Data Breach Procedure

Version 1 – Approved 8 March 2022

Contents

Purpose

The purpose of this procedure is to:

a) describe the roles and responsibilities of University community members when responding to data breaches;
b) explain the steps and processes to be undertaken when responding to data breaches; and
c) detail how the University will notify relevant authorities and affected individuals and entities of a data breach.

Applicable governance instruments

Instrument	Section	Principles
Data and Information Governance Policy	1 Privacy	1.1-1.7
	2 Cyber security	2.1-2.4
	3 Information, communication and technology services and facilities user agreement	3.1-3.6
	4 Data and information management	4.1-4.2, 4.4

Risk Management and Business Resilience Policy	1 Risk Management 3 Crisis Management	1.3-1.6 3.1-3.4
Communications and Brand Policy	1 Communication	1.1
Privacy Act 1988 (Cth)	Part IIIC	N/A
Personal Information Protection Act 2004 (Tas)	Schedule 1	N/A
Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth)	Part 2B	N/A

Procedure

1. Introduction

1.1. The University collects personal information for many different purposes in accordance with our Privacy Statements, and uses, stores, manages and destroys that information in accordance with legislative requirements.

1.2. A data breach occurs when personal information is subject to unauthorised access or disclosure, or where the information is lost and unauthorised access or disclosure is likely to occur. A data breach can be accidental or intentional in nature.

1.3. Examples of a data breach may include:

- the loss or theft of a device containing personal information
- a University database or information repository containing personal information being hacked or accessed without authorisation
- the University mistakenly providing personal information to an unauthorised person or entity.

1.4. A data breach becomes an "eligible data breach" when:

- there is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information, that the University holds
- this is likely to result in serious harm to one or more individuals and
- the University hasn't been able to prevent the likely risk of serious harm with remedial action.

1.5. The University recognises the seriousness of data breaches within its Risk Management Framework, wherein a "major data breach" is reflected as a Tier 1 operational risk.

2. Roles and responsibilities

2.1. Key roles and responsibilities in the investigation and management of a suspected data breach are identified throughout the procedure and summarised within Attachment 1.

3. Timeframes

3.1. This table details the timeframes imposed under relevant legislation that the University must comply with when responding to a suspected data breach.

Legislation	Requirement
Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth) (SOCI Act)	Must report a critical cyber security incident to the Australian Cyber Security Centre as soon as practicable, and in any event **within 12 hours**, after the entity becomes aware. Must report other types of cyber security incidents to the Australian Cyber Security Centre as soon as practicable, and in any event **within 72 hours**, after the entity becomes aware.
General Data Protection Regulation (GDPR; European Union)	Must notify the supervisory authority competent **within 72 hours** after having become aware of the personal data breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the natural persons impacted.
Privacy Act 1988 (Cth)	The assessment of a suspected eligible data breach must be reasonable and expeditious and must occur **within 30 days** after becoming aware of the suspected eligible data breach. The University must notify the Office of the Australian Information Commissioner (OIAC) **as soon as practicable** after it becomes aware that there are reasonable grounds to believe that there has been an eligible data breach. The University must then notify affected individuals of the content of the notification to the OAIC **as soon as practicable** after the notification to the OAIC.

4. Step 1: Contain

Reporting data breaches

4.1. If a University community member becomes aware of an actual or suspected data breach, they must report it as soon as possible via email to databreach@utas.edu.au. University staff may also report details of the data breach via the "Report A Data Breach" form located in the University's Service Portal.

4.2. University community members should also:

- Take all action possible to contain the data breach and act on advice provided by IT Services or Compliance.
- Otherwise keep the incident confidential except where it is necessary to disclose information about the incident in accordance with this Procedure.

Containing data breaches and remediating harm

4.3. If the data breach involves the possible unauthorised disclosure of personal information to a third party, the reporting person may:

- if the breach was an email, send a separate email to the recipient requesting that the original email be deleted (if it remains unopened) or, if that original email has been opened, request that the contents of it not be disclosed to any other person and the email be deleted.

- if the breach was by post, contact the recipient and ask them not to open or read the posted materials, or, if they have been opened and read, not to disclose the contents of the posted materials to any other person. The University will arrange for the materials to be returned to the University or to be appropriately destroyed.

5. Step 2: Assess

Investigating reported data breaches

5.1. Cyber Security and Compliance must conduct a preliminary investigation of any report of an actual or suspected data breach as soon as reasonably practicable to determine:

- if a breach has occurred, and
- if it is an eligible data breach.

5.2. This will include assessing the facts of the suspected breach, what containment and/or remediation actions have already been undertaken (if any), and whether any further actions are required.

5.3. When conducting this preliminary investigation, Cyber Security and Compliance must be mindful of the relevant mandatory legislative reporting timeframes detailed within paragraph 3 of this Procedure.

5.4. Cyber Security will oversee investigation of breaches that have occurred through University ICT systems, or cloud services/external systems that contain University data.

5.5. Where there is a data breach, Compliance must report the findings of the preliminary investigation and assessment to General Counsel (the University's Privacy Officer) and the Chief Information Officer as soon as possible. The report should include an opinion on whether the data breach is an eligible data breach.

Reviewing assessment of data breach and escalation

5.6. General Counsel will assess the findings of the preliminary investigation to determine whether the data breach is an eligible data breach and is likely to result in serious harm to the affected individuals (including with reference to the University's risk rating matrix).

5.7. General Counsel and the Chief Information Officer will also consider:

- Whether the steps taken by the University to date in response to the breach have been appropriate and effective or should be amended, and
- Whether any external service providers (such as specialist IT support) are required and allocate sufficient resourcing to support this.

Non-eligible data breaches

5.8. If General Counsel determines that the data breach is not an eligible data breach, Compliance will record the incident in the University non-compliance register.

Eligible data breaches

5.9. Where General Counsel determines that an eligible data breach has occurred but that the breach is relatively minor (for example, when there has been no external compromise of personal information), the response to the eligible data breach may be undertaken by Compliance and IT/Cyber Security.

5.10. Where General Counsel assesses the eligible data breach to be a major incident, General Counsel and the Chief Information Officer may convene the Crisis Management and Recovery Team

(CMRT). Members of the CMRT will be assigned tasks in a manner that ensures containment and assessment activities are prioritised.

6. Step 3: Notify

Notifications under the Privacy Act and the GDPR

6.1. If General Counsel determines that the data breach is an eligible data breach, the University must notify in accordance with the relevant legislation.

6.2. Notifications must be approved by General Counsel prior to being sent.

6.3. General Counsel (or delegate) must keep a record of:

- the date, time and method of notification to each individual, and
- if available, any confirmation of receipt of the notification received from an individual (unless the data breach affects so many individuals that individual notifications are impractical).

Reporting under the SOCI Act

6.4. If General Counsel or Chief Information Officer determine that the suspected data breach incident is a reportable cyber security incident under the SOCI Act, the University must notify in accordance with that legislation. Attachment 2 of this Procedure details this process.

6.5. If General Counsel and Chief Information Officer are unavailable and unable to assess whether the suspected data breach incident is a reportable cyber security incident within the legislative timeframes, Cyber Security or Compliance may instead make this determination. In this event, Cyber Security or Compliance must as soon as practicable after making this determination provide an oral or written briefing to General Counsel and Chief Information Officer.

7. Step 4: Review

Conducting post-data breach review

7.1. In the event of a major data breach that required a CMRT response, the CMRT will undertake a post-incident review.

7.2. For any other eligible data breach incidents, IT Services/Compliance will jointly undertake a post-incident review.

7.3. These reviews may, among other things, undertake the following actions:

- complete any further investigation as necessary or desirable;
- determine whether any data handling or data security practices led or contributed to the relevant data breach; and
- consider whether there are any further actions that need to be taken because of the data breach.

8. Reporting

8.1. Following a review, Compliance will:

- update the University non-compliance register, and
- provide a written report to the Audit and Risk Committee with findings and recommendations for further actions.

9. Annual review, training and testing of the Procedure

9.1. The Chief Information Officer is responsible for organising an annual data breach response exercise for electronic data breaches. The findings of the exercise will further refine this Procedure and increase awareness and understanding of the role that each stakeholder has in the event of a data breach.

10. Additional resourcing and funding

10.1. General Counsel and the Chief Information Officer are responsible for ensuring appropriate resourcing and funding is in place to respond to data breaches.

Related procedures

Information Management Procedure

Versions

Version	Action	Approval Authority	Responsible Officer/s	Approval Date
Version 1	Approved	Chief Operating Officer	General Counsel	8 March 2022

Attachment 1 - Key roles and responsibilities

Key roles and responsibilities in the investigation and management of a suspected data breach are contained within the below table.

University community members	• Identify and report suspected data breaches. • Protect any personal information held by the University against unauthorised disclosure. • Participate in data breach investigations as required.
IT Services	• Provide specialised advice to the individual reporting the incident on options for preventing further damage and preserving evidence of the possible breach.
Cyber Security	• The technical lead for all suspected or actual data breach incidents. • Lead the management of all data breach remediation and containment efforts. • With Compliance, conduct a preliminary investigation into the breach. • Provide advice and support to the Chief Information Officer, General Counsel, and the CMRT as required.
Compliance	• The privacy lead for all suspected or actual data breach incidents. • With Cyber Security, conduct a preliminary investigation into the breach. • Report findings of the preliminary investigation to General Counsel and the Chief Information Officer. • Record incidents in the University non-compliance register. • Provide advice and support to General Counsel, the Chief Information Officer, and the CMRT as required.
Chief Information Officer	• Receive preliminary investigation findings from Compliance. • With General Counsel, assess whether the University's response to the breach has been effective or needs to be amended. • Where necessary, allocate additional ICT and funding resources – including obtaining external support – to respond to the breach. • Participate in the CMRT. • Organise annual data breach exercise.
General Counsel (UTAS Privacy Officer)	• Manage the University's Data Breach Procedure. • Oversee the University's compliance to the Notifiable Data Breaches Scheme. • Assess whether an eligible data breach has occurred and, where relevant, approve any Notifiable Data Breach Statements.

	• Where relevant, notify the Office of the Australian Information Commissioner (OAIC), Ombudsman, other entities and affected individuals of the breach.
Data, Information Management and Cyber Security Governance Committee	• Promote the adoption of information management and information and communications technology (ICT) security controls to ensure integrity, availability and confidentiality of personal information. • Provide guidance on improvements to protect personal information from unauthorised disclosure.
Audit and Risk Committee	• Receive and review internal audit reports and management responses relating to data breaches.

Attachment 2 – Summary of cyber security incident reporting obligations under SOCI Act

	Critical cyber security incident	**Other type of cyber security incident**
When does it apply?	Part 2B obligations will not commence until 3 months after the Security of Critical Infrastructure (Application) Rules 2021 are registered on the Federal Register of Legislation.	Part 2B obligations will not commence until 3 months after the Security of Critical Infrastructure (Application) Rules 2021 are registered on the Federal Register of Legislation.
Cyber security incident	one or more acts, events or circumstances involving any of the following: (a) unauthorised access to: (i) computer data; or (ii) a computer program; (b) unauthorised modification of: (i) computer data; or (ii) a computer program; (c) unauthorised impairment of electronic communication to or from a computer; (d) unauthorised impairment of the availability, reliability, security or operation of: (i) a computer; or (ii) computer data; or (iii) a computer program.	one or more acts, events or circumstances involving any of the following: (a) unauthorised access to: (i) computer data; or (ii) a computer program; (b) unauthorised modification of: (i) computer data; or (ii) a computer program; (c) unauthorised impairment of electronic communication to or from a computer; (d) unauthorised impairment of the availability, reliability, security or operation of: (i) a computer; or (ii) computer data; or (iii) a computer program.
When does the reporting obligation arise?	When an entity becomes aware that: (a) a cyber incident has occurred or is occurring; and (b) the incident is having or has had a significant impact on the availability of the asset.	When an entity becomes aware that: (a) a cyber incident has occurred, is occurring or is imminent; and (b) the incident has had, is having or is likely to have, a relevant impact on the asset. *Note: the relevant impact may be on the availability, integrity or reliability of the asset and confidentiality about information relating to or stored in the asset or computer data.*
Who must report?	Responsible entity for the critical infrastructure asset i.e. the university	Responsible entity for the critical infrastructure asset i.e. the university

Timing for report?	As soon as practicable, and in any event **within 12 hours**, after the entity becomes aware.	As soon as practicable, and in any event **within 72 hours**, after the entity becomes aware.
How to report?	Give an oral or written report. If an oral report is given, the responsible entity must make a written record of the report in the approved form and give a copy to the Australian Cyber Security Centre **within 84 hours** after the oral report is given.	Give an oral or written report. If an oral report is given, the responsible entity must make a written record of the report in the approved form and give a copy to the Australian Cyber Security Centre **within 48 hours** after the oral report is given.
Penalties	Penalties of up to 50 penalty units exist where reports are not given within the required time frames or approved form	Penalties of up to 50 penalty units exist where reports are not given within the required time frames or approved form

Further guidance is available from the Australian Cyber Security Centre and the Cyber and Infrastructure Security Centre.