UOW
GLOBAL
ENTERPRISES

# DATA BREACH RESPONSE PLAN

*Acknowledgement:* UOW Global Enterprises acknowledges the use of guidance published by the NSW Information and Privacy Commission, the Office of the Australian Information Commissioner and the Office of the Victorian Privacy Commissioner

UOW
GLOBAL
ENTERPRISES

# 1. INTRODUCTION

This document sets out UOW Global Enterprises (UOWGE) procedures for managing a data breach, including:

- What is a data breach?
- The steps involved in responding to a data breach
- The considerations around notifying persons whose privacy may be affected by the breach
- Template report and action document

# 2. WHAT IS A DATA BREACH?

A data breach occurs when the data for which UOWGE is responsible suffers a security incident resulting in a breach of confidentiality, availability or integrity. Some of the most common breaches at UOWGE may occur due to:

- Accidental loss or theft of data (including accidentally sending emails to unintended recipients)
- Unauthorised use, access to or modification of data or information systems
- Unauthorised disclosure of classified material information (e.g. including emails or documents sent to incorrect recipients either intentional or unintentional), or personal information posted onto a website without consent
- Compromised user account (e.g. accidental disclosure of user login details through phishing)
- Computer hacking or malware infection and ransomware requests
- Equipment failure, faulty business procedures or operational break-downs.

# 3. RESPONDING TO A DATA BREACH

The Privacy Officer is to be informed of any data breach so that appropriate support and assistance may be provided to ensure best practice response actions are undertaken. The Privacy Officer will also be responsible for managing any complaints received as a result of the breach.

There are four key steps required in responding to a data breach:

1. Contain the breach and conduct a preliminary assessment
2. Evaluate the associated risks
3. Notify affected individuals (where appropriate).
4. Prevent re-occurrence of the breach.

Each step is set out in further detail below. The first three steps should be carried out simultaneously or in quick succession. The decision on how to respond should be on a case-by-case basis. The last step provides recommendations for longer-term solutions and prevention strategies.

UOW
GLOBAL
ENTERPRISES

## Step 1: Contain the breach and conduct a preliminary assessment

All necessary steps must be taken to contain the breach and minimize any resulting damage. The following actions should be taken:

1. Immediately contain the breach. For example, shut down the system that caused the breach, recover the information, suspend the activity that led to the breach, revoke or change access codes or passwords.

2. Report the incident to the Privacy Officer who will take the lead and decide priority actions. Priority actions may include consideration of a response team to assist with the breach assessment, impact, communication and stakeholder relationships. Refer to section 3 for recommended response team roles and responsibilities.

3. Determine who needs to be made aware of the incident internally, and potentially externally. For example, if the incident is suspected to involve criminal activity, the Police may need to be notified.

4. If a third party has received the data then all efforts should be made to contact the third party before any potential misuse. Subject to point 5. below, the third party is to be instructed to either destroy or return the information and any copies made.

5. There must be no destruction of any evidence that may be valuable in identifying the cause of the breach, or that would enable UOWGE to address all risks posed to affected individuals or UOWGE.

The template at Appendix A should be used to record actions.

## Step 2: Evaluate the Associated Risks

To determine what other steps are needed, an assessment of the type of data involved in the breach and the risks associated with the breach is to be undertaken.

Factors to consider include:

### 1. What personal information was involved in the breach?

- Does it involve significant personal information or a combination of data which may put the subject of the breach at a particular risk of harm, (generally, the more significant or a greater combination of data may have a higher risk of harm to individuals).

### 2. What was the cause of the breach?

- To the extent possible, determine the extent of the breach e.g. the number and nature of likely recipients

- Did the breach occur as part of a targeted attack or through inadvertent oversight?

- Was it a one-off incident or does it expose a more systemic vulnerability?

- What steps have been taken to contain the breach?
- Has the data been recovered (including any copies made)? This would have been considered at Step 1.
- Is the data encrypted or otherwise not readily accessible?

### 3. What is the foreseeable harm to the affected individuals/organisations?

- Consider the possible use for the data. For example, could it be used for identity theft, threats to physical safety, financial loss, or damage to reputation?
- Who is the recipient of the data?

## Step 3: Consider notifying affected individuals/organizations

In general, if a data breach creates a risk of harm or loss to an individual/organisation, the affected individual/organisation should be notified. Prompt notification in these cases can help to avoid or lessen the damage by enabling the individual/organisation to take steps to protect themselves. Notification demonstrates a commitment to open and transparent governance, consistent with best practice.

However, there may be occasions where notification may be counter-productive. For example, information collected may be less sensitive and notifying individuals about a privacy breach which is unlikely to result in an adverse outcome for the individual may cause unnecessary anxiety and de-sensitize individuals to a significant privacy breach.

The assessment and decision to notify individuals is to be referred to the Privacy Officer, prior to any action being taken on the decision.

Factors to consider when deciding whether notification to affected individuals is appropriate include:

- Are there any legal or contractual obligations that require notification to the affected individuals?
- What is the risk of harm, loss or damage to the individual/organisation? (Consider the risk of physical harm and a risk of humiliation or damage to the individual's reputation).
- Determine if the affected individuals are protected by the European Union General Data Protection Regulation (the GDPR). If so, and the data breach is likely to result in a high risk to the rights and freedoms of individuals then the following steps must be taken in order to comply with the GDPR's mandatory data breach notification requirements.
- The relevant supervisory authority must be advised of the data breach within 72 hours of becoming aware of the breach.
- The personal data breach must be communicated to the affected individual without undue delay.

Additionally, the Notifiable Data Breaches Scheme under the *Australian Privacy Act 1988* (Privacy Act) must be applied to all 'eligible data breaches' where the breach is likely to result in serious harm to any of the individuals to whom the information relates. In order to comply with this scheme:

- A statement must be provided to the Australian Information Commissioner notifying of an eligible data breach as soon as practicable after UOWGE becomes aware of the breach; and
- The affected individual must be notified as soon as practicable after preparing the statement for the Australian Information Commissioner.

## Notification to Affected Individuals

Where a decision has been made to notify the affected individuals, the following factors require consideration:

1. Timing of the notification - In general, individuals/organizations affected by the breach should be notified as soon as practicable, unless GDPR requirements apply (see above). However, there may be instances where notification would compromise an investigation or may reveal a software vulnerability.

2. Decide on the best method of notification - The preferred method is via direct communication (telephone, email or letter). Instances where it is impracticable to communicate directly (such as being too cost prohibitive or contact details of affected individuals are not known and cannot be reasonably obtained) may require indirect notification, such as via website, group messaging, media. However, consideration must be given to whether the notification may cause an increase in risk of harm.

3. Decide who should sign off on the notification – Typically, the area that has the direct relationship with the affected individual should sign off on the notification. If any third parties are involved, there may be some limited circumstances where the notification by the third party may be more practical e.g. if the third party holds the contact details of the affected individuals.

4. Determine what is to be included in the Notification – The content of the notifications will vary depending on the particular breach and the method of notification chosen. Notifications should include, as appropriate:

   - information about the breach, including when it happened
   - a description of the data involved in the breach and a description of the breach
   - assurances (as appropriate) about what data has not been disclosed
   - a general account of what UOWGE has done to control or reduce the harm
   - what steps the person/organisation can take to further protect themselves and what UOWGE can do to assist people with this
   - contact details of the person for questions or requests for information
   - the right to lodge a privacy complaint.

A sample notification letter is located at Appendix B.

## Notification to Others

1. Where notification must be made to the relevant supervisory authority (under the GDPR) or to the Australian Information Commissioner (under the Notifiable Data Breaches Scheme under the Privacy Act), the Privacy Officer must prepare and submit notification reports. Reports should contain similar content to that provided to affected individuals but personal information about the individuals is not required. It may be appropriate to include:

    - a description of the breach
    - the type of personal information involved in the breach
    - what response the IPC has made to the breach
    - what assistance has been offered to affected individuals
    - the name and contact details of the appropriate contact person, and
    - whether the breach has been notified to other external contact(s).

2. Consideration should be given to notifying the following authorities or organizations (as appropriate):

    - police
    - insurers or others (if required under contractual obligations)
    - professional or other regulatory bodies
    - financial institutions or credit reporting agencies (if their assistance is necessary for contacting affected individuals or assist with mitigating harm.)

## Step 4: Prevent Future Breaches

Once steps 1-3 have been taken to mitigate the risks associated with the breach, UOWGE should review and learn from the data breach to implement measures that could be taken to prevent a re-occurrence.

Preventative actions could include:

- a security review of both physical and technical security controls (a root cause analysis)
- a review of policies and procedures to reflect the lessons learned
- a review of employee training practices
- a review of service delivery with contracted service providers (if involved in the breach).

# 4. RESPONSE TEAM ROLES AND RESPONSIBILITIES

A typical data breach response team may include:

| Officer: | Responsibility: |
|---|---|
| Team Leader | Responsible for leading the response and reporting to senior management |
| Senior Executive | Provide support if the breach is serious and poses a significant risk to UOWGE |
| Privacy Officer (Executive Director, Commercial and Legal or their delegate) | • To provide privacy expertise;<br>• Assist with actions in this Response Plan<br>• Maintain the Data Breach Register |
| Legal support | Identify legal obligations and provide advice. |
| IT support/forensic support | • Assist to identify the breach and the extent of the breach<br>• Facilitate response actions<br>• Assist with root cause analysis. |
| HR support | Provide assistance if the breach was due to staff members actions |
| Media/Communications support | Assist in communicating with media and external stakeholders (where required). |
| External specialist IT Consultants (Only to be deployed if necessary) | Assist if the data breach is considered complex and requires a specialist skill set to conduct an effective analysis. |

UOW
GLOBAL
ENTERPRISES

# APPENDIX A

## TEMPLATE REPORT AND ACTION

| **Description of data breach** | **Action Taken** |
|---|---|
| When - What - How – | Notification –<br><br>Containment - |
| **Description of risks** | **Action Proposed** |
| Risk - Harm - Affecting – | |
| **Description of causes** | **Action Proposed** |
| How - Why - | Change – Train – Remind – Review – Stop – Media – Remedy – Etc – |
| **Notification**<br>**(to internal stakeholders, the NSW Privacy Commissioner and/or other external contacts)** | |
| | |

UOW
GLOBAL
ENTERPRISES

# APPENDIX B

## SAMPLE CORRESPONDENCE TO AFFECTED INDIVIDUALS

**(This should be developed in consultation with the Executive Director, Commercial and Legal )**

Dear [*name*]

I am writing to you about a recent data breach involving (*insert details of the kind of information compromised*). UOW Global Enterprises became aware of this breach on [*date*].
The details of the breach are as follows:

*(Describe the event, including, as applicable, the following):*

- *The date that the breach was known to have occurred*
- *A brief description of what happened.*
- *Description of the data that was inappropriately accessed, collected, used or disclosed.*
- *Risk(s) to the individual caused by the breach.*
- *Steps the individual should take to protect themselves from potential harm from the breach.*
- *A brief description of what UOWGE is doing to investigate the breach, control or mitigate harm to individuals and to protect against further breaches.*

Please be assured that we are doing everything we can to rectify the situation. We take our role in safeguarding your data and using it in an appropriate manner very seriously.

If you have any ongoing concerns about this matter I would be happy to discuss these with you.

Yours sincerely