Data Breach Response Plan

1. INTRODUCTION

Griffith University is committed to protecting the privacy of staff, students, and alumni, including individuals who use the services of the University.

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

- identify the staff roles and responsibilities and reporting lines in the event of a data breach;
- identify, contain, escalate, assess and respond to data breaches in a timely manner;
- proactively help mitigate and remEDIATE potential serious harm to affected individuals; and
- document its processes and data breach responses.

This Plan:

- will assist the University to meet its statutory obligations as a File Number Recipient under the mandatory Notifiable Data Breach scheme (NDB scheme) in Part IIIC of the Privacy Act 1998 (Cth); and particularly the obligations which require the University to notify any individuals likely to be at risk of serious harm by a data breach and the Office of the Australian Information Commissioner (OAIC);
- aims to better protect important business assets and enables the University to deal with adverse media or stakeholder attention from a breach or a suspected breach and instil confidence of the University’s capacity to respond appropriately; and
• is to be used in conjunction with Data Security Incident Management Framework and the risk level to be assessed against the University’s Risk Management Framework.

2. **ROLES AND RESPONSIBILITIES**

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All staff</strong></td>
<td>Are to report actual or suspected data breach incidents within 24 hours of becoming aware of the incident. Reports can be made direct to the Chief Digital Officer via email <a href="mailto:cdo@griffith.edu.au">cdo@griffith.edu.au</a> or anonymously via the University’s whistle blower hotline. The <strong>Your Call</strong> organisational identification code for the University is GRIFFITH. Telephone <strong>Your Call</strong> on: 1300 790 228 on business days between 9.00 am and 12 am and provide all the details on hand.</td>
</tr>
</tbody>
</table>
| **Chief Digital Officer (CDO)**     | • Determines and assess the seriousness of the data breach incident. To assess the seriousness of the breach consideration must be made to relevant matters (see section 4.2.1).  
• If the severity of the incident is above a medium risk to appoint a senior manager (from Digital Solutions or from another area of the University) as a Problem Manager to commence preliminary investigation and assessments.  
• To provide early notification of the incident to the Data Breach Response Steering Committee.  
• Activate the Digital Solutions Crisis Management Team (DS-CMT) for managing and overseeing the investigation and assessment (refer to step 1 and 2 below). |
| **Problem Manager**                 | The Problem Manager is to investigate and manage the data breach incident response team and will become a member of the DS-CMT. The Problem Manager will:  
• Conduct initial investigation;  
• Assess containment and/or remediation actions;  
• Assess preliminary investigations;  
• As required, conduct detailed investigation;  
• Mobilise, investigate, forensics and source external specialist resources;  
• Assess whether an eligible data breach has occurred; and  
• Prepare post incident review. |
| **Digital Solution Crisis Management Team (DS-CMT)** | • Chaired by CDO, will oversee and support the investigation process using the DS Crisis Management Plan.  
• Approve containment and/or remediation actions;  
• Confirm whether an eligible data breach has occurred  
• Assess notification requirements;  
• Approve post incident review |
### Role and Responsibility

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| **Vice President (Corporate Service)**    | • Provide updates to the Executive Group, Chancellor, Council as needed;  
                                            | • Provide support and resources to the CDO by ensuring availability of key senior resources and external subject matter expertise, if required;  
                                            | • Approve the release of any communications to affected individuals and the OAIC;  
                                            | • Approve the release of any communications to the media, staff, and students, with advice from the Chief Marketing Officer and Director Legal Services;  
                                            | • Approve final incident report and share with Executive Group.                                                                              |
| **Senior Manager Risk and Compliance**    | • Member of DS-CMT;  
                                            | • Provide regulatory and compliance advice and guidance;  
                                            | • Advisory member of Data Breach Response Steering Committee.                                                                                     |
| **Chief Marketing Officer**               | • Managing the formulation and transmission of all communications via all media                                                                 |
| **Director Legal Services**               | • Provide advice to the University on all legal, legislation, regulatory, contractual, Notifiable Data Breach, and Right to Information matters. |

### Data Breach Response Steering Committee

Chaired by the Vice President (Corporate Services), members of this committee include: CDO, Director Legal Services, Chief Marketing Officer, Senior Manager Risk and Compliance. Others may be invited based on the breach e.g. Director Audit, Risk, and Compliance; Director of People and Wellbeing, Academic Registrar and system business owner. The committee will act in accordance of the University’s Crisis Management Plan.

This steering committee provides oversight and support to DS-CMT to ensure adequate priority and resources are available.

### 3. DEFINITIONS

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| **Personal Information** | Is information or an opinion, including information or an opinion forming part of a database, whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.  
 | Personal information can be almost any information that is associated with an identifiable living individual. It can include correspondence, audio recording, images and alpha-numerical identifiers.  
 | The information must be about the individual and the individual’s identity must be reasonably ascertainable from the information or opinion. |
| **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. This access can be internal, external or a combination of the two. |
**Examples:**

- *Data breaches resulting from human error* – loss of employee laptop, USB or paper records that contain personal information or accidental disclosure of personal information to the wrong recipient.

- *Data breaches resulting from malicious activity* - hacking, phishing, scams or inappropriate or fraudulent use of systems containing personal information.

- *Data breaches resulting from unforeseen circumstances* – events that occur to 3rd party agents/providers of the University who hold personal information on behalf of the University or if a cloud service provider suffers a data breach.

A data breach may also constitute a breach of the *Privacy Act 1988 (Cth).*

<table>
<thead>
<tr>
<th>Eligible Data Breach</th>
<th>Happens if there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by the University and the access, disclosure or loss is <em>likely to result in serious harm</em> to any of the individuals who the information relates.</th>
</tr>
</thead>
</table>
| Likely risk of serious harm | To determine if a breach or a suspected breach is likely to result in a risk of serious harm, the following could apply:  
  - Multiple individuals could be affected.  
  - There could be potential for a real risk of serious harm to affected individuals.  
  - A systematic Program in the University’s privacy processes or procedures is revealed or suspected.  
  - Media or stakeholder attention might be anticipated.  
  - Intellectual property may be jeopardised.  
  - The impact on the University may include investigation by a regulator and or potential for a sanction, enforceable undertaking, fine or penalty, compensation payment.  
  - Meets the relevant factors test (see section 4.2.1). |
| Office of the Australian Information Commissioner (OAIC) | The Office of the Australian Information Commissioner (OAIC) is headed by the Information and Privacy Commissioner who has regulatory powers under the *Privacy Act 1988 (Cth).* The powers conferred allow for the OAIC to work with entities to facilitate legal compliance and best privacy practices. The OAIC has a number of enforcement, investigatory and other regulatory powers to achieve the objectives and purpose of the *Privacy Act 1988 (Cth).* |
4. RESPONSE PROCESS

There are four key steps required to respond to a breach or a suspected breach. Generally, steps 1-3 should be carried out concurrently in or close succession.

4.1 STEP 1: REPORT, INITIATE, MOBILISE AND CONTAIN

4.1.1 Report
If a staff member knows or suspects a data breach has occurred that staff member must report it within 24 hours of becoming aware or forming the suspicion. Reports can be made direct to the Chief Digital Officer via email cdo@griffith.edu.au or anonymously via the University's whistle blower hotline.

4.1.2 Initiate
Once notified of a potential data incident, the CDO will follow the Data Security Incident Management procedure. After making initial enquiries, the CDO will make a determination that a potential may have/has occurred. The CDO would appoint a Problem Manager to conduct further risk assessment.

4.1.3 Contain
The Problem Manager is responsible for conducting risk assessment and 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. Actions to contain and or remediate may include:

- steps to stop (if possible) or limit the unauthorised practice;
- if needed, freeze the affected system to collect data and logs for forensics investigation;
- recover the records; and
- shut down the system that was breached.

Containment and remediation is a crucial step in reducing any potential harm to affected individuals. If remedial action is successful in preventing serious harm to affected individuals, notification (step 3) may not be mandatory.

4.1.4 Mobilise
If risk assessment indicates a Medium or High risk, the CDO will use the Data Security Incident Management procedures and activate the DS-CMT to commence investigations and assessments.

4.2 STEP 2: INVESTIGATE AND ASSESSMENT

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

**Suspected data breach:** the assessment must be reasonable and expeditious. All reasonable steps must be taken to complete the assessment within **30 days** of the date the University becomes aware of or suspects a data breach.

The Problem Manager will conduct further assessment to understand the severity of the data breach by gathering the facts and evaluating the risks, including potential harm to affected individuals, and where possible act to remediate any further risk of harm.

**Assessment will factor the following:**

- Date, time, duration, and location of the breach.
- The type of personal information involved and by whom.
- How the breach was discovered and by whom.
- The cause and extent of the breach.
• Internet and network log files for impacted systems.
• Access and authentication data for impacted systems.
• Details of all recent changes and modifications for the impacted systems.
• A list of affected individuals, or possible affected individuals.
• The risk of serious harm to the affected individuals.

4.2.1 Assessing Serious Harm

When assessing whether access or disclosure would be likely, or would not be likely, to result in serious harm, the following relevant matters should be taken into consideration when making an assessment:

• What kind of information it is?
• Is the information sensitive?
• Is the information protected by one or more security measures?
• If the information is protected by security measures, is there a likelihood that any of those security measures could be overcome?
• Who are the persons, who have or who could have obtained, the information?
• If a security technology or methodology is used to make the information unintelligible or meaningless, what is the likelihood of those who have obtained the information of causing harm to any individuals to whom the information relates?
• What is the nature of the harm?

The answer to these questions will determine whether disclosure of information would be likely or would not be likely to result in serious harm to any of the individuals to whom the information relates.

4.3 STEP 3: EVALUATION AND NOTIFICATION

4.3.1 Notifying

During the investigation and assessment (step 2), if it is deemed that the data breach is an eligible data breach, the University must give notification to the OAIC and all affected individuals about the data breach.

The timeframe for notification is as soon as practicable after the University becomes aware of the eligible data breach. This timeframe will vary depending on the circumstances. Factors such as time, effort, external subject matter expertise or cost required to prepare the eligible data breach notification will also be relevant.

There may also be other notifications which would be more appropriate in particular circumstances (see section 4.3.4).

4.3.2 Procedure for Notifying the OAIC

Mandatory information to report:

The Vice President (Corporate Services) as the University’s Privacy Officer must notify the OAIC using the OAIC Notification Template. It is mandatory to include the following:

• the identity and contact details of the University;
• a description of the eligible data breach;
• the kind(s) of personal information involved in the data breach; and
• the steps the University will recommend to individuals to take to reduce the risk that they experience because of the data breach.
Optional information to report:

It is optional to include the following additional information to the OAIC; however, it is encouraged to provide additional information to assist the OAIC in understanding the eligible data breach. The OAIC may contact the University for further information if this information is not provided.

The optional information does not need to be provided in notifications to individuals, and the Vice President (Corporate Services) may request that the optional information provided be held in confidence by the OAIC.

Additional information includes:

- date the breach occurred (if known);
- date the breach was discovered;
- primary cause of the data breach (malicious or criminal attack, system fault or human error);
- description of how the data breach occurred;
- number of individuals whose personal information is involved in the data breach;
- description of any action the University has taken to assist individuals whose personal information was involved in the data breach;
- description of any action the University has taken to prevent reoccurrence;
- how the University intends to notify individuals (see options in section 4.3.3) who are likely to be at risk of serious harm as a result of the data breach; and when the notification will occur;
- list any other data protection authorities, law enforcement bodies or regulatory bodies that the University has reported the breach to; and
- any other information that might be relevant to assist the OAIC.

Correspondence

The notification to the OAIC must be approved and signed by the Vice President (Corporate Services) prior to being sent to the OAIC by email to enquiries@oaic.gov.au with the subject “Eligible data breach notification to OAIC, Griffith University”.

Once the notification has been submitted, the Vice President (Corporate Services) (or nominee) should contact the OAIC by telephone to confirm the notification has been received. The record of the OAIC’s acknowledgement of receipt of the eligible data breach statement and reference number must be recorded and sent to CDO.

4.3.3 Procedure for Notifying Affected Individuals

If there has been an eligible data breach, the Data Breach Steering Committee is responsible for assessing the options available for notifying the affected individual or individual of the data breach.

Notification should include what is known of the following:

- how and when the data breach occurred;
- the type of personal information involved in the eligible data breach;
- what the University has done or will be doing to reduce or eliminate the risk of harm brought about the data breach;
- any assurance (if applicable) about what data has not been disclosed (i.e. if a breach only affects an individual’s basic identify or contact information, but not their financial information or any sensitive or medical information (for the health clinics);
- what steps the individuals can take to protect themselves and what the University will do to assist people to do this (if applicable);
- contact details for the University for questions or request for information or assistance;
whether the University has notified the OAIC about the eligible data breach; and

how the individual might lodge a privacy complaint with the OAIC or with the Office of the Information Commissioner Queensland if they wish.

There are three options available for notifying:

- **Option 1: notify all individuals**
  
  If it is practicable, the University can notify each of the individuals to whom relevant information was part of the eligible data breach. This option is best, if the University cannot determine which individuals are at risk of serious harm from an eligible data breach but the University has formed the view that serious harm is likely for one or more of the individuals.

  The benefit of this approach includes ensuring that all individuals who may be at risk of serious harm are notified and allowing them to consider whether they need to take any action in response to the eligible data breach.

- **Option 2: notify only those individuals at risk of serious harm**
  
  The University may choose to notify only those individuals who are at risk of serious harm from the eligible data breach.

  The benefit of this option is avoiding the unnecessary distress to individuals who are not at risk, limiting possible notification fatigue to individuals not concerned and reducing administrative costs, where it is not required by the NDB scheme.

- **Option 3: publish notification**
  
  If option 1 and 2 are not practicable, for example the University does not have up-to-date contact details, then the University can publish a copy of the statement on the University’s website and maintain it on the website for no less than six months.

4.3.4 Procedure for Making Additional Notifications

The Data Breach Steering Committee must consider whether any of the following need to be made aware of the actual or suspected data breach:

<table>
<thead>
<tr>
<th>Notifiable Group</th>
<th>Notification trigger points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff and / or student</td>
<td>If the breach is likely to be reported on in the media, or if there are widespread discussions of it within the University community.</td>
</tr>
<tr>
<td>Cyber Liability Insurer</td>
<td>Notify the Insurance Manager to inform of the breach or suspected breach to determine if a claim can be made. Where the data has been passed on to a 3rd party, contamination, destruction, modification or corruption of data, denial of access, theft of access codes, unauthorised access and use, cyber extortion, network interruption, defence costs, data administrative fines, investigation costs, forensic service and reputation repair costs can be claimed.</td>
</tr>
<tr>
<td>Third party service providers</td>
<td>If the breach involves or affects a third-party service provider’s facilities, infrastructure or personnel.</td>
</tr>
<tr>
<td>Specialist advisors</td>
<td>If the University requires independent legal advice, IT investigators, forensic investigators. <strong>Note</strong> – check with the Insurance Manager to determine if associated costs are covered by a Insurance Policy.</td>
</tr>
<tr>
<td>Australian Cyber Security Centre</td>
<td>If the data breach involves cybercrime, the Australian Cyber Security Centre, a Government lead cyber security</td>
</tr>
</tbody>
</table>
4.3.5 Additional Consideration

The **Data Breach Response Steering Committee** should consider the following factors:

- If law enforcement authorities are involved, check with them whether notification should be withheld or delayed avoiding compromising the investigation; and
- If the data breach is likely to attract publicity, the Chief Marketing Officer should activate the OMC Crisis Management Plan, to co-ordinate and prepare content for any media release or statement. All media or public enquiries relating to the data breach must be referred to the Chief Marketing Officer and Director Legal Services but be approved by the Vice President (Corporate Services) prior to release.

If at any time after being notified of a breach or suspected breach, the Data Breach Response Steering Committee, forms the opinion that serious harm to affected individuals is likely, a notification is to be made to the affected individuals and the OAIC.

**Confirmed eligible data breach**: notify the OAIC and affected individuals **as soon as practicable** after becoming aware of an eligible data breach.

In considering notification the Response Steering Committee will have regard to whether or not serious harm is likely, that is, more probable than not. In deciding whether this is the case, regard will be given to the list of relevant matters (see section 4.2.1)

4.4 STEP 4: REVIEW

Following an eligible data breach, a post-breach review will be conducted by the Problem Manager to assess the response to the data breach and the effectiveness of the data breach response plan. The report will be circulated to the Chief Digital Officer, Vice President (Corporate Services), Director Legal Services, the Chief Marketing Officer, the Director Audit Risk and Compliance and the Executive Group.

In conducting the review, the Problem Manager should:

- Seek input from the Digital Solution’s Data Breach Incident Response Team.
- Determine whether any data handling or data security practices led or contributed to the relevant data breach.
- Consider whether there are any further actions that need to be taken because of the relevant data breach, such as:
  - updating security measures;
  - reviewing and updating this plan;
  - making appropriate changes to practices, systems, other processes, policies and procedures;
  - revising staff training practices;
  - review external vendors security/contract terms and ongoing engagement; and
  - consider undertaking an audit to ensure necessary outcomes are implemented.