Data Breach Response Plan Schedule

1 Purpose

To define the process where actual, suspected or potential Data Breaches are identified, reported, assessed and managed.

2 Scope

This Response Plan applies to all University staff responsible for the creation, use or storage of University Data requiring approval to leave the custody and control of the University. This includes but is not exclusive to; Research Data, personally identifiable Information, communications and Intellectual Property. This Response Plan does not extend to complaints of alleged privacy breaches made against the University by individuals, nor alleged privacy breaches of the University's contracted service providers. This Response Plan applies to actual, suspected or potential Data Breaches involving the loss of, unauthorised access to, or unauthorised disclosure of, University Data or University Repositories. This response plan provides the actions to be taken aligned to Incident Management provisions as per section 4.12 of the ICT Information Management and Security Policy. This Data Breach Response Plan is publicly accessible on the University's website to comply with transparency obligations under the *Information Privacy Act 2009* (Qld) and the Mandatory Data Breach Notification Scheme.

3 Schedule

This Response Plan sets out the processes to be followed by University staff in the event that the University experiences a Data breach or suspects that a Data Breach has occurred. A Data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, University Data or University Repositories.

The IP Act does not impose a mandatory obligation on agencies to notify the Office of the Information Commissioner (OIC) or affected individuals in the event of a Data Breach. However, it is strongly recommended that agencies notify the OIC and affected individuals when a Data Breach is likely to cause serious harm to any individuals.

The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (the NDB Act) does impose a mandatory obligation on organisations covered by the Act to notify any individuals likely to experience serious harm by an Eligible Data Breach. The Office of the Australian Information Commissioner (OAIC) must also be notified.

Accordingly, the University needs to be prepared to act quickly in the event of a confirmed or suspected Data Breach to determine whether it is likely to result in serious harm, and whether it constitutes an Eligible Data Breach.

Adherence to this Response Plan will ensure that the University can contain, assess and respond to Data Breaches expeditiously and mitigate potential harm to the person(s) affected.

This document should be read in conjunction with the University's Privacy Policy and Procedure.

4 Process where a breach occurs or is suspected

4.1 Alert

Where an Eligible Data Breach is known to have occurred, or is suspected, any University staff member or Student who becomes aware of this must, within one business day, alert ICT in the first instance. For Students, this alert can be made by emailing databreach@usq.edu.au or via iConnect. For staff, they should complete an alert request in the “ServiceHub”.

Information that should be provided, if known, at this point includes:

1. When the breach occurred (time and date).
2. Description of the breach (type of University Data involved and individuals impacted).
3. Cause of the breach and how it was discovered.
4. Which systems (if any) are affected.
5. Which division is involved.
6. What corrective action (if any) has occurred to remedy or mitigate impacts of the breach, or suspected breach.

4.2 Assess the severity of harm and potential impact

Once notified, the Chief Digital Information Officer must make a preliminary assessment as to the severity and potential impact of the breach, or suspected breach. If Personal Information is involved in the breach, immediate notification should be made to the Privacy Officer so that a joint preliminary assessment of severity of harm can be made with the Chief Digital Information Officer.

4.2.1 Criteria for assessing severity of harm

1. The type and extent of Personal Information involved.
2. The number of individuals affected.

3. Whether the Personal Information is protected by any security measures (password protection or encryption).

4. The person or kinds of people who now have access to the Personal Information.

5. Whether affected individuals are likely to experience serious harm.

6. Whether there could be Media or stakeholder attention from the breach or suspected breach.

7. How the University Data could be used (could it cause reputational harm or financial loss to the University and should our insurers be notified).

8. Whether theft of University Data was a potential cause (could Corrupt Conduct be involved and should law enforcement be notified).

Once a preliminary assessment of the severity and potential impact of the breach or suspected breach has been made by the Chief Digital Information Officer, the Privacy Officer will be notified and required to keep a record of the preliminary assessment (prepared or informed by the Chief Digital Information Officer).

4.3 Assess whether an Eligible Data Breach has occurred

Once notified by the Chief Digital Information Officer, the Privacy Officer (in consultation with the Chief Digital Information Officer) must make a preliminary assessment as to whether an Eligible Data Breach has occurred and what notification to individuals and regulators is required (if any). The Privacy Officer will then determine if the Data Breach should be managed at the local level or escalated to the Data Breach Response Team (Response Team). This determination will depend on the nature and severity of the breach. This Decision will then be communicated with the Chief Operating Officer and Chief Financial Officer and the Vice-Chancellor, by the Privacy Officer.

If a data breach involves a contracted service provider or cloud-hosted platform acting on behalf of the University, the University will treat the information as 'held' for the purposes of the IP Act. The University will ensure contractual arrangements require timely notification and cooperation in accordance with the Mandatory Data Breach Notification Scheme.

4.3.1 Data Breach managed at the division level

Where the Privacy Officer determines that the Data Breach is to be managed at the local level, the Chief Digital Information Officer must:

- Ensure that immediate corrective action is taken (if this has not already occurred). Corrective action may include:

    - retrieval or recovery of the Personal Information,
    - ceasing unauthorised access,
    - shutting down or isolating the affected system.
- The Chief Digital Information Officer must also provide any additional comments to the Privacy Officer, within two business days of receiving instructions under 4.3, that need to be added to the preliminary assessment report. The report must contain responses to the following items:
    - Description of breach or suspected breach
    - Action taken
    - Outcome of action
    - Processes that have been implemented to prevent a repeat of the situation
    - Recommendation as to whether further action is necessary

The preliminary assessment report will be logged by the Privacy Officer with a copy provided to the Chief Operating Officer and Chief Financial Officer and Vice-Chancellor.

4.3.2 Data Breach managed by the Response Team

Where the Privacy Officer determines that the Data Breach must be escalated to the Response Team, the Chief Digital Information Officer will convene the Response Team and notify the Chief Operating Officer and Chief Financial Officer and Vice-Chancellor.

The Response Team can be made up of a combination of the following persons:

- Persons from one of the Business Continuity and Crisis Management Teams, ie Strategic Crisis Group, Operational Crisis Group, Crisis Communications Group
- Chief Digital Information Officer
- Privacy Officer
- Legal Services (General Counsel or nominee)

The following persons may also be added to the Response Team dependant on impact:

- Chief People Officer (or nominee)

- Provost (or nominee)
- Deputy Vice-Chancellor (Academic Affairs) (or nominee)
- Deputy Vice-Chancellor (Research and Innovation) (or nominee)
- Pro Vice-Chancellor (Engagement) (or nominee)
- Director (Integrity and Professional Conduct)
- Chief Operating Officer and Chief Financial Officer nominee

4.4 Role of the Response Team

The Response Team will deal with every incident on a case-by-case basis by assessing the circumstances and associated risks, to inform an appropriate course of action.

4.4.1 Response Team actions

The Response Team may undertake any of the following actions during its assessment, once convened:

- Immediately contain the breach (if this has not already occurred). Corrective action may include: retrieval or recovery of the Personal Information, ceasing unauthorised access, shutting down or isolating the affected system.
- Confirm or change the preliminary assessment by the Chief Digital Information Officer regarding the severity and impact of the breach.
- Confirm or change the preliminary assessment by the Privacy Officer regarding whether the breach amounts to an Eligible Data Breach, and what notifications to individuals and regulators are necessary.
- Determine whether notifications to other professional bodies, insurers, the State Archivist, or financial institutions are necessary.
- Assess whether theft of University Data may have been a potential cause and determine if reports to law enforcement or the Crime and Misconduct Commission are necessary.
- Collect and document any additional Information about the breach details to add to the preliminary assessment report, logged by the Privacy Officer. This report will inform the preparation of any incident report to the Audit and Risk Committee of Council, and Lesson Learnt report for the Vice-Chancellor's Executive, if necessary.
- Call upon the expertise of, or consult with, relevant staff, as appropriate.

- Engage an independent cyber security or forensic expert, as appropriate.
- Develop a communication or Media strategy including the timing, content, and method of any announcements to Students, staff or the Media.
- Recommend activities to be undertaken by the University to prevent or mitigate a repeat of the breach.
- Determine if an audit of relevant operations or areas is required to ensure recommendations are implemented and effective.
- Any other actions deemed necessary by the Response Team.

The Response Team must undertake its assessment within two business days of being convened. The Privacy Officer will provide periodic updates to the Vice-Chancellor, as appropriate.

4.5 Notification

If the Response Team determines that the breach is an Eligible Data Breach requiring mandatory or non-mandatory notification to a regulator, the Privacy Officer must prepare a recommended prescribed statement for approval by the Vice-Chancellor and provide a copy to the OAIC or OIC, as soon as practicable (and no later than 30 days after becoming aware of the breach or suspected breach). Notifications will include all details required as per OIC Guidelines.

The Privacy Officer must also prepare a recommended prescribed statement for approval by the Vice-Chancellor for notification to affected individuals. The University should notify the affected individuals directly, eg by phone, letter, email or in person. Indirect notification, eg by Notice on the University's website or by Media release, should generally be reserved for when direct notification is prohibitively expensive, or could cause further harm.

Records of any and all notifications attempted and made will be logged by the parties making the notifications.

4.6 Data Breach Register

All data breaches, whether notifiable or not, must be recorded in the University's Data Breach Register. The Register will include the date of breach, description, type of personal information involved, number of individuals affected, risk assessment outcome, notifications made, and remedial actions taken. This is required under section 72 of the *Information Privacy Act 2009* (Qld).

4.7 Response Plan Review

This Response Plan will be reviewed on at least an annual basis, or following actual, suspected or potential Data Breaches. It will be re-evaluated in line with any changes to business processes, planning, legal and contractual requirements

5 References

- NBD Act - https://www.oaic.gov.au/privacy/notifiable-data-breaches
- Australian Privacy Principles - https://www.oaic.gov.au/privacy/australian-privacy-principles
- Privacy ACT 1988 - https://www.legislation.gov.au/Series/C2004A03712

This Response Plan has been informed by:

- The Office of the Australian Information Commissioner's “Guide to developing a data breach response plan”
- The Office of the Australian Information Commissioner's “Data breach notification guide: a guide to handling personal information security breaches”
- The Office of the Information Commissioner's “Guideline on privacy breach management and notification”
- The NDB Act
- The Act and Australian Privacy Principles (Schedule 1 of the Act)
- The IP Act and the Information Privacy Principles (Schedule 3 of the IP Act)

6 References

Nil.

7 Schedule Information

Accountable Officer	Chief Operating Officer and Chief Financial Officer
Responsible Officer	Chief Digital Information Officer
Policy Type	University Procedure
Policy Suite	ICT Information Management and Security Policy

Approved Date	3/11/2025
Effective Date	3/11/2025
Review Date	13/10/2027
Relevant Legislation	*Crime and Corruption Act 2001* (Qld) *Information Privacy Act 2009* (Qld) *Privacy Act 1988* (Cth) *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth) *Public Records Act 2023* (Qld)
Policy Exceptions	Policy Exceptions Register
Related Policies	Acceptable use of ICT Resources Policy Assets Policy Code of Conduct Policy Handling Personal Student Information Policy and Procedure Intellectual Property Policy Marketing and Brand Policy Privacy Policy
Related Procedures	Commercialisation of Intellectual Property Procedure Intellectual Property Procedure Privacy Procedure Website Procedure
Related forms, publications and websites	Privacy Plan
Definitions	**Terms defined in the Definitions Dictionary**
	Corrupt Conduct Defined in section 15 of the Crime and Corruption Act 2001 . Council

Council means the governing body, the University of Southern Queensland Council.

Decision

A determination made by an Employee, contractor or other authorised delegate in the course of their duties on behalf of the University.

Information

Any collection of data that is processed, analysed, interpreted, organised, classified or communicated in order to serve a useful purpose, present facts or represent knowledge in any medium or form. This includes presentation in electronic (digital), print, audio, video, image, graphical, cartographic, physical sample, textual or numerical form.

Intellectual Property

The result of an individual's intellectual endeavours that is capable of being protected by legal rights. Examples include, but are not limited to: inventions and discoveries in relation to new products and processes that can be protected by a patent; Copyright in Teaching Materials; other works in which Copyright subsists including literary works (including computer programs), dramatic works, musical works, artistic works, films, sound recordings, broadcasts, published editions and certain types of performances; industrial designs, which protect the shape, configuration, pattern or ornamentation of a product, that is, what gives a product a unique appearance; plant breeders' rights, which protect varieties of plants and trees; trademarks, which protect the branding, reputation and goodwill of products and services; circuit layout rights, which protect the layout plans or designs of electronic components in integrated circuits, computer chips, or semi-conductors used in personal computers and computer-reliant equipment; and trade secrets and know-how, that is, knowledge about products, processes, and inventions and discoveries: prior to the time they are incorporated into a publication or become the subject of a patent or design application; or which are never made the subject of an application for Intellectual Property registration.

Media

All print, radio, television and electronic Media including the internet and allied distribution channels. Includes social Media which are works of user-created video, audio, text or multimedia that are published and shared in a social environment, such as a blog, podcast, forum, wiki, or video hosting site. More broadly, social Media refers to any online technology that enables people to publish,

converse and share content online.

Notice

A Notice from the University is a document, whether physical or electronic. A Notice may be: given by hand to the addressee or delivered to the address provided by the addressee to the University; or sent by registered or pre-paid mail to the address provided by the addressee to the University; or sent by electronic communication to the University-issued email account provided by the University to a Student during the period of Enrolment until the completion of their program; or sent by electronic communication to the email address provided to the University by an addressee not enrolled at the University. A Notice is taken to be received if: given by hand to the addressee or delivered to the address provided to the University by the addressee; or sent by registered or pre-paid mail - three University Business Days after the date of posting; or sent by electronic communication - at the time that would be the time of receipt under the Electronic Transactions Act 1999 or its succeeding legislation. A Notice that would be deemed to have been received out of business hours or on a non-University Business Day will instead be deemed received on the next University Business Day.

Personal Information

Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable from the information or opinion - (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not.

Research Data

Researchers have a responsibility to retain clear, accurate, secure and complete records of research data. It is critical that data includes records necessary for the reconstruction and evaluation of reported results and processes leading to those results. Research data relates to facts, observations, measurements or experiences on which an argument, theory or test is based. Research Data may be numerical, descriptive, visual or tactile. It may be raw, or analysed, experimental or observational and may be held in any format or media. Examples include, but are not limited to: Laboratory notebooks; Field notebooks; Primary Research Data; Questionnaires; Audio and video recordings; Photographs; Films; Test responses, and Any other records that are necessary for the reconstruction and evaluation of the reported results of research. Research Collections may include slides, specimens, samples and artefacts; with related provenance information. Research data (and primary materials) includes evidence supporting findings.

For example, in the Creative Arts this may include early drafts and concept documents prior to the final output of the creative work.

Student

A person who is enrolled in a UniSQ Upskill Course or who is admitted to an Award Program or Non-Award Program offered by the University and is: currently enrolled in one or more Courses or study units; or not currently enrolled but is on an approved Leave of Absence or whose admission has not been cancelled.

University

The term 'University' or 'UniSQ' means the University of Southern Queensland.

University Members

Persons who include: Employees of the University whose conditions of employment are covered by the UniSQ Enterprise Agreement whether full time or fractional, continuing, fixed-term or casual, including senior Employees whose conditions of employment are covered by a written agreement or contract with the University; members of the University Council and University Committees; visiting, honorary and adjunct appointees; volunteers who contribute to University activities or who act on behalf of the University; and individuals who are granted access to University facilities or who are engaged in providing services to the University, such as contractors or consultants, where applicable.

Vice-Chancellor

The person bearing the title of Vice-Chancellor and President, or as otherwise defined in the University of Southern Queensland Act 1998 , including a person acting in that position.

Definitions that relate to this schedule only

Data Breach

A data breach involves the loss of, unauthorised access to, or unauthorised disclosure of, University data and/or University repositories.

Eligible Data Breach

As defined under the NDB Act.

University Data

	Can include: research data, personally identifiable information, communications and intellectual property (broader than just 'personal information' under the IP Act). **University Repositories** University systems used to store university records and data.
Keywords	
Record No	22/620PL