Privacy Data Breach Response Process

A. What is a Privacy Data Breach?

A privacy data breach is unauthorised access or disclosure of personal information, or loss of personal information. Personal information is information about an identified individual or an individual who is reasonably identifiable.

A privacy data breach may be caused by malicious action (either external or internal), human error, or a failure in information handling or security systems.

Examples include:

- loss or theft of physical devices (such as laptops and storage devices) or paper records that contain personal information
- unauthorised access to personal information by an employee
- unauthorised access to personal information by an external party
- inadvertent disclosure of personal information due to 'human error', for example an email sent to the wrong person
- disclosure of an individual's personal information to a scammer, as a result of inadequate identity verification procedures.

B. Privacy Data Breach Response Process

The University's Privacy Data Breach Response Process is comprised of four steps:

- **Step 1: Report and contain** the privacy data breach to prevent any further compromise of personal information.
- **Step 2: Assess** the privacy data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals and, where possible, taking action to remediate any risk of harm.
- **Step 3: Notify** individuals, regulatory bodies such as the NSW Information and Privacy Commissioner (NSW IPC), the Office of the Australian Information Commissioner (OAIC) or the Data Protection Authority (GDPR), or others if required. In some circumstances it will be mandatory for the University to notify one or more of these regulatory bodies.
- **Step 4: Review** the incident and consider what actions can be taken to prevent future breaches.

Step 1: Report and Contain

If a University staff member suspects that a privacy data breach has occurred, the University staff member must immediately:

(a) stop unauthorised practices by resetting passwords, revoking access privileges or remediate system or security weaknesses.
(b) report the suspected data breach to their supervisor and Head of Work Unit. Suspected Health Clinic privacy data breaches, should also be reported to the Health Clinic Manager;
(c) complete the Data Breach Report and provide it to their Head of Work Unit and the Information Privacy Officer on privacy@scu.edu.au; and
(d) where the suspected data breach involves technology-based data, notify Technology Services' Service Desk.

The Head of Work Unit, in consultation with the Information Privacy Officer (and Technology Services representative where relevant), must take immediate action to limit the breach, remediate harm and preserve evidence.

To identify strategies to contain a privacy data breach, the Head of Work Unit should consider:

- How did the privacy data breach occur?
- Is the personal information still being shared, disclosed, or lost without authorisation?
- Who has access to the personal information?
- What can be done to secure the information, or stop the unauthorised access or disclosure, and reduce the risk of harm to affected individuals?

During this preliminary stage, be careful not to destroy evidence that may be valuable in identifying the cause of the breach, or that would enable the University to address all risks posed to affected individuals or the University.

Step 2: Assess

Preliminary assessment by the Information Privacy Officer

The Information Privacy Officer must review the Privacy Data Breach Report and undertake any preliminary investigations to confirm the report or seek any clarification or additional detail as necessary.

Based on their review of the Privacy Data Breach Report and the preliminary assessment, the Information Privacy Officer must make an initial assessment of:

(a) whether the reported incident is a privacy data breach;
(b) if it is a privacy data breach, whether the breach may be subject to mandatory reporting and if so any time limitations relating to that reporting;
(c) if it is a privacy data breach, the risk posed by the breach based on:
    - the number of individuals affected by the breach;
    - the type of personal information involved;
    - likelihood of serious harm to affected individuals;

- the breach or suspected breach indicates a systematic problem in the University's processes or systems;
- media or stakeholder attention as a result of the breach or suspected breach; and
- whether remedial actions have successfully prevented harm to affected individuals.

The Information Privacy Officer will provide their initial assessment to Head, Governance Services. The initial assessment must be provided to the Head, Governance Services as soon as possible. Where the incident involves a possible privacy data breach which requires mandatory reporting, the Head, Governance Services must be notified within 24 hours.

Assessment by the Head, Governance Services

The Head, Governance Services may request further information from the Information Privacy Officer or relevant Head of Work Unit.

The Head, Governance Services will determine:

(a) whether the incident is a privacy data breach; and
(b) if it is a privacy data breach, the risk of serious harm to either the University or an individual.

If the Head, Governance Services determines that the incident is **not a privacy data breach**, the Information Privacy Officer and relevant Head of Work Unit will take such action as is necessary to close out the incident.

If the Head, Governance Services determines that the incident **is a privacy data breach but that serious harm is, at most, unlikely** (based on the University Risk Matrix):

(a) the incident will not be escalated to the Privacy Data Breach Response Group;
(b) the Information Privacy Officer will record the incident in the Privacy Data Breach Register; and
(c) the Head, Governance Services will work with the Information Privacy Officer and the relevant Head of Work Unit to determine what action is necessary to close out the incident. This may include giving voluntary notification to the affected individuals and the NSW Information and Privacy Commissioner.

If the Head, Governance Services determines that the incident **is a privacy data breach and that serious harm is at least possible** (based on the University Risk Matrix), the incident will be escalated to the Privacy Data Breach Response Group. The Head, Governance Services will also notify the relevant Executive members who may request to be made members of the Privacy Data Breach Response Group.

The Head, Governance Services will make their determination as soon as possible. Where the incident involves a possible privacy data breach which requires mandatory reporting, the Head Governance Services must escalate the incident to the Privacy Data Breach Response Group within 48 hours of the report of a data breach.

Assessment by the Privacy Data Breach Response Group

The Privacy Data Breach Response Group will be comprised of:

- Head, Governance Services (or nominee)
- Director, Technology Services (or nominee)
- Information Privacy Officer
- Relevant Head of Work Unit
- Relevant Executive members (if they have requested to be part of the Privacy Data Breach Response Group)

The Privacy Data Breach Response Group may co-opt other members such as:

- Director, HR Services (or nominee) – where the privacy data breach involves employees
- Chief Marketing Officer (or nominee) – where the privacy data breach is likely to attract publicity
- Deputy Vice Chancellor (Students) (or nominee) – where the privacy data breach involves a large number of students
- Deputy Vice Chancellor (Research) (or nominee) – where the privacy data breach involves research data
- University Lawyer – where the privacy data breach has significant legal risks or there may be resulting legal or regulatory action.

The Head, Governance Services will convene a meeting of the Privacy Data Breach Response Group as soon as possible. The Privacy Data Breach Response Group may meet in person or via tele- or video- conference. The Privacy Data Breach Report and the results of the preliminary investigation will be tabled at the first meeting of the Privacy Data Breach Response Group.

The Privacy Data Breach Response Group is responsible for assessing whether:

(a) the data breach is likely to result in serious harm to one or more individuals; and
(b) the University has not been able to prevent the likely risk of serious harm with remediate action.

Based on their assessment of the above, the Privacy Data Breach Response Group will make a recommendation to the Vice President (Operations).

On receipt of the recommendation from the Privacy Data Breach Response Group, the Vice President (Operations) will determine whether:

(a) mandatory notification to regulatory bodies such as the OAIC and the GDPR or affected individuals is required; and
(b) even if notification is not mandatory, voluntary notification to regulatory bodies such as the OAIC, NSW IPC or affected individuals should be made.

The Vice President (Operations) will make this determination as soon as possible and, in any event, within 30 days of the data breach. Where the data breach requires mandatory notification, the Privacy Data Breach Response Group will make the determination in the time required under the relevant legislation (for GDPR notifications, this is 72 hours).

If the Vice President (Operations) determines that mandatory notification is not required:

(a) the Information Privacy Officer will record the incident in the Privacy Data Breach Register; and
(b) the Information Privacy Officer and the relevant Head of Work Unit will take any actions necessary to close out the incident. This may include giving voluntary notification to the OAIC, the NSW IPC or affected individuals as determined by the Vice President (Operations).

Step 3: Notify

Mandatory notification

If the Privacy Data Response Group determines that mandatory notification to the OAIC, under the GDPR or the affected individuals is required, the Head, Governance Services is responsible for preparing and sending out the relevant notifications with assistance from the Information Privacy Officer. The Information Privacy Officer must keep a record of all notifications.

Voluntary notification

If the Head, Governance Services or the Vice President (Operations) determines that there should be voluntary notification to the OAIC, the NSW IPC or affected individuals, the Head, Governance Services is responsible for preparing and sending out the relevant notifications with assistance from the Information Privacy Officer. The Information Privacy Officer must keep a record of all notifications.

Additional notifications

The Head, Governance Services and the Vice President (Operations) must consider whether additional people or entities should be made aware of the actual or suspected privacy data breach. For example:

- Internal staff – if the breach is likely to be reported on in the media or there is widespread discussion concerning the breach by staff members
- Insurers – if there is likely to be a claim against any of the University's insurance policies. This will be managed by the Manager, Insurance and Risk
- Law enforcement agencies – if the breach involves criminal activity

In addition, if the data breach is the result of possible misconduct by a University student or staff member:

(a) a complaint may be made in accordance with the Complaint Policy – Staff; or
(b) an allegation may be made in accordance with the Rules – Student Academic and Non-Academic Misconduct Rules.

Additional considerations

If law enforcement agencies are involved, the Head, Governance Services will ascertain whether notification should be withheld or delayed to avoid compromising the investigation.

If the privacy data breach is likely to attract publicity, the Head, Governance Services must notify the Chief Marketing Officer so as to co-ordinate the timing and prepare content for any media release or statement.

Step 4 - Review

The Head, Governance Services will conduct a post-breach review and assessment to improve personal information handling practices. The Head, Governance Services will seek informal input and assistance from the Privacy Data Breach Response Group and the others as required.

The Head, Governance Services will:

(a) determine whether any data handling or data security practices led or contributed to the relevant privacy data breach;

(b) consider whether there are any further actions that need to be taken as a result of the relevant privacy data breach, such as:

  (i) updating security measures;

  (ii) reviewing and updating this privacy data breach response plan;

  (iii) making appropriate changes to practices, systems, other processes, policies and procedures;

  (iv) revising staff training practices;

  (v) reviewing external vendors' security or contract terms and ongoing engagement; and

  (vi) considering undertaking an audit to ensure necessary outcomes are implemented.

Where a privacy data breach occurs resulting in mandatory notification, the Head, Governance Services will provide a report to the Vice Chancellor's Group on the breach and the outcome.

The Head, Governance Services will provide an annual report to the Vice Chancellor's Group and the Audit and Risk Management Committee regarding the incidence and outcome of privacy data breaches.