECU.

5.2 Manager, Information Security

5.2.1 The Manager, Information Security is 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 ECU, Students, Staff Council Members, Contractors and other Relevant Individuals

5.3.1 ECU students, staff, Council Members, Contractors and other Relevant Individuals are required to comply with the content of this policy 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.
- Information Management Policy (under development).
- Integrated Risk 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.stones@ecu.edu.au

8. APPROVAL HISTORY

Policy Approved by:	Acting Vice-Chancellor
Date Policy First Approved:	17 November 2015
Date last modified:	June 2017 - Reviewed – no changes

Revision History:	Added reference to “other relevant individuals”
Next Revision Due:	June 2018
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	