DATA BREACH RESPONSE PLAN

PART A: DATA BREACH REPORTING PROCEDURES FOR UNIVERSITY PERSONNEL

BACKGROUND

Objective

The University of Adelaide and its controlled entities (collectively, "**University**", "**we**", "**us**") are committed to protecting the privacy of individuals, including students, staff and alumni.

The purpose of this Data Breach Response Plan (**Plan**) is to enable the University to:

(a) identify, contain, escalate, assess and respond to data breaches in a timely manner;

(b) proactively help mitigate and remediate potential harm to affected individuals;

(c) document its processes and data breach responses;

(d) identify the staff roles and responsibilities, delegations of authority and reporting lines in the event of a data breach and points of contact; and

(e) identify the staff responsible for managing the data breach response.

This Plan will assist the University to meet its statutory obligations as a Tax File Number Recipient under the new mandatory Notifiable Data Breaches scheme (**NDB scheme**) in Part IIIC of the Privacy Act, that came into effect from 22 February 2018. This Plan is also designed to address the requirements to notify personal data breaches in accordance with the General Data Protection Regulations (GDPR) where the GDPR is applicable to the University.

This Plan operates under the Privacy Policy and Privacy Management Plan and must be followed when assessing and responding to an actual or suspected data breach.

The Plan consists of the following sections:

Section	Description
Part A	sets out the procedures for all University Personnel and Area Managers who become aware of an actual or suspected data breach
Flowchart	outlines the Phases for reporting and assessing data breaches
Part B	sets out the assessment procedure for the Data Breach Response Group
Schedule 1	Data Breach Report Form
Schedule 2	Eligible Data Breach Assessment Form
Schedule 3	OAIC Notification Template
Schedule 4	Options for Notification Checklist
Schedule 5	Supervisory Authority Notification Template - GDPR

Note: Schedules 2 – 5 are held by the Risk Services Branch. These forms can be requested by emailing legalcompliance@adelaide.edu.au.

Key Concepts

Australian Law

Personal information

Personal information means information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information is true or not, and whether the information is recorded in a material form or not. It includes all personal information regardless of its source and regardless of whether it is publicly available.

Data breach

A **data breach** occurs when personal information is subjected to unauthorised access or disclosure, or where the information is lost and unauthorised access or disclosure is likely to occur.

Example: data breaches resulting from human error
• *Loss of an employee's laptop, USB or paper records that contain personal information held by the University (e.g. left on a train, at the airport etc.)*
• *A University employee accidentally disclosing personal information to the wrong recipient (e.g. sending correspondence to the wrong student, publishing a link on MyUni which identifies all students and their grades etc.)*
Example: data breaches resulting from malicious activity
• *Hacking into the University's email accounts, software or databases containing Personal Information*
• *Scams that trick an employee of the University into releasing personal information*
• *Inappropriate or fraudulent use of a database containing personal information*
Example: data breaches resulting from unforeseen circumstances
• *Unforeseen events that occur to a contractor who holds personal information on behalf of the University (e.g. Adam Data Centre) or if a cloud service provider suffers a data breach (e.g. ShareCloud)*

Eligible data breach

An **eligible data breach** is a data breach that is likely to result in serious harm to any of the individuals to whom the information relates.

The University must notify the Office of the Australian Information Commissioner (**OAIC**) and affected individuals if:

(a) it has reasonable grounds to believe that an eligible data breach has occurred; or

(b) it is directed to do so by the OAIC (for instance if a data breach is reported directly to the OAIC by an affected individual and/or if the OAIC disagrees with the University's assessment that the incident is not an eligible data breach).

GDPR

Personal data

Personal data means ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Notifiable Data Breach

A **personal data breach** is a **notifiable data breach** *unless* it is unlikely to result in a risk to the rights and freedoms of natural persons.

The University must report notifiable data breaches to the supervisory authority.

When the **notifiable data breach** is likely to result in a high risk to the rights and freedoms of natural person, the University must also notify the affected individuals.

Key Points

- **University Personnel** must immediately report actual or suspected data breaches to their **Area Manager** using the **Data Breach Report** form.
- The **Area Manager** must take immediate action to contain the actual or suspected data breach, and provides the **Data Breach Report** to the **Manager, Audit & Compliance (**legalcompliance@adelaide.edu.au or 8313 0482).
- The **Manager, Audit & Compliance** must conduct a preliminary investigation and reports findings to the **Chief Information Officer**.
- If necessary, the **Chief Information Officer** convenes the **Data Breach Response Group** to assess the breach.
- If the **Chief Information Officer** (as recommended by the **Data Breach Response Group**) determines that an **eligible data breach** has occurred, the OAIC and affected individuals are notified by the **Chief Information Officer**.
- If the **Chief Information Officer** (as recommended by the **Data Breach Response Group**) determines that a **notifiable data breach** has occurred under GDPR, the supervisory authority and affected individuals (if applicable) are notified by the **Chief Information Officer**.

Key Roles and Responsibilities

Title	Role
University Personnel (employees, titleholders, contractors, volunteers, including personnel of controlled entities etc.)	• Report incidents immediately to their Area Manager • Complete the Data Breach Report and give to Area Manager • Participate in investigations as required
Area Managers (Head of School or Branch, or relevant line manager)	• Receive Data Breach Reports from University Personnel within their area • Contain breach, remediate harm, and preserve evidence • Forward Data Breach Report to the Manager, Audit & Compliance • Assist with investigations as required

Manager, Audit & Compliance	• Receive Data Breach Reports from Area Manager and alert General Counsel and Chief Information Officer of potential data breach • Conduct a preliminary investigation • Provide findings to Chief Information Officer • Participate as a member of the Data Breach Response Group • Record incidents in the University Non-compliance Register and/or Risk Register
Chief Information Officer	• Receive preliminary investigation findings from Manager, Audit & Compliance • Accept or reject preliminary investigation findings • Determine the seriousness of the data breach • Decide whether to convene of the Data Breach Response Group, and whether to include additional members • Approve assessment by Data Breach Response Group • Make notifications as appropriate • Conduct post-action review
Data Breach Response Group	• Assess containment and/or remediation actions • Assess preliminary investigation • Assess whether an eligible data breach has occurred • Assess notification requirements • Assist with post-action review

Timeframes

An actual or suspected data breach must be investigated and managed as soon as the University becomes aware of the data breach, or suspects that it has occurred.

Australian Law

The University will become aware of an eligible data breach as soon as it has "reasonable grounds to believe" (rather than just "reasonable grounds to suspect") that an eligible data breach has occurred.

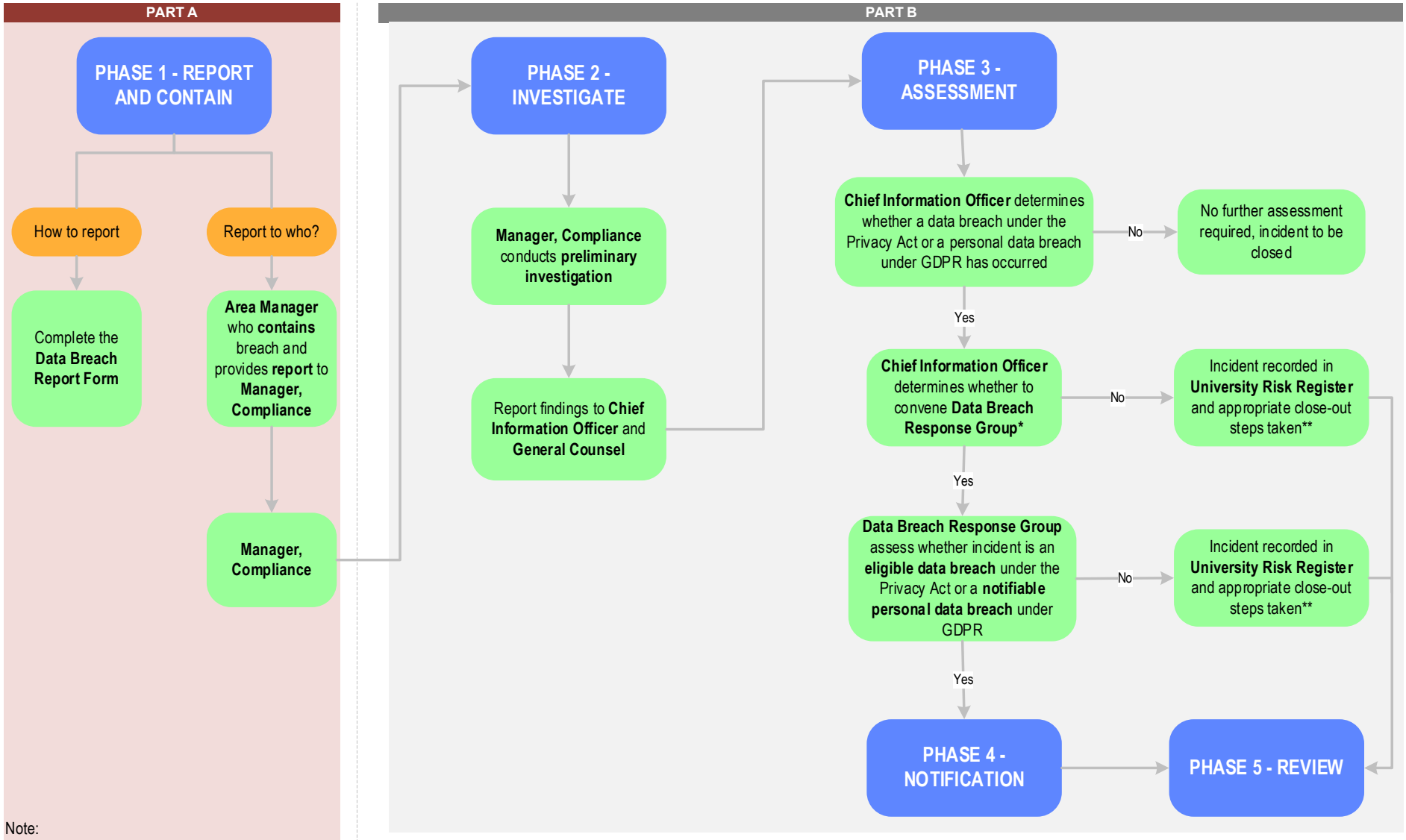
Suspected data breach	Confirmed eligible data breach
Assessment must be reasonable and expeditious All reasonable steps to complete the assessment within **30 days** of the date that the University became aware of or suspected a data breach This timeframe should be treated as the **maximum timeframe** for completing the assessment	Notify the OAIC and affected individuals **as soon as practicable** after becoming aware of an eligible data breach

GDPR

Under GDPR the University becomes aware when it has a reasonable degree of certainty that a security incident has occurred that has led to the personal data being compromised. However, it is expected that the University will have implemented all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place, such that it puts an obligation on the University to ensure that it will be aware of any breaches in a timely manner.

Personal Data Breach	Reporting requirements
Does the personal data breach pose a *risk* to natural persons, or a *high risk*? A personal data breach that poses a *risk* to natural persons must be reported to the supervisory authority. A personal data breach that poses a *high risk* to the rights and freedoms of natural persons needs to be reported to affected individuals and the supervisory authority. A personal data breach does not have to be reported if it is unlikely to result in a *risk* to the rights and freedoms of natural persons.	Notify the supervisory authority within 72 hours after becoming aware of a personal data breach that poses a *risk*, or a *high risk*, to the rights and freedoms of natural persons. Where 72 hours has passed, disclosure needs to occur without undue delay and be accompanied by reasons for the delay. Affected individuals are required to be notified without undue delay where the personal data breach poses a *high risk* to their rights and freedoms.

University of Adelaide Data Breach Response Plan - Flowchart



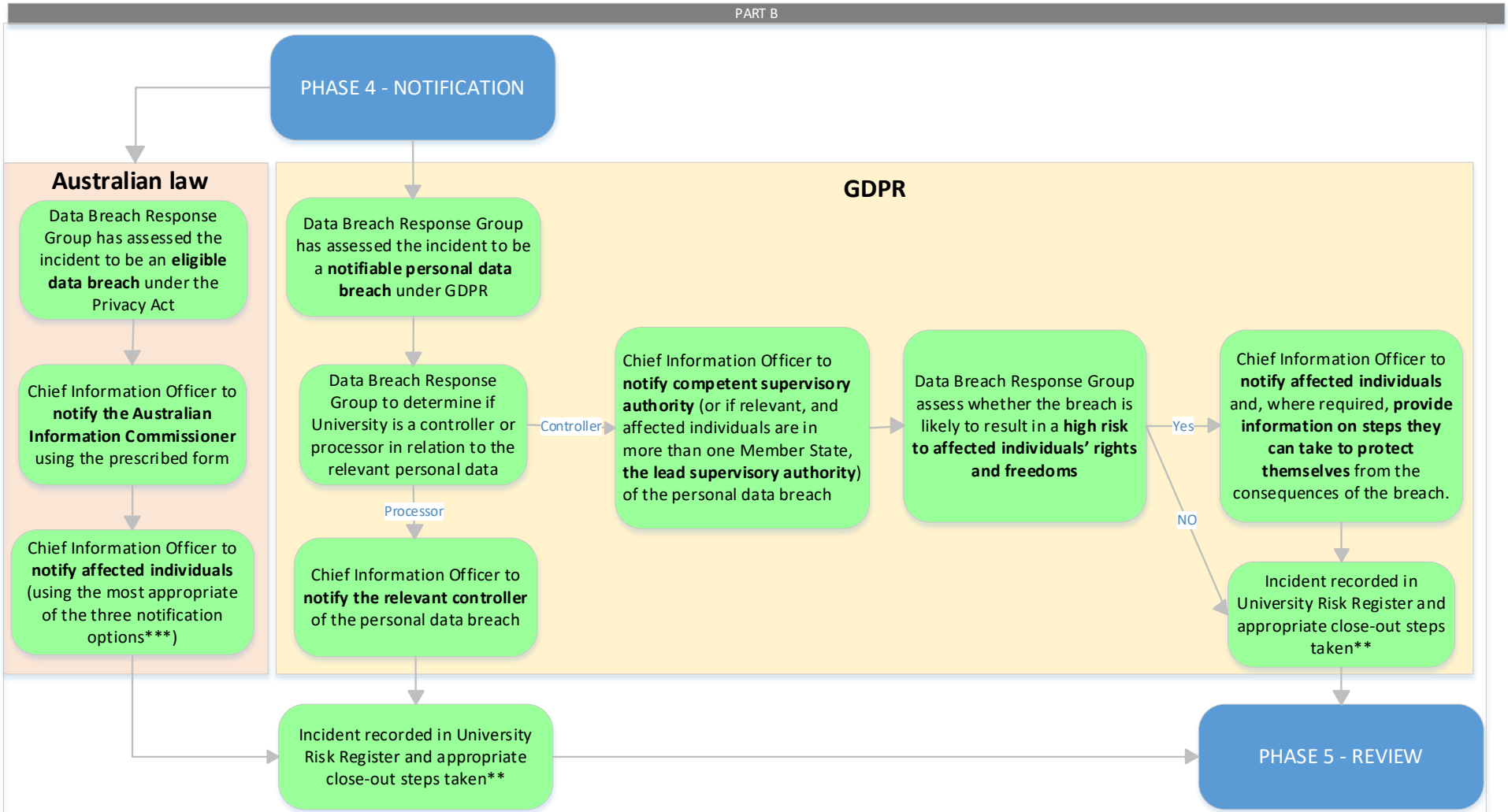
Note:

* the Data Breach Response Group will be convened unless the Chief Information Officer determines that there is no likelihood that a data breach is an eligible data breach for the purposes of the Privacy Act 1988 (Cth) and no likelihood that a personal data breach is a notifiable breach under the General Data Protection Regulation.

** this action needs to include documenting any personal data breach under the GDRP as required by Article 33(5)

For further information about the steps in this Flowchart go to the relevant Phase in the Data Breach Response Plan

University of Adelaide Data Breach Response Plan – Phase 4
Notification Flowchart



Note:
** this action needs to include documenting any personal data breach under the GDRP as required by Article 33(5)
For further information about the steps in this Flowchart go to the relevant Phase in the Data Breach Response Plan
***depending on the notification option selected, if applicable have regard to the remedial undertaken for particular affected individuals

1. PHASE 1: REPORT & CONTAIN

1.1 Procedure for Reporting Data Breaches

Australian Law & GDPR

If any University Personnel becomes aware of an actual or suspected data breach, they must report it as soon as possible. University Personnel should immediately:

(a) record the details of the data breach in the **Data Breach Report Form** provided in **Schedule 1** (**Data Breach Report**);

(b) provide a copy of the **Data Breach Report** to their **Area Manager** either in person or by email; and

(c) otherwise keep the incident confidential except where it is necessary to disclose information about the incident in accordance with this Plan.

Upon receiving the **Data Breach Report**, the **Area Manager** must immediately:

(a) take action to contain the data breach, remediate harm, and preserve evidence;

(b) notify the **Manager, Audit & Compliance** of the incident and provide a copy of the completed **Data Breach Report** by emailing: legalcompliance@adelaide.edu.au; and

(c) otherwise keep the incident confidential except where it is necessary to disclose information about the incident in accordance with this Plan.

1.2 Procedure for Containing Data Breaches and Remediating Harm

Australian Law & GDPR

The **Area Manager** is responsible for taking immediate action to contain the breach and remediate harm, including by seeking assistance from the appropriate business units or external suppliers as necessary.

Important: At any time, appropriate steps should be taken to reduce any potential harm to affected individuals. If remedial action is successful in preventing serious harm (or in the case of GDPR, risk or high risk) to affected individuals, notification may not be mandatory. However the University's notification requirements will be determined in the relevant phase of this Plan.

Below are examples of containment / remedial steps that may be appropriate:

Example: If the data breach involves electronic records held on an ICT system: • *Isolate the causes of the data breach in the relevant system, software or database* • *Shut down the compromised system, software or database* • *Reset log-in details and passwords for compromised devices, systems or databases* • *Quarantine any compromised devices* • *Activate the University's Disaster Recovery Plan and/or Business Continuity Management Framework*
Example: If the data breach involves the loss of a device or physical files • *Remotely disable the lost device* • *Arrange a search of the site where the loss occurred by contacting any relevant authorities (e.g. the public transport authority if lost on a train, an airline if left on a plane etc.)*
Example: If the data breach involves the unauthorised disclosure of personal information to a third party

- *By email – recall the email from the recipient and/or ask the recipient not to read and to delete the email*
- *By post – contact the recipient and ask them not to open or read the posted materials, and arrange for collection/return of the posted materials*
- *By publication online – deactivate the link to the publication*

1.3 Preserving Evidence of a Suspected Data Breach

Australian Law & GDPR

The **Area Manager** must take any reasonable steps available to them to preserve and/or record evidence of an actual or suspected data breach.

Example:

- *Making a note of any other person/s who witnessed the incident*
- *Recording the exact time of the incident*
- *If a cyber attack has occurred – recording the details of any pop-up message or email you receive in relation to the cyber attack*
- *If there has been accidental disclosure of personal information to the wrong person – retaining copies of any emails or file notes relating to the incident, and storing them on the University's recordkeeping system (HPE CM)*

Records must be kept in accordance with the University's Information Management Policy.

For Phases 2 – 5 see Part B of this Plan

DATA BREACH RESPONSE PLAN

PART B: DATA BREACH MANAGEMENT PROCEDURES FOR INTERNAL USE

2. PHASE 2: INVESTIGATE

2.1 Procedure for investigating reported Data Breaches

Australian Law & GDPR

The **Manager, Audit & Compliance** must review any report of an actual or suspected data breach as soon as reasonably practicable (or where GDPR applies, immediately in order to meet the 72 hour time frame). Upon reviewing the **Data Breach Report**, the **Manager, Audit & Compliance** must:

(a) notify the **General Counsel** and **Chief Information Officer** that a **Data Breach Report** has been received;

(b) assess what containment and/or remediation actions have already been undertaken by the **Area Manager** (if any), and whether any further actions are required; and

(c) undertake any preliminary investigations necessary to confirm the report and/or seek any clarification or additional detail as necessary.

Important: At any time, appropriate steps should be taken to reduce any potential harm to affected individuals. If remedial action is successful in preventing serious harm (or in the case of GDPR, risk or high risk) to affected individuals, notification may not be mandatory. However the University's notification requirements will be determined in the relevant phase of this Plan.

Once the **Manager, Audit & Compliance** has reviewed the **Data Breach Report** and undertaken their preliminary investigation to confirm the incident, they must make an initial assessment of:

(a) whether the reported incident is not a data breach (such that further investigation is not required);

(b) whether the reported incident is a data breach (such that a further investigation is required); and

(c) if there is a data breach, give an initial risk rating using the University's Risk Matrix having regard to relevant issues including (if known):

(i) number of individuals affected by the breach or suspected breach;

(ii) type of personal information;

(iii) likelihood of serious harm to (or where GDPR applies, risk or high risk to the rights and freedoms of) affected individuals;

(iv) the breach or suspected breach indicates a systematic problem in the University's processes or systems;

(v) media or stakeholder attention as a result of the breach or suspected breach; or

(vi) whether remedial actions have successfully prevented harm to (or where GDPR applies, risk or high risk to the rights and freedoms of) affected individuals.

2.2 Reporting and Escalation

Australian Law & GDPR

The **Manager, Audit & Compliance** must provide the findings of the preliminary investigation to the **General Counsel** and **Chief Information Officer** as soon as possible.

3. PHASE 3: ASSESSMENT

3.1 Procedure for escalation to the Data Breach Response Group

Australian Law & GDPR

The **Chief Information Officer** will assess the preliminary investigation findings to determine whether to convene the **Data Breach Response Group**. The **Chief Information Officer** may request further information from the **Manager, Audit & Compliance** if reasonably required to make a determination.

If the **Chief Information Officer**:

(a) determines the incident is not a data breach, the incident will not be escalated to the **Data Breach Response Group**, and the **Chief Information Officer** must direct the **Area Manager** or **Manager, Audit & Compliance** to undertake any action that is reasonably necessary to close-out the incident appropriately;

(b) determines the incident is a data breach and suspects that serious harm (or where GDPR applies, risk or high risk) is at least *possible* (as per the likelihood scoring system in the University Risk Matrix), it should be escalated to the **Data Breach Response Group** for further assessment (see section 3.3); or

***note**: 'risk' is a lower threshold than 'serious harm'.*

(c) determines the incident is a data breach and determines that serious harm (or where GDPR applies, risk or high risk) is at most *unlikely* (as per the likelihood scoring system in University Risk Matrix):

(i) the incident should not be escalated to the **Data Breach Response Group**;

(ii) the **Chief Information Officer** will direct the **Manager, Audit & Compliance** to record the incident in the University Risk Register; and

(iii) the **Chief Information Officer** may direct the **Area Manager** or **Manager, Audit & Compliance** to undertake any action that is reasonably necessary to close-out the incident appropriately, which may include giving voluntary notification to affected individuals and / or OAIC (or where GDPR applies, the supervisory authority).

3.2 Members of the Data Breach Response Group

Australian Law & GDPR

The **Data Breach Response Group** comprises the following permanent members:

Position Title
Chief Information Officer (Convenor) (or nominee)
General Counsel (or nominee)
Manager, Audit & Compliance (or nominee)
Chief Risk Officer (or nominee)

The **Chief Information Officer** may co-opt additional members onto the **Data Breach Response Group** or engage external providers to assist in containment or investigation of the breach, depending on the nature or severity of the data breach. Additional members may include (but Is not limited to) the following:

Branch / Office	Requirement	Position Title
Human Resources	Where data breach involves employees (as affected individuals or involved in the breach)	Director – HR Services (or nominee)
IT Security	Where data breach involves ICT systems (e.g. unauthorised access to a database, a cyberattack etc.)	Chief Information Security Officer (or nominee)
Media & Corporate Relations	Where data breach affects a large number of individuals or is serious, and therefore likely to attract publicity	Deputy Director, Media and Corporate Relations (or nominee)
Advancement	Where data breach affects alumni or donor related data	Executive Director, Advancement
Student Services	Where data breach affects a large number of students and it is likely they will want to contact the University	Associate Director – Student Administration (or nominee)
Insurance	Where data breach will potentially be covered by insurance held by the University (e.g. cyber insurance or insurance against theft or damage to physical property)	Insurance Specialist (or nominee)
Records Services	Where data breach affects records of the University	University Archivist & Manager, Records Archives and Rare Books (or nominee)
Office of Research Ethics, Compliance & Integrity	Where data breach affects human research data	Manager, Ethics, Compliance & Integrity (or nominee)
External Supplier	Where data breach involves a third party supplier or contractor of the University	Subject to nature of data breach
External service providers	Legal services (e.g. if the University requires specialist legal advice) IT services (e.g. if the University requires additional assistance with a data breach involving ICT systems) Accounting or auditing services (e.g. if the University requires additional assistance with a data	***Note:* External service providers must be preapproved by Insurance Services prior to engagement to ensure costs are covered by insurance**

	breach involving financial information) Public relations services (e.g. if the University requires advice on how to manage media enquiries, possible reputational damage etc.)	

If position titles change after the Plan is published, it shall be replaced with the equivalent position or most similar position.

3.3 Procedure for Conducting Assessment of Data Breach

Australian Law & GDPR

If a determination is made in accordance with 3.1(b), the **Chief Information Officer** must convene a meeting of the **Data Breach Response Group** **as soon as possible**.

Where GDPR applies, keep in mind the 72 hour timeframe for notification to the supervisory authority and convene appropriately.

The **Data Breach Response Group** is responsible for assessing and determining whether:

(a) the data breach is likely to result in serious harm (or where GDPR applies, likely to result in risk or high risk) to the affected individual or individuals;

(b) mandatory notification to the OAIC (or where GDPR applies, the supervisory authority) and affected individuals is required; or

(c) if notification is not mandatory, voluntary notification to the OAIC (or where GDPR applies, the supervisory authority) and/or affected individuals is desirable.

In conducting the assessment, the following issues must be considered:

(d) the **type** of Personal Information involved;

(e) the **context** of the affected information and the breach;

(f) the **cause and extent** of the breach; and

(g) the **likelihood of serious harm** to (or where GDPR applies, the likelihood of risk or high risk to the rights and freedoms of) affected individuals.

Where GDPR applies, the following additional issues must be considered in relation to whether a high risk is posed to affected individuals:

(a) whether the University has implemented appropriate technical and organisational protection measures that has rendered the personal data affected by the breach unintelligible to unauthorised personnel; or

(b) whether the University has taken subsequent measures, making the high risk to the rights and freedoms of natural persons now unlikely to materialise.

Where the University has undertaken remedial steps to the extent that the personal data breach is no longer likely to result in a *high risk* to the rights and freedoms of affected persons, the University is not required to notify affected persons of the personal data breach. Further if the *risk* to the rights and freedoms of affected persons is unlikely to result then notification is not required to the supervisory authority.

The **Data Breach Response Group** must meet in person or via secure teleconference. The **Data Breach Report** and the results of the preliminary investigation (including any containment and/or remediation steps taken) must be tabled at the first meeting of the **Data Breach Response Group.**

The **Data Breach Response Group** must complete the **Eligible Data Breach Assessment Form (Schedule 2)**.[1] In all cases, the assessment should be conducted expeditiously and completed within 30 days of the date that the data breach occurred.

The **Chief Information Officer** will be responsible for determining whether an **eligible data breach** (and/or a notifiable personal data breach under GDPR) has occurred, based on the **Data Breach Response Group's** assessment and recommendation.

Important: The obligation to notify the OAIC and affected individuals as soon as reasonably practicable is triggered when the University determines that an **eligible data breach** has occurred.

The 30 day assessment timeframe is the **maximum** timeframe for completing the risk assessment. It is possible that the obligation to notify could be triggered at the time the University becomes aware of the data breach where it is clear that it not immediately or soon after within 1-2 days of the data breach occurring.

Important: Where GDPR applies, the obligation to notify the supervisory authority within 72 hours is triggered when the University becomes aware that a personal data breach that is likely to result a risk or a high risk to individuals has occurred. If the risk to individuals is *unlikely* then notification to the supervisory body is not required.

The 72 hour assessment timeframe should be treated as the **maximum** timeframe for completing the risk assessment and notifying the supervisory authority. As 'risk' is a low threshold, in practical terms, it is likely most personal data breaches will need to be reported to the supervisory authority subject to the assessment of likelihood.

The obligation to notify affected individuals without undue delay is triggered when the University becomes aware that the personal data breach is likely to result in a high risk to the rights and freedoms of individuals.

3.4 Non-eligible Data Breaches

Australian Law & GDPR

If during Phase 3, the **Chief Information Officer** determines the data breach is *not* an **eligible data breach** or a notifiable **personal data breach**, the **Chief Information Officer** will direct the **Manager, Audit & Compliance** to record the incident in the University Risk Register (if appropriate), and the **Chief Information Officer** may direct the **Area Manager** or **Manager, Audit & Compliance** to undertake action that is reasonably necessary to close-out the incident appropriately.

The close-out actions may include giving voluntary notification to the OAIC (or where GDPR applies, the supervisory authority) and/or affected individuals in accordance with notification procedures set out in Phase 4 based on a recommendation by the **Data Beach Response Group** having regard for the nature and circumstances of the incident.

Once close-out steps have been carried out (if any) Phase 5 should be completed as appropriate.

3.5 Record Keeping and Evidence Preservation

Australian Law & GDPR

[1] Eligible Data Breach Assessment Form (Schedule 2) is held by the Risk Services Branch. Request the form by emailing legalcompliance@adelaide.edu.au.

University Personnel including the **Data Breach Response Group** must keep records of all steps taken in response to the data breach and decisions made in connection with it in accordance with the University's Information Management Policy. This includes:

(a) keeping a record of all steps taken during the preliminary investigation and subsequent assessment of the reported data breach; and

(b) ensuring that any relevant evidence of the data breach (such as computer imaging, forensic investigation or other investigative processes) is preserved and stored securely.

The information may be required by forensic investigators, legal advisors, law enforcement and regulators, as well as for use in preparing notifications to and communications with affected individuals and the OAIC (or where GDPR applies, the relevant supervisory authority) and any other regulator or relevant entities.

Evidence and records must be sufficient to demonstrate to the OAIC, (or where GDPR applies, the relevant supervisory authority), the reasonable steps taken to comply with statutory and other legal obligations where the University is required to do so.

Where the assessment by the **Data Breach Response Group** is for the purpose of obtaining legal advice:

(c) all documents, written communications, reports, notes or advice relating to the data breach must be marked "*Confidential and Subject to Legal Professional Privilege*"; and

(d) no other reports, forms or other documents relating to the data breach will be prepared except those which are required or requested by the **General Counsel** (or nominee).

4. PHASE 4: NOTIFICATION

4.1 Notification

Australian Law

If during Phase 3, the **Chief Information Officer** determines the data breach to be an **eligible data breach**, the University must give notification to the **OAIC and all affected individuals** about the data breach.

The statutory timeframe for **eligible data breach** notification is **as soon as practicable after the University becomes aware of the eligible data breach**. The OAIC understands that this timeframe will vary depending on the organisation's circumstances. Factors such as the time, effort, or cost required to prepare the eligible data breach notification will also be relevant.

There may also be other notifications which would be appropriate in the particular circumstances (e.g. notifying insurers, the police, cybercrime agencies etc.) – see 4.4.

Important: At any time, steps should be taken to reduce any potential harm to affected individuals. If remedial action is successful in preventing serious harm to affected individuals, notification may not be mandatory. However the University's notification requirements will be determined in the relevant phase of this Plan.

GDPR

If during Phase 3, the **Chief Information Officer** determines that the personal data breach is likely to result in ***risk*** to the rights and freedoms of natural persons, the University must give notification to the **supervisory authority**.

If the **Chief Information Officer** determines that the personal data breach is likely to result in a ***high risk*** to the rights and freedoms of natural persons, the University must give notification to the **supervisory authority and all affected individuals** about the personal data breach.

Important: At any time, steps should be taken to reduce any potential harm to affected individuals. If remedial action is successful in preventing *risk* or *high risk* to affected individuals,

notification may not be mandatory. However the University's notification requirements will be determined in the relevant phase of this Plan.

4.2 Procedure for Notifying

Australian Law

The **Chief Information Officer** or a nominated member of the **Data Breach Response Group** must prepare a draft **notification to the OAIC** using the **OAIC Notification Template (Schedule 3)**.[2]

It is mandatory to include the following information in Part A of the OAIC Notification:

(a) the identity and contact details of the University;

(b) a description of the eligible data breach;

(c) the kind or kinds of Personal Information affected by the breach; and

(d) the University's recommendation as to the steps that individuals should take to protect their position in response to the data breach.

Under Australian law, it is optional to include the following additional information in Part B of the OAIC Notification[3]:

(e) additional details about the circumstances of the breach;

(f) number of individuals affected;

(g) additional information about the steps taken to respond to the breach; and

(h) any other information that might be relevant to assist OAIC in considering the appropriate response to the notification.

The notification to the OAIC must be **approved and signed by the Chief Information Officer** prior to being sent.

The notification must be sent to the OAIC by email to enquiries@oaic.gov.au with the subject "*Eligible data breach notification to OAIC, University of Adelaide*".

Once the **Chief Information Officer** (or nominee) has submitted the notification to the OAIC, the record of the OAIC's acknowledgement of receipt of the eligible data breach statement and reference number must be recorded and sent to legalcompliance@adelaide.edu.au. Following submission of the notification to the OAIC the **Chief Information Officer** (or nominee) should contact the OAIC by telephone to confirm it has been received.

GDPR

Where GDPR applies, the **Chief Information Officer** or a nominated member of the **Data Breach Response Group** must prepare a draft **notification to the relevant supervisory authorities** using the **Supervisory Authority Notification Template (Schedule 5).**[4]

It is mandatory to include the following information in the Supervisory Authority Notification:

(a) the identity and contact details of the University;

(b) a description of the eligible data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

---

[2] OAIC Notification Template (Schedule 3) is held by the Risk Services Branch. Request the template by email to legalcompliance@adelaide.edu.au.

[3] While this information may be voluntary it may be relevant to the notice and otherwise support APP11.1 compliance. Note it may still be subject to access under Freedom of Information Act

[4] Supervisory Authority Notification Template (Schedule 5) is held by the Risk Services Branch. Request the template by email to legalcompliance@adelaide.edu.au.

(c) the name and contact details of the data protection officer or other contact point where more information can be obtained;

(d) the likely consequences of the personal data breach;

(e) the measures taken or proposed to be taken by the University to address the personal data breach, including where appropriate, measures to mitigate its possible adverse effects; and

(f) any other information that might be relevant to assist the relevant supervisory authority in considering the appropriate response to the notification.

If it is not possible to provide all of the above information at the same time, the information may be provided in phases without undue further delay.

The notification to the supervisory authority must be **approved and signed by the Chief Information Officer** prior to being sent.

Once the **Chief Information Officer** (or nominee) has submitted the notification to the supervisory authority, any record of the supervisory authority's acknowledgement of receipt of the personal data breach notification (including any reference number) must be recorded and sent to legalcompliance@adelaide.edu.au. Following submission of the notification to the supervisory authority the **Chief Information Officer** (or nominee) should contact the supervisory authority to confirm it has been received.

In addition to notifying the University's lead supervisory authority, the University is required to consider whether an additional notification needs to be provided to a second competent supervisory authority.

A second competent supervisory authority is required to be notified where the personal data breach substantially affects individuals in another Member State. In these circumstances, the University should also notify the supervisory authority in that Member State of the personal data breach.

4.3 Procedure for Notifying Affected Individuals

Australian Law & GDPR

If there has been an **eligible data breach**, the **Data Breach Response Group** is responsible for assessing the options available for notifying affected individuals of the data breach, using the **Options for Notification Checklist (Schedule 4)**.[5]

The **Chief Information Officer** or a nominated member of the **Data Breach Response Group** must then prepare a draft **notification to affected individuals**.

Note that where GDPR applies, affected individuals only need to be notified where the personal data breach is likely to result in a ***high risk*** to their rights and freedoms.

Under Australian Law, the notification to affected individuals must include:

(a) how and when the data breach occurred;

(b) the types of Personal Information involved in the data breach;

(c) what the University has done or will be doing to reduce or eliminate the risk of harm brought about by the data breach;

(d) any assurances (if applicable) about what data has not been disclosed (i.e. if a breach only affects an individual's basic identity or contact information, but not their financial information or any sensitive information);

[5] Options for Notification Checklist (Schedule 4) is held by the Risk Services Branch. Request the checklist by emailing legalcompliance@adelaide.edu.au.

(e) what steps the individuals can take to protect themselves and what the University will do to assist people to do this (if applicable);

(f) contact details for the University for questions or requests for information or assistance (e.g. helpline numbers, e-mail addresses or websites);

(g) whether the University has notified the OAIC about the data breach; and

(h) how an individual can lodge a privacy complaint with the OAIC.

Where GDPR applies, the notification to affected individuals must include the same categories of information provided to the supervisory authority described in paragraphs (c), (d) and (e) above, along with the likely consequences of the personal data breach.

The notification to affected individuals must be **approved and signed by the Chief Information Officer** prior to being sent out to the relevant persons.

Once approved, the **Chief Information Officer** is responsible for sending out the notification to individuals and/or delegating the responsibility to the appropriate business unit.

The **Chief Information Officer** must keep a record of:

(a) the date, time and method of notification to each individual; and

(b) any confirmation of receipt of the notification received from an individual (unless the data breach involves a very large number of individuals, and it would be impractical to do so).

4.4 Procedure for Making Additional Notifications

Australian Law & GDPR

The **Data Breach Response Group** must also consider whether any of the following persons need to be made aware of the actual or suspected data breach:

Category	Notification trigger
Internal staff	If the breach is likely to be reported on in the media, or if there are widespread discussions of it between staff members
Cyber Liability Insurer (AIG Australia Limited)	If the breach involves unauthorised access, use or disclosure of electronic records (i.e. hacking, online scams, malware, physical theft of devices containing electronic records etc.)
Law enforcement agency	If the breach involves theft or other criminal activity, it will generally be appropriate to notify police
Third party service providers	If the breach involves or affects a third party service provider's facilities, infrastructure or personnel
Regulators - ASIC - ATO	If the breach involves financial information, notification may be appropriate
Specialist advisors - Legal - Public relations - Forensic IT	If the University requires independent legal advice, IT investigations, or a PR strategy ***Note: Specialist advisors must be preapproved by the Insurance Team prior to engagement to ensure costs are covered by the Insurer***
Cybercrime support networks - The Australian Cybercrime Online Reporting Network - The Computer Emergency Response Team (CERT)	If the data breach involves unauthorised access, use or disclosure of electronic records (i.e. hacking, online scams etc.)

If the **Data Breach Response Group** determines that additional notification is desirable, approval must be obtained from the **Chief Information Officer** before such notification is made.

4.5 Additional Considerations

Australian Law & GDPR

The **Data Breach Response Group** should also consider the following factors:

(a) If law enforcement authorities are involved, check with them whether notification should be withheld or delayed to avoid compromising the investigation (but note that where GDPR applies, notification to affected individuals must occur without undue delay); and

(b) If the data breach is likely to attract publicity, the External Relations Branch must be briefed so as to co-ordinate the timing and prepare content for any media release or statement. All media or public enquiries relating to the data breach must be referred to **Deputy Director, Media and Corporate Relations** and responses should be approved by the **Chief Information Officer** (or nominee) prior to release.

5. PHASE 5: REVIEW

5.1 Procedure for Conducting Post Breach Review

Australian Law & GDPR

The **Chief Information Officer** (or nominee) is responsible for conducting a post-breach review and assessment, once the immediate consequences of the data breach have been dealt with.

In conducting the review, the **Chief Information Officer**:

(a) should seek informal input and assistance from other members of the **Data Breach Response Group** and other business units, as required;

(b) must

  (i) complete any further investigations as necessary or desirable;

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

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

    (A) updating security measures;

    (B) reviewing and updating this data breach response plan;

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

    (D) revising staff training practices;

    (E) reviewing external vendors' security/contract terms and ongoing engagement; and

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

(c) then as soon as reasonably practicable:

  (i) update the University Risk Register and / or Non-compliance Register as appropriate; and

  (ii) provide a written report to the Audit, Compliance & Risk Committee with their findings and recommendations for further actions.

Below are some examples of further actions that could be considered in particular situations:

Example: If the data breach was caused by employee conduct, could the University:

- *provide any staff training to prevent the data breach from re-occurring*
- *provide any once-off or regular staff reminder to prevent the data breach from re-occurring*
- *provide any additional oversight or supervision of staff, to prevent the data breach from re-occurring*
- *increase its auditing or monitoring of staff to prevent the data breach from re-occurring*
- *change any staff policies or procedures to prevent the data breach from re-occurring*
- *introduce any new controls or restrictions on staff access to prevent the data breach from re-occurring*

Example: If the data breach involved a security breach by a third party, could the University:

- *improve its IT security in any way*
- *improve its building security in any way*
- *apply any additional security protections to protect the Personal Information (e.g. encryption, use of pseudonyms)*
- *increase its security surveillance in any way*
- *give any directions to its staff or contractors that would prevent the security breach from re-occurring*
- *change any IT or building security policies or procedures to prevent the data breach from re-occurring*
- *introduce any new access restrictions to prevent the data breach from re-occurring*