DATA BREACH RESPONSE PROCEDURE

Purpose and Intent

ECU is committed to protecting the privacy and integrity of the Personal Information of its staff, students, and third parties with whom it engages, together with protecting the security of its systems.

This Procedure sets out the steps to be taken where there is a potential or actual Data Breach involving ECU, its Staff or Students, or third parties with whom ECU engages. Where there is a potential or actual Cyber Security Incident, the matter should be dealt with in accordance with the DCS Cyber Security Incident Process.

This Procedure applies to all ECU staff, students, contractors, affiliates, and any third party who collects or manages Personal Information for or on ECU's behalf.

Definitions

The definitions contained in ECU's Privacy Policy and University Glossary apply to this Procedure. In addition, the following definitions apply:

TERM	DEFINITION
Data Breach	Means the loss, unauthorised access or unauthorised disclosure of Personal Information.
Serious Harm	Means harm to an individual's physical or mental well-being, finances or reputation. Examples of serious harm include: • financial fraud including unauthorised credit card transactions or credit fraud; • identity theft causing financial loss or emotional and psychological harm; • family violence; or • physical harm or intimidation.

Initial steps to be taken for a suspected or actual Data Breach or Cyber Security Incident

Students must contact their University supervisor or Unit Coordinator if they become aware that:

- Personal Information in their management or control as part of their University activities (in particular research activities), may have been lost, accessed by, or disclosed to, an unauthorised third party, or that there is a real risk that such Personal Information will be lost, accessed by, or disclosed to, an unauthorised third party; or
- there has been a suspected or actual Data Breach or Cyber Security Incident involving the University, or that there is a real risk of a Data Breach or Cyber Security Incident involving the University.

Staff who become aware of a suspected or actual Data Breach or Cyber Security Incident must complete a notification form in the manner prescribed by SGSC or DCS, where:

- Any Cyber Security Incident will be notified to the Director, Digital Campus Services, for action in accordance with the DCS Cyber Security Incident Process; and
- Any Data Breach will be notified to the Director, Strategic and Governance Services Centre (Director, SGSC), for action in accordance with this Procedure.

Either of the Director, Digital Campus Services or the Director, SGSC may determine that the matter should be addressed as a critical incident in accordance with the Critical Incident and Business Continuity Management Policy.

Data Breach Notification

The Director, SGSC may, having regard to the circumstances set out in the notification:

1. if there is insufficient evidence to warrant further investigation, take no further action;
2. determine that no Data Breach has occurred;
3. take action to resolve the matter including by contacting affected persons, or making recommendations to relevant areas of the University for improvement; or
4. escalate the matter to a response team (**Response Team**), especially if.
    - there is a real risk of Serious Harm to the individuals involved;
    - it relates to a significant number of individuals who may have been affected;
    - it suggests systemic issues with ECU's Personal Information practices or procedures;
    - there is a real risk of reputational damage to ECU; or
    - if it is otherwise appropriate in the circumstances.

The Director, SGSC may consult with relevant members of the Response Team for the purposes of determining whether the Data Breach should be escalated to the Response Team).

In determining the appropriate steps to be taken, the Director, SGSC, will have regard to whether:

- ECU is bound by any contractual or legislative obligations with respect to the handling of the Data Breach;
- there are other ECU staff with interest, authority, accountability or expertise relating to the type of information which has or may have been subject to the Data Breach, that should be notified; and
- if a third party controls the data breached or if there is a Data Breach by a third party, ECU or the third party is best placed to manage the Data Breach, having regard to the interests of the individuals involved and the University's statutory functions.

Elevating a matter to the Response Team

<u>Members of the Response Team (Response Team)</u>

The Response Team is to be convened by the Director, SGSC (or nominee) and will include at least the following personnel:

- Director, SGSC (or nominee);
- Manager, Enterprise Risk;
- Manager, Legal and Integrity;
- Chief Information Officer;
- Chief Data Officer;
- Manager, Digital Governance, Security, Risk and Operations;
- Relevant Privacy Officer; and
- at least one of the Director, Brand and Marketing or the Manager, Corporate Communications.

It should also include, as optional members, where relevant:

- ECU staff (including Executive Deans or Directors) with key interest, authority, accountability or expertise given the type of information and the persons involved with the potential Data Breach;
- Director, Human Resources Services Centre, if the matter relates to ECU Staff;
- Director, Office of Development and Alumni Relations, if the matter relates to student alumni; and
- Director, Research Services if the matter relates to research involving ECU staff or students.

Procedure for Response Team

Data Breaches must be dealt with on a case-by-case basis, by assessing the potential level of harm, impact and risk involved, and using that assessment to decide the appropriate course of action. There are four key steps the University will consider when responding to a suspected Data Breach that has been elevated to the Response Team:

STEP 1 **Consider making notifications**	• Determine whether individuals, third parties, or reporting agencies should be notified (e.g. the Australian Information Commissioner where required under the *Privacy Act 1988* in relation to tax file number information, law enforcement agencies, or any party to which the University has a contractual obligation). • Determine who is responsible for making such notifications on the University's behalf.

STEP 2
 	
Containment and preliminary assessment
	• Immediately take steps to contain the Data Breach:
	  ○ **DCS** to be alerted if physical access to information is an issue.
	  ○ **DCS** to secure and protect information in accordance with ECU's information technology security policies, business continuity plans, and industry best practice.
	• Convene a meeting of the Response Team (virtual or otherwise).
	• Inform the ECU Executive, provide ongoing updates on key developments.
	• Preserve evidence that may be valuable in determining the cause of the Data Breach, or that may allow ECU to take appropriate corrective or preventative action.
	• **Brand and Marketing** to consider developing a communications or media strategy to manage public expectations and media interest.
	• If third parties are involved in the Data Breach, determine the best means to engage with such parties, having regard to any relevant contractual or statutory obligations.

STEP 3
 	
Evaluate and determine risk of harm
	• Conduct an initial investigation, and promptly collect information about the Data Breach, including:
	  ○ the date, time, duration, and location of the Data Breach;
	  ○ the type of information access;
	  ○ how the potential Data Breach was discovered and by whom;
	  ○ the probable cause and extent of the Data Breach;
	  ○ a list of potentially affected individuals; and
	  ○ the risk of Serious Harm to the potentially affected individuals.
	• Establish the cause and extent of the Data Breach.
	• Assess priorities and risks based on what is known.
	• Reconsider notifications (step 1) as the initial investigation is undertaken.

STEP 4 **Review the incident and take necessary preventative action**	• Fully investigate and assess the cause of the Data Breach. • Take necessary and remedial action to prevent further Data Breaches occurring or re-occurring. • Ensure notifications (step 1) have been sufficient. • Report to the ECU Executive on investigation outcomes, remedial actions, and improvement recommendations. • Report to relevant stakeholders, which may include the relevant Executive Dean or Director (or equivalent), University Executive, and QARC.

Relevant personnel should ideally undertake steps 1, 2 and 3 either simultaneously or in quick succession. The Response Team will keep appropriate records of the suspected Data and its actions, including remedial actions and any decisions made, in accordance with ECU's record keeping policies and appropriate confidentiality restrictions.