October 2020

# Data Breach Response Plan

## 1 Introduction

1.1 A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. In the context of the Privacy legislation, it extends to an action that prevents Unitec from being able to access personal information on a temporary or permanent basis.

1.2 Unitec is committed to managing personal information in accordance with the Privacy Act 2020 and Unitec's Privacy Policy and Procedures.

1.3 Unitec needs to be prepared to act quickly in the event of a data breach or suspected data breach and determine whether it is likely to result in serious harm and, in conjunction with the Privacy Officer, whether the breach is a notifiable privacy breach. A notifiable privacy breach is a privacy breach that it is reasonable to believe has caused, or is likely to cause, serious harm to an affected individual or individuals.

1.4 IT is to be proactive in managing this risk by completing annual risk analysis and regular security audits of Information systems and supporting infrastructure with timely remedial action.

1.5 The Data Breach Response Plan has been informed by: the Privacy Act 2020, the current guidelines available on the Privacy Commissioner webpage (with these reviewed for updates on an ongoing basis)

1.6 This document should be read in conjunction with Unitec's Privacy Policy and Procedures.

## 2 Purpose

2.1 The purpose of this Data Breach Response Plan is to set out the processes to be followed by Unitec Staff in the event that Unitec experiences a data breach or suspects that a data breach has occurred.

# 3 Data Breach Alert

3.1 Where a suspected data breach has been identified, the following information must be collated immediately and provided to the Director Information Technology and the Privacy Officer:

a) When the breach occurred (time and date)
b) Description of the breach
c) How many people are likely to have been affected?
d) Cause of the breach (if known) otherwise how it was discovered
e) Which system(s) if any are affected?
f) What area of the business / School is affected?
g) Whether any corrective action has already been taken to remedy or ameliorate the breach (or suspected breach) and if so, details of the action and any advice received today.

3.2 Once notified of the information above, the Director Information Technology and Privacy Officer will determine the type of data breach that has occurred and:

a) Whether financial information is involved
b) Whether personal information is involved
c) Whether the information is of a sensitive nature
d) Whether there been unauthorized access to the information, or unauthorized disclosure of the information or a loss of information.

3.3 Where the breach involves financial information or is in any way commercially sensitive, the Executive Director Finance will be immediately informed.

3.4 In all instances, the Chief Executive will be informed where the breach is of a serious nature and could in any way impact upon the reputation of the Institute (refer 3.6 below).

**Criteria for determining severity**

3.5 In determining whether a breach could potentially be of a serious nature, the Director Information Technology and Privacy Officer (in conjunction with the Executive Director Finance and / or the Director Human Resources, as appropriate) will have regard to:

a) The type and extent of information involved
b) Whether multiple individuals have been affected
c) Whether the information is protected by any security measures (password protection or encryption)
d) The person or kinds of persons who now have access
e) Whether there is (or could there be) a real risk of serious harm to the affected individual(s) including any specific damage (financial loss through identity theft, loss of employment, physical injury or other forms of specific harm); loss of benefits (any adverse effect on the rights, benefits, privileges, obligations or interests of the individual(s)) or emotional harm.
f) Whether there could be media or stakeholder attention as a result of the breach or suspected breach

3.6 If the breach is or could potentially be serious, the Data Breach Response Team will be engaged and the Chief Executive informed of this decision**.**

**Data Breach Response Team**

3.7 The Data Response Team will include the following roles:

a) Director Information Technology
b) Privacy Officer / Legal Counsel
c) Executive Director People and Infrastructure
d) Executive Director Finance (where the breach relates to financial information)
e) Records and Information Management Specialist
f) Communications Manager
g) Director HR Operations (where the breach impacts on a staff member)

# 4 Procedure

4.1 **Step 1: Immediately contain the breach**

a) Immediately contain the breach (if this has not already occurred). Corrective action may include retrieval or recovery of the personal information, ceasing unauthorised access, shutting down or isolating the affected system. In the case of a staff member, their machine will be quarantined and their network account locked until such time the response team are satisfied there is no further risk.
b) Director Information Technology to appoint a suitable person to lead the initial investigation.
c) Data Response Team to identify personnel from other areas, this might include people from within Unitec or those from outside who have the expertise to deal with the situation.
d) Decide who needs to know within the organisation, build a list of those who need to be informed, internal auditors, risk managers, legal advisers.
e) Be careful not to destroy evidence that may be needed by Unitec or the Police in finding the cause of the problem or which might allow you to fix the issue.

4.2 **Step 2: Evaluate the risks**

a) Evaluate the risks associated with the breach, including collecting and documenting all available evidence of the breach.
b) Call upon the expertise of, or consult with, relevant staff in the particular circumstances
c) Engage an independent cyber security or forensic expert as appropriate
d) Assess whether serious harm is likely
e) Consider developing a communication or media strategy including the timing, content and method of any announcements to students, staff or the media

4.3 **Step 3: Consideration as to whether affected people should be notified**

a) What is the risk of harm to people whose information has been breached?
b) Is it reasonable to believe that the breach caused (or could cause) serious harm to the affected individuals? This will involve a collective review of the matters considered at paragraph 3.6(e) above.

c) In assessing serious harm, regard should be had to:
   i. the particular situation and, for example, whether there is a risk of identity theft, could it result in physical harm or damage to the individual's reputation or relationships, does it relate to health information;
   ii. who has obtained the information as a consequence of the breach?
   iii. how many individuals are affected, how wide spread is the breach and how long has it been occurring.
   iv. If the breach relates to an entity or person that Unitec has a commercial relationship with, then even if this is not personal information, what are the legal and contractual obligations.

4.4 **Step 4: Notification Process**

The above information will be communicated to the Privacy Officer as soon as reasonably practicable. The Privacy Officer will then apply the Privacy Procedures for notifying a Notifiable Privacy Breach to the Privacy Commissioner and advise on the circumstances in which notification should be made to the affected individual(s) or public notification given (having regard to sections 114 to 116 of the Privacy Act 2020).

4.5 **Step 5: Notify third parties (if necessary)**

The Data Response Team should consider whether the following groups or organisations should also be informed. Bear in mind any obligations of confidentiality.

a) Third party contractors or other parties who may be affected
b) Internal business units not previously advised of the privacy breach, for example, members of senior management
c) Unitec Board of Directors
d) Union or other employee representatives
e) Police
f) Insurers
g) Professional or other regulatory bodies
h) Credit card companies, financial institutions or credit reporting agencies

4.6 **Step 6: Prevent a repeat**

Once the breach matters have been dealt with, the response team should turn attention to the following:

a) Identify lessons learnt and remedial action that can be taken to reduce the likelihood of recurrence – this may involve a review of policies, processes, refresher training
b) Prepare a report for submission to the Executive Leadership Team, Unitec Council and notifiable parties
c) Consider the option of an audit to ensure necessary outcomes are effected and effective
d) The amount of effort should reflect the significance of the breach, and whether it happened as a result of a systemic problem or an isolated event. It could include:
e) A security audit of both physical and technical security
f) A review of policies and procedures
g) A review of employee training practices
h) A review of any service delivery partners caught up in the breach

4.7 **Step 7: Consider whether a disciplinary process is required**

If the breach was caused by a staff member or student, consult with Human Resources or Student Success

(as applicable) to assess whether a disciplinary process under the Disciplinary Policy or the Student Disciplinary Statute is warranted. If a contractor caused the breach, consult with the relevant relationship manager and Legal Counsel as to whether the relevant contract should be terminated.

## 5 Roles and Responsibilities

| Role | Responsibilities |
|---|---|
| IT Representatives | • Ensure all relevant information is provided |
| Director - Information Technology | • Appoint data breach Investigation lead<br>• Identify relevant personnel<br>• Convene the response team if assessed serious in nature. |
| Data Breach Response Team | • Assess and determine the potential impact of data breach<br>Ascertain whether the breach is a notifiable privacy breach<br>Undertake steps outlined in this plan including containment of the data breach and prevent reoccurrence |
| Privacy Officer | • Comply with the Privacy Procedures when the breach is identified as a notifiable privacy breach<br>• Ensure timely notification to the Privacy Commissioner where this is appropriate<br>• Liaise with Communications in relation to the manner in which notification to the affected individuals is to take place. |
| Communications | • Work with Privacy Officer and Data Response team in on appropriate means of notifying a serious breach to the affected individuals or whether notification to other parties is deemed appropriate. |
| Human Resource | • Carry out any resulting staff disciplinary processes |
| Student Success | Carry out any resulting student disciplinary processes |

## Reference Documents

- Privacy Act 2020
- Unitec Privacy Policy and Procedures

  Office of the Privacy Commissioner Responding to privacy breaches
  https://www.privacy.org.nz/privacy-for-agencies/privacy-breaches/responding-to-privacy-breaches
- Office of the Privacy Commissioner "Data Safety Toolkit"

# 6 Approval Details

| | | | |
|---|---|---|---|
| **Version number** | 5 | **Issue Date** | 29 October 2020 |
| **Version History** | Date of amendment/s:<br>• 23 April 2018<br>• 24 April 2018<br>• 11 May 2018<br>• 28 June 2018<br>• 29 October 2020 | Amendment/s:<br>• Initial Draft<br>• Update Roles and Responsibilities<br>• Amendments from Legal & Audit and Risk<br>• Amendments from IMS GM - Information Technology | |
| **Approval authority:** | Executive Leadership Team | **Date of Approval** | 19 October 2020 |
| **Procedure Sponsor** **(Has authority to approve minor amendments)** | Privacy Officer | **Procedure Owner:** | Director Information Technology |
| **Contact Person** | Sinead Hart | **Date of Next Review** | Yearly review |