Contegrity Ethics Pty Ltd

Mandatory Data Breach Response Plan

Table of Contents Page

1. Purpose

This Data Breach Response Plan establishes a framework that sets out the roles and responsibilities involved inContegrty Ethics Pty Ltd ABN 91 664 152 827 (**Contegrity Ethics**) managing a Data Breach. It also describes the stepsContegrty Ethics personnel will follow if the company experiences a Data Breach or suspects a Data Breach has occurred. A Data Breach occurs when Personal Information or Protected Company Information is unlawfully used or disclosed.

The objective of this plan is to enableContegrty Ethics to contain, assess and respond quickly to a potential Data Breach in order to mitigate potential harm to affected persons and organisations.

A fast and orderly response to a potential Data Breach can:

- substantially decrease the impact of a breach on affected individuals and organisations;
- reduce the costs associated with dealing with a breach; and
- reduce the potential reputational damage toContegrty Ethics that can result.

Following this Data Breach Response Plan is important to ensure thatContegrty Ethics meets its obligations under the Privacy Laws.

Terms and abbreviations are defined and explained in the “Terms and Definitions” section of this Policy.

2. Scope

The Data Breach Response Plan sets out the following:

- Roles and responsibilities of Contegrity Ethics personnel and subcontractors
- Procedures to be followed in the event of a Data Breach.

The scope of the policy includes data held byContegrty Ethics in any format or medium (paper-based or electronic) that is Personal Information, Confidential Information, or Protected Company Information. This policy does not apply to information or data classified as public.

3. Context and Overview

3.1 Contegrity Ethics Organization and its Context

Contegrity Ethics has created an online decision support tool that helps individuals and organisations to identify and assess conflicts of interest and develop management plans, enabling them to meet their professional obligations and to maintain trust. As part of its business activities,Contegrty Ethics has access to and in some case collects and holds Personal Information and Sensitive Information, as defined under the Privacy Act.Contegrty Ethics is committed to compliance with all applicable laws and regulations.

Contegrity Ethics' Mandatory Data Breach Plan is aimed at:

- compliance with information security laws and regulations, such as the Privacy Act, or any other governmental regulations relating to information security and data privacy and applicable toContegrty Ethics; and
- applying good information security practices to respond to Information Security Incidents and Suspected Eligible Data Breaches in a manner which protectsContegrty Ethics as well asContegrty Ethics' customers' reputations and minimises the risk of occurrence of an Eligible Data Breach.

3.2 Regulatory Environment

As an organisation which collects and processes Personal Information and Sensitive Information,Contegrty Ethics has an obligation to respect the privacy of individuals and to follow the Australian privacy laws, which include but are not limited to:

- the Privacy Act 1988 (Cth) (as amended from time to time);
- the National Privacy Principles contained in Schedule 3 to the Privacy Act or where applicable, the Australian Privacy Principles contained in Schedule 1 of the Privacy Act;
- all other applicable laws that require a person to observe privacy or confidentiality obligations in respect of Personal Information.

The Notifiable Data Breaches scheme under the Privacy Act recognises that strong data management is integral to the operation of businesses and that people who interact with a business such asContegrty Ethics have to trust that their privacy is protected and be confident that Personal Information will be handled in line with their expectations and consistent with legal obligations. In this context, one of the biggest risks organisations face is a Data Breach. Even organisations with great information security can fall victim to a Data Breach, due to the rapid evolution of data security threats and the difficulty of removing the risk of human error. A Data Breach involving Personal Information can put affected individuals at risk of serious harm and cause significant damage an organisation's reputation. Furthermore, organisations are exposed to increased penalties under the Privacy Act.

4. Management Commitment

Contegrity Ethics' management undertakes to demonstrate leadership and commitment with respect toContegrty Ethics' Mandatory Data Breach Plan by:

- ensuring the integration of the Mandatory Data Breach Plan requirements intoContegrty Ethics' processes and procedures;
- ensuring that the resources needed for planning, implementation, operation, monitoring, review, maintenance and improvement of the Mandatory Data Breach Plan are available;
- communicating the importance of effective information security management and of conforming to the Privacy Act requirements;
- ensuring training, awareness and competence of employees, officers and/or subcontractors;
- performing regular reviews of the Mandatory Data Breach Plan's effectiveness;
- promoting Information Security initiatives; and
- accepting responsibility or assigning responsibility for support and supervision of all activities around the Mandatory Data Breach Plan.

5. Identifying a Data Breach

5.1 What Is A Data Breach?

A Data Breach occurs when an Information Security Incident leads to unauthorised access, disclosure, or loss of Personal Information, Protected Company Information, or Business Critical Data held by or on behalf ofContegrty Ethics.

Examples of Data Breaches include:

- unauthorised access to, loss or destruction of Personal Information, whether it is by anContegrty Ethics employee or officer, or an external party;
- loss or theft of devices (such as laptops or mobile phones) or paper records, that contain Personal Information;
- disclosure of Personal Information due to human error, for example by placing information online in a way that can be accessed or sending an email to the wrong person; and
- system errors which lead to disclosure of Personal Information, such as misconfiguration of access permissions to a supplier or posting of data in a public arena.

Personal Information is information about an identified individual, or an individual who is reasonably identifiable. Information that is not about an individual on its own can become Personal Information when it is combined with other information, if this combination results in an individual becoming reasonably identifiable as a result.

A Data Breach may be caused by malicious action (by an external or insider party), human error, or a failure in information handling or security systems.

5.2 Consequences of a Data Breach

A Data Breach can cause significant harm to both individuals whose Personal InformationContegrty Ethics holds as well as toContegrty Ethics as an organisation.

- Individuals whose Personal Information is involved in a Data Breach may be at risk of serious harm, including harm to their physical or mental well-being, financial loss, or damage to their reputation.
- A Data Breach can also negatively impactContegrty Ethics' reputation and cause damage to its commercial interests.

Contegrity Ethics can reduce the reputational impact of a Data Breach by minimising the risk of harm to affected individuals, and by demonstrating accountability in its Data Breach response. These are both key objectives of this Data Breach Response Plan.

6. Responding to a Suspected Eligible Data Breach

In the event of a Suspected Eligible Data Breach the person who discovers the breach should immediately contactContegrty Ethics' director in person or by phone.

The Data Breach Response Team consists of the persons holding the following positions inContegrty Ethics or supportingContegrty Ethics as a consultant:

- Director and Privacy Officer
- Legal resource
- Cybersecurity/IT

EUROPEAN/GDPR DATA BREACH

In the event of a GDPR Data Breach, the GDPR requires organisations to report GDPR Data Breaches to the relevant supervisory authority within 72 hours of becoming aware of the GDPR Data Breach, where feasible. If the GDPR Data Breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms,Contegrty Ethics must also inform those individuals without undue delay.

6.1 Overview

The Data Breach Response Team should carry out the following steps:

(a) Conduct a preliminary assessment of the Suspected Eligible Data Breach to determine whether immediate steps can and should be taken to contain the Data Breach.

(b) Conduct a Risk Assessment to assess the severity rating of the Suspected Eligible Data Breach. This step will also include determining whether a Data Breach did in fact occur.

(c) Conduct any further steps required to contain the Data Breach if it was not fully contained in step (a) above.

(d) Determine whether an Eligible Data Breach has occurred within 30 days, or lesser period if required under relevant Privacy Laws.

(e) Notification of Eligible Data Breaches to affected individuals.

(f) Assess what steps are required to prevent future Data Breaches.

(g) Prepare a Data Breach Incident Report.

A Data Breach Incident Reporting Form (Appendix I) should be completed byContegrty Ethics in all instances of a Data Breach or Suspected Eligible Data Breach.

6.2 Assess Containment of the Data Breach - Preliminary Risk Assessment

Once a Suspected Eligible Data Breach has been identified, a preliminary Risk Assessment should immediately be undertaken to determine what initial steps (if any) should be taken to contain the Suspected Eligible Data Breach. This Risk Assessment must be undertaken by the person or persons most suitably qualified to carry out the initial investigation.

By way of example, if the cause of the Suspected Eligible Data Breach is that Personal Information has been placed on a public website, such information should be immediately removed from the website, where this can be achieved. If, however, it is suspected that a person has maliciously breachedContegrty Ethics' information systems, before taking any steps which may alert the hacker thatContegrty Ethics is aware of their presence it is important to gain an understanding of:

(a) how and when they accessedContegrty Ethics' systems (hackers may have been in the system for a considerable period of time prior to being discovered);

(b) the information or systems they have accessed or were seeking to access;

(c) the suspected objectives of the hacker (for example, usingContegrty Ethics to access third party systems versus ransomware);

(d) whether there are back-ups of any vital information (a hacker may delete or encrypt information).

The following questions should be addressed when conducting the preliminary Risk Assessment of a Suspected Eligible Data Breach:

- What information is involved, and what is the nature of that information?
- What was the cause of the Data Breach?
- What is the extent of the Data Breach?
- What are the harms (to customers/affected persons) that could potentially be caused by the Data Breach?
- How can the Data Breach be contained?

Further actions may include interviews with staff involved and/or affected, or the request of further investigation by appropriate IT staff or external advisors into system failures or security issues.

If in the course of conducting the preliminary Risk Assessment it is determined that there is a likelihood of serious harm being caused to an affected individual as a result of a Data Breach, then urgent remedial action should be taken to contain the Data Breach to try to prevent serious harm from occurring. Given the nature of Personal Information held byContegrty Ethics, any customer information affected by a Data Breach will require urgent remedial action.

6.3 Assess whether third parties are involved

Assess whether the Suspected Eligible Data Breach may have arisen due to action or inaction by a third-party service provider which:

- has access to Confidential Information or Protected Business Information;
- has connections intoContegrty Ethics Information Processing Facilities/ Systems; and/or
- provides a technology solution or platform being used byContegrty Ethics.

Alternatively, anContegrty Ethics service provider may notifyContegrty Ethics of a Suspected Eligible Data Breach involvingContegrty Ethics data.

Where appropriate and possible, contracts should be enforced, or other legal steps taken to ensure that such third party:

(a) co-operates reasonably withContegrty Ethics in relation to the Suspected Eligible Data Breach, including providing all information and assistance reasonably required;

(b) independently and expeditiously assess whether or an Eligible Data Breach has occurred;

(c) prior to reporting an Eligible Data Breach, informContegrty Ethics of its intention to report the Data Breach and allowContegrty Ethics a reasonable period to respond before proceeding. Where the parties have formed differing views as to whether an Eligible Data Breach has occurred, the parties shall use reasonable efforts to obtain alignment and, in respect of a Suspected Eligible Data Breach involving onlyContegrty Ethics Data,Contegrty Ethics' view should take precedence.

6.4 Engagement of external resources

Consider what, if any, external resources or expertise should be engaged. This could include:

- forensic data experts
- IT system or network specialists
- legal support
- media or communications specialists.

6.5 Conduct a Risk Assessment

The following factors are relevant when conducting a Risk Assessment:

(a) The type of information involved in the Suspected Eligible Data Breach

- Is it Personal Information, Sensitive Information or Confidential Information?
- Does the type of information that has been compromised create a greater risk of harm?
- Who is affected by the Suspected Eligible Data Breach?

(b) Determine the context of the affected information and the Suspected Eligible Data Breach

- What is the context of the information involved?
- What parties may or are known to have gained unauthorised access to the affected information?
- Have there been other Data Breaches that could have a cumulative effect?
- How could the information be used?

(c) Establish the cause and extent of the Data Breach

- Is there a risk of ongoing Data Breaches or further exposure of the information?
- Is there evidence of theft or other malicious intent?
- Is the information adequately encrypted, anonymised or otherwise not accessible?
- What was the source of the Data Breach? (Risk of harm may be lower where source of the Data Breach is accidental rather than intentional)
- Has the information been recovered and protected?
- What steps have already been taken to mitigate the harm?
- Is this a systemic problem or an isolated incident?
- How many individuals are affected by the Suspected Eligible Data Breach?

(d) Assess the risk of harm to the affected persons

- Who is the recipient of the information?
- Does the recipient have a malicious purpose?
- What harm to persons could result from the Suspected Eligible Data Breach?

(e) Assess the risk of other harms

Other possible harms, including toContegrty Ethics or third parties it transacts with that may be suffered because of the Suspected Eligible Data Breach, including:

- Loss of public or customer trust
- Reputational damage
- Legal liability
- Breach of third-party confidentiality obligations.

The Data Breach Impact Severity Ratings Form in Appendix 2 provides a standardised approach for assessing the severity of a Suspected Eligible Data Breach and outlines the reporting requirements for Data Breach notification.

7. Containment of the Data Breach

If the Data Breach was not fully contained following the preliminary Risk Assessment, once sufficiently detailed analysis has been conducted in relation to the source of the Data Breach and any required steps have been taken to obtain a back-up of impacted data, the Data Breach should be fully contained.

This step should be carried out concurrently with some of the activities in the preliminary Risk Assessment if in the course of conducting the preliminary Risk Assessment it is determined that there is a likelihood of serious harm being caused to an affected individual as a result of a Suspected Eligible Data Breach. Under these circumstances, urgent remedial action should be taken to contain the Data Breach to try to prevent serious harm from occurring.

8. Eligible Data Breach Determination

8.1 Assessment of Data Breach

Contegrity Ethics must carry out a reasonable and expeditious assessment of whether there are reasonable grounds to believe that the relevant circumstances amount to an Eligible Data Breach within 30 days of first becoming aware of a Suspected Eligible Data Breach, or such shorter period if required under Privacy Laws. Where possible,Contegrty Ethics must endeavour to complete the assessment in a much shorter timeframe, as the risk of serious harm to individuals often increases with time. If this is not possible,Contegrty Ethics should document the reasonable steps taken and the reasons for the delay.

This test to determine whether the incident is an Eligible Data Breach involves deciding whether, from the perspective of a reasonable person, the Data Breach would be likely to result in serious harm to an individual whose personal information was part of the Data Breach.

For these purposes, a ‘reasonable person’ means a person inContegrty Ethics’ position (not an individual whose Personal Information was part of the Data Breach), who is properly informed, based on conducting a Risk Assessment. In general,Contegrty Ethics would not be expected to make external enquiries about the circumstances of each individual whose information is involved in the Data Breach.

8.2 Factors to be considered

Consider the following factors as a whole, having regard to the likelihood of the harm eventuating for individuals whose Personal Information was compromised due to the Data Breach and the consequences of the harm, in addition to any other relevant matters:

- the kind(s) of information compromised
- the sensitivity of the information compromised
- whether a security technology or methodology was used to protect the information, and whether it was designed to encrypt the information or make it meaningless to unauthorised persons
- if the information is protected by one or more security measures, the likelihood that any or all of those security measures could be overcome
- the persons, or the kinds of persons, who have obtained, or who could obtain, the information
- the geographic location of any computers and IT systems used to hack intoContegrty Ethics’ information systems
- the likelihood that the persons, or the kinds of persons, who have obtained or could obtain the information:
    - have the intention of causing harm to any of the individuals to whom the information relates;
    - have obtained, or could obtain, information or knowledge required to circumvent the security technology or methodology; or
    - are likely to attempt to sell or transfer the information to third parties or publish the information online, including on the Dark Web;
- the nature of the harm to any individual.

8.3 Loss of Protected Company Information

A Data Breach involving loss of Protected Company Information or Business Critical Data could cause significant damage toContegrty Ethics but may not be an Eligible Data Breach. Although notification may not be required under the Privacy Laws, all other steps should be taken in this Data Breach Response Plan, including remedial action to mitigate unauthorised access to and use of Protected Company Information or impact on the availability of Business Critical Data and to assess systems to prevent future Data Breaches.

8.4 Data breach impact severity ratings

The Risk Assessment assigned to a Data Breach or Suspected Eligible Data Breach can range from negligible to very high and should be considered against each of the categories below:

- Are multiple individuals affected?
- Does the Data Breach or Suspected Eligible Data Breach involve Personal Information or Confidential Information?
- Does the Data Breach or Suspected Eligible Data Breach involve financial information or other Sensitive Information?
- How long has Personal Information or Company Information been accessible? The longer it has been accessible, the higher the likelihood that serious harm may result.
- What specific harms could potentially result from a specific Data Breach or Suspected Eligible Data Breach? Examples may include identity theft; financial loss; threats to an individual's physical safety; loss of business or employment opportunities; humiliation; or damage to reputation or relationships.
- What is the likelihood (now or potentially in the future) of the Data Breach leading to serious harm to the affected individual(s)?
- Does the Data Breach or Suspected Eligible Data Breach:
    - pose a threat toContegrty Ethics or third-party systems, or their capacity to deliver services
    - indicate a systemic problem withContegrty Ethics practices or procedures?
- Could the Data Breach or Suspected Eligible Data Breach cause financial loss toContegrty Ethics or liability to a third-party?

8.5 Has Remedial Action Succeeded

If remedial action taken byContegrty Ethics to contain the Data Breach results in the risk of serious harm to affected individuals being avoided, it will not be considered an Eligible Data Breach. Remedial action can be taken before, or in the course of managing, a Data Breach incident.

Examples of this include:

- ensuring that appropriate and up-to-date security mechanisms are deployed acrossContegrty Ethics' networks and devices containing Personal Information;
- ensure that files are properly encrypted, with the corresponding encryption keys stored in a separate and secure location;
- where Personal Information has been accidentally sent to an incorrect person, seeking a binding assurance from the recipient declaring that they did not copy the information and have deleted the material.

Notwithstanding the above, any Data Breach involving customer Personal Information will always be considered an Eligible Data Breach.

9. Notification to Affected Individuals

9.1 Notification process

Notification should occur as soon as reasonably possible after a determination has been made that an Eligible Data Breach has occurred and should be direct by phone or email to the affected individuals. The notification should include the following information:

- Incidence description
- Type(s) of information involved
- Response to the Data Breach
- Assistance offered to affected persons
- Whether the Data Breach was notified to external regulators (OAIC)
- Legal implications
- How individuals can lodge a complaint with the company or the relevant regulatory bodies (OAIC)

9.2 Reporting to OAIC

The OAIC recommends that the following factors be considered when deciding whether to report a breach to them:

- Any applicable legislation that may require notification
- The type of Personal Information involved and whether there is a real risk of serious harm arising from the Data Breach
- Whether the Data Breach affected many people
- Whether the information was fully recoverable without further disclosure
- Whether the affected individuals have been notified
- If there is a reasonable expectation that the OAIC may receive complaints/inquiries about the Data Breach

9.3 Notification to other parties

In addition to notification to affected individuals and to the OAIC,Contegrty Ethics should consider whether notification should be made to other parties such as:

- Contegrity Ethics' financial services provider
- Police or law enforcement bodies
- the Australian Securities & Investments Commission (ASIC)
- the Australian Taxation Office (ATO)
- the Australian Transaction Reports and Analysis Centre (AUSTRAC)
- the Australian Cyber Security Centre (ACSC)
- State or Territory Privacy and Information Commissioners
- Insurance providers
- Contegrity Ethics' customers
- Strategic partners/suppliers/vendors

10. Preventing Future Breaches

Once steps have been taken to mitigate the risks associated with a Data Breach, the Data Breach Response Team must take the time to investigate and understand the root cause of the Data Breach and conduct debriefing sessions with relevant staff to determine if:

- changes toContegrty Ethics' policies and procedures are necessary;
- additional resources are recommended to reduce the chances of future Data Breaches occurring;
- further staff training should be undertaken;
- the response to the Data Breach was timely and appropriate; and
- the Data Breach Response Plan was effective in dealing with the Suspected Eligible Data Breach and whether harm to individuals was prevented, mitigated or reduced.

The Data Breach Response Team should ensure that any necessary recommendations are allocated and actioned appropriately.

The significance of the Data Breach should be reviewed as to whether it was an isolated event or a recurring breach. A prevention plan should include:

- A security audit of both physical and technical security
- Implementing necessary fixes to minimise the likelihood that the Information Security Incident can reoccur. This may involve closing down vulnerabilities, applying patches, closing ports.
- A review of employee selection and training practices
- A review of policies and procedures to reflect the lessons learned from the investigation
- Staff training in preventing and responding to Data Breaches effectively.

11. Prepare Data Breach Incident Report

This report should follow the format of the form in Appendix 1 and document:

- the suspected or actual Data Breach;
- the process followed in response to becoming aware of the Suspected Eligible Data Breach;
- rationale for determining whether or not the Information Security Incident was an Eligible Data Breach; and
- any steps taken to prevent future Data Breaches.

12. Definitions

The following terms and abbreviations are used in this document:

Term	Definition
Availability of information	Information is available and accessible to authorised individuals when it is needed.
Business Critical Data	Data which must remain available to prevent business disruption and loss of revenue.
Confidential Information	Information that is not known to, or readily accessible by, the public and disclosure of that information could cause harm to or disadvantage a person or organisation. Access and disclosure of Confidential Information must be controlled and will only be given to persons who require access to perform their duties.
Confidentiality of information	Information is not made available or disclosed to unauthorised individuals, entities, or processes.
Data Breach	An Information Security Incident, in which Personal Information, Confidential Information or Business Critical Data is lost or subjected to unauthorised access, modification, disclosure, or other misuse or interference.
Eligible Data Breach	A Data Breach which has caused serious harm to an individual requiring notification under the Notifiable Data Breaches Scheme in the Privacy Act.
GDPR	General Data Protection Regulation, the equivalent to the Australian Privacy Act 1988 (Cth) in the European Union, which took effect in May 2018 and enacted individually in member countries (for example, applying in the UK via the Data Protection Act 2018).
GDPR Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data (GDPR equivalent of Personal Information), whether due to accidental or deliberate causes.
Information Security	Preservation of Confidentiality, Integrity and Availability of information.
Information Security Incident	An identified occurrence of a system, service or network state indicating a possible breach of Information Security policy or failure of safeguards, or other situation that has a significant probability of compromising business operations and/or threatening information security or otherwise may be security relevant.
Integrity of information	Maintaining the accuracy and consistency of information, which requires that only authorised people can modify information.
OAIC	Office of the Australian Information Commissioner.
Personal information	Any information or an opinion about an identified individual, or an individual who is reasonably identifiable, as defined in the Privacy Act.

Term	Definition
Privacy Act	Privacy Act 1988 (Cth).
Privacy Laws	Privacy laws which are applicable to a specific Data Breach, which may include the Privacy Act, and/or the GDPR and equivalent laws in other jurisdictions.
Protected Company Information	Confidential Information aboutContegrty Ethics and its customers, suppliers and other entities. Protected Company Information is held in many forms, including but not limited to paper reports, computerised databases, and documents and it may be transmitted in many ways including by hand, by courier, or electronically using email or through systems controlled byContegrty Ethics or by external third-parties.
Risk Assessment	The process of identifying, evaluating, and estimating the levels of risks associated with a known Data Breach or Suspected Eligible Data Breach. For the purposes of this Data Breach Response Plan, it includes determining whether it appears probable that a Data Breach has occurred, and the classification of information compromised in accordance with the Data breach Impact Severity Rating.
Sensitive Information	A sub-set of Personal Information as defined in the Privacy Act which is given a higher level of protection under the National Privacy Principles, and includes an individual's financial information.
Suspected Eligible Data Breach	An Information Security Incident in which there are reasonable grounds to suspect that there may have been a Data Breach which could be an Eligible Data Breach.

Appendix 1 - Data Breach Incident Reporting Form

PART A - Information to be completed by the person reporting the incident (after notifying a member of the Data Breach Response Team in person or by phone)

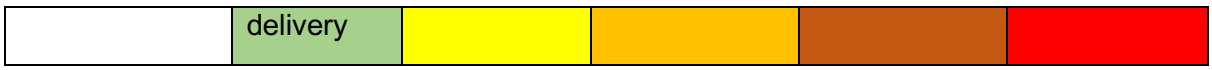
Full name	
Position Title and Department	
Contact information	
Details of the incident	
Date, time, duration, and location of the Suspected Eligible Data Breach	
How was the Suspected Eligible Data Breach discovered	
Description of the Information Security Incident, including whatContegrty Ethics systems may be affected	
Cause of the Data Breach (if known)	
Did any other staff member witness the Information Security Incident at the time?	
Signature:	Date:

PART B - Information to be completed by a member of the Data Breach Response Team

Did a Data Breach occur?	
Duration and location of the Data Breach	
Contegrity Ethics' systems affected	
Cause of the Data Breach	
Data Breach impact severity rating (refer to Appendix 2)	
Provide reasoning for the allocation of the Data Breach impact rating	
Notification assessment	
Details of remedial action or improvements recommended	

Appendix 2 - Data breach Impact Severity Rating Form

Impact Severity	Negligible	Low	Medium	High	Very high
Risk to individual safety due to unauthorised access or disclosure of Confidential/ Personal Information	No injury/ minimal risk to personal safety	Single injury/low risk to personal safety of client/ employee/ consumer	Multiple injuries/moderate risk for safety of client/ employee/ consumer	Death/disabling injury/high risk to safety of client/ employee/ consumer	Multiple deaths or disabling injuries/very high risk to safety of client/ employee/ consumer
Distress caused to any party or damage to any party's standing or reputation	Negligible no public concern- only routine internal reporting	Minor distress, minor damage – visible limited/ localised media interest, internal reporting	Substantial short-term distress – restricted negative publicity from local media, internal inquiry	Substantial long-term distress – mainstream media report, internal inquiry	Substantial long-term distress to multiple parties – broad public concern and media coverage
Non-compliance- unauthorised release of information classified as protected or confidential, to a third-party	Minor compliance issues – no or negligible impact, offence punishable by small fine	Short- to medium-term action required – minor impact, offense punishable by moderate fine	Immediate action needed to achieve compliance – measurable impact offense punishable by major fine	Shutdown of service for non-compliance – significant impact offence punishable by imprisonment	Shutdown of multiple services for non-compliance – major consequences to a person or agency
Threat toContegrty Ethics capacity to deliver services due to Information Security Incident	No or negligible threat to, or disruption of business or systems of service	Minimal threat to, or disruption of localised business or systems or service delivery	Moderate threat to or cessation of a service for a week, and subsequent disruption	Multiple essential/ critical services impaired or disrupted over a month	Cessation of multiple essential/ critical services for several months



Appendix 3 - Data Breach Response Summary

1. Notify and assemble the Data Breach Response Team
2. Assess nature and intent of Data Breach – accident vs ransomware
3. Assess steps required to contain the Data Breach
4. Where practicable, remediate the issue which led to the Data Breach
5. Assess nature of information affected by Data Breach – Personal Information vs Confidential Information
6. Identify relevant legal jurisdictions applicable to Data Breach – Australia vs Australia and Europe/USA
7. Understand timeframes mandated in applicable Privacy Laws to notify impacted individuals
8. Notify other relevant internal or external stakeholders
9. Identify impacted individuals
10. Assess harm caused to impacted individuals
11. Assess whether notification is required to impacted individuals
12. Notify impacted individuals if required under Privacy Laws or if notification decision is made on other grounds
13. Notify regulatory agencies if required under Privacy Laws
14. Consider steps required to strengthen Cybersecurity posture to address weaknesses exposed by the Data Breach