# Incident Response Plan

## Document Control Information

|  |  |
| --- | --- |
| File Name |  |
| Description |  |
| Version |  |
| Classification  |  |
| Policy First Effective Date |  |
| Policy Approval Date (Current Version) |  |
| Policy Effective Date (Current Version) |  |
| Next Policy Review Date |  |
| Document Owner |  |

## Revision History

This document is formally reviewed at least annually (including when there are significant changes to the business, when risks are identified, when there are changes to adopted standards or when there are changes in legal regulations that impact. Interim updates will be documented and integrated as required in response to changing business objectives or the risk environment. Changes will be communicated as broadly as possible through the use of email, company announcements, and other methods as applicable.

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Comments |
|  |  |  |  |

## Contents

[Incident Response Plan 1](#_Toc52279770)

[Document Control Information 1](#_Toc52279771)

[Revision History 1](#_Toc52279772)

[Contents 2](#_Toc52279773)

[Purpose 3](#_Toc52279774)

[SCOPE 3](#_Toc52279775)

[Communication Plan 4](#_Toc52279776)

[Incident management 5](#_Toc52279777)

[What Is a Cyber Security Incident 5](#_Toc52279778)

[Who Is On The Incident Response Team? 6](#_Toc52279779)

[Declaring A Cyber-Security Incident 6](#_Toc52279780)

[Incident Severity Levels 7](#_Toc52279781)

[Identification 8](#_Toc52279782)

[Incident Response 10](#_Toc52279783)

[Incident Response Team Contact Details 13](#_Toc52279784)

[Appendix a 14](#_Toc52279785)

[Incident Register 14](#_Toc52279786)

[Cyber-Security Initial Assessment Checklist 15](#_Toc52279787)

[Cyber-Security Incident Initiation Checklist 16](#_Toc52279788)

[Recovery Progress Checklist 17](#_Toc52279789)

[Cyber-Security Incident Close Checklist 18](#_Toc52279790)

[Definitons 19](#_Toc52279791)

## Purpose

Cyber Security incidents will be managed within, and integrated to, existing operational procedures. This document should be stored in a location that is secure but accessible to all required parties. In addition to this, backup copies should be stored in other locations to ensure its availability. The core storage point should always be treated as the ‘source of truth’ and most updated version. Ideally, summary sections should be printed and laminated, pinned to office walls similar to fire escape plans.

## Scope

The scope of this procedure includes:

* All employees
* All Contractors and Consultants working on our software
* Assessment of any software purchased for use in

# Communication Plan

## Responsibilities

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Function | Name | Title | Email | Phone |
| Communication Lead |  |  |  |  |
| Backup Communication Lead |  |  |  |  |
| PR Lead |  |  |  |  |
| Internal Communications Lead |  |  |  |  |

## Public Communication Template

## Public Communication Channels

*
*
*

## Internal Communication Template

## Internal Communication Channels

*
*

# Incident management

## What Is a Cyber Security Incident

Cyber-security incidents are those in the following categories:

|  |  |
| --- | --- |
| Category | Example |
| Infrastructure compromises or defence breach | Network denial of service attack, network intrusion |
| Server system compromise | Network intrusion via website(s) (including website defacement), disruption of system service (potentially involving network, hardware, software or system failures) |
| Social engineering | Spreading bad press, impersonating website(s), communications (bills, etc.), or identity (in social network, discussion forums, etc.), phishing phone call, phishing email |
| Malware | Malware (including malicious mobile codes via email / web / other means) |
| Control system compromise or failure | Control system attack or attacks impacting control systems |
| Inappropriate usage or conduct | Misuse of IT systems, unauthorised disclosure of information (e.g. posted to internet forums), unauthorised destruction of information |

##  Who Is On The Incident Response Team?

The Cybersecurity Incident Response Team consists of the following members:

* COO
* PMO Manager
* Technical Lead
* Data Quality Manager
* DevOps Manager

## Declaring A Cyber-Security Incident

Any of the following team members can declare an Incident/vulnerability:

## Incident Severity Levels

The following table illustrates common Severity Levels for Cyber-security incidents:

|  |  |  |
| --- | --- | --- |
| Incident Level | Scope of Incident | Incident Response Focus |
| Level 4 | Occurs within a business unit. Little or insignificant disruption to service operations. | Incident managed within by own resources |
| Level 3 | Affects a few business units within. Minor disruption to service operations. | Incident managed within by using additional resources. Notification to other business units for information or support. |
| Level 2 | Widespread within one or more business units. Medium to High impact to service operations. | Incident managed with the assistance of external parties.  |
| Level 1 | Catastrophic. Major disaster within with large scale disruption to service operations.  | Incident managed with the assistance of external parties. |

## Identification

A potential cybersecurity incident may be identified from a range of sources. An initial evaluation needs to be undertaken to determine if it constitutes an incident for the purposes of activating this plan. The following diagram illustrates the workflow:



Where a staff member or IT support staff suspect a cybersecurity incident they should:

* Advise IT Support staff/lodge a service desk incident
* Immediately notify their Line manager

The first priority in any incident is to ensure physical safety and, if there is a chance of the incident further spreading, isolate the environment.

Normally IT support staff will recognize and review a suspected incident with the Manager. They will make an initial determination of the incident, and if they deem it necessary the COO or DevOps Manager will activate this plan.

The COO, DevOps Manager or another member of the Cyberecurity Incident Response team in their absence, will use a range of factors to determine whether to activate this plan. Including, but not limited to, the following:

* A Level 1 or Level 2 severity incident (mandatory activation)
* Who is affected by the incident or suspected incident? Multiple individuals?
* Is there a real or suspected risk of serious harm to the affected individuals?
* Does the incident or suspected incident indicate a systemic problem in processes or procedures?
* Could there be media or stakeholder attention because of the incident or suspected incident?
* is there a significant reputational risk to <CLIENT NAME> as a result of the incident?

## Incident Response

The following workflow outlines the process to be undertaken once an incident has been declared. Note that an incident may be declared as the result of an initial assessment, or by advice from the Incident Management Team.





### Step 1 – Assemble IRT And Validate Initial Assessment

Within 2 hours of a cybersecurity Incident being declared, the COO or DevOps Manger must:

1. Assemble the Incident Response team and validate the initial assessment;
2. Take all necessary steps to ensure physical safety and, or required, isolate the environment;
3. Ensure evidence is preserved that may be valuable in determining the cause of the incident;

### Step 2 – Initial Investigation / Development Of Rectification Plan

As a next step, the Incident Response Team perform an initial investigation

Collect information about the incident, including:

• Nature and extent of the incident

• Advice from external parties

• Impacted services and/or external organisations

• Any other risks

Develop a rectification plan; and

Seek Management approval to proceed (where possible).

### Step 3 – Implement Rectification Plan

The team will manage the rectification process, including;

1. Meetings to review progress;
2. Communications updates;
3. Assess if there is a requirement to bring in external resources from other agencies or companies to assist;
4. Documentation of activities undertaken; and
5. Identification of follow up actions.

### Step 4 –Standown/Review

When the Incident is believed to have been resolved, the Team will;

1. Document any further actions required to resolve issues arising from the incident;
2. Document any further actions required to prevent a re-occurrence;
3. Seek approval to stand down.

### Step 5 –Post Incident Activities

A range of further activities take place after the incident has been resolved. These include:

1. A post Incident Review to identify any learning and improve this process;
2. Perform any required (regulatory) notifications;
3. Follow-up on outstanding action items; and
4. Ensure appropriate communication and progress updates are performed, as a next step, the Incident Response Team perform an initial investigation

# Incident Response Team Contact Details

|  |  |  |
| --- | --- | --- |
| Role | Email | Phone |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Appendix a

## Incident Register

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Date of Occurrence | Incident Description | Incident Level | Frequency | Impact Description | Root Cause Analysis | Recovery Action | Corrective Action |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

## Cyber-Security Initial Assessment Checklist

|  |  |
| --- | --- |
| Incident |  |
| Date |  |
| Logged By |  |
| Perform initial impact analysis. Write a description of the incident and how it is being evidenced |
| If deemed necessary isolate environment in which incident has occurred. Ensure that steps have been taken to ensure the physical safety of staff  |
| Determine whether incident response plan should be invoked. Review with Manager – Information Technology |
| Update department co-ordinators |

## Cyber-Security Incident Initiation Checklist

|  |  |
| --- | --- |
| Incident |  |
| Date |  |
| Logged By |  |
| Ensure relevant IRT members present |
| Review/validate initial assessment and if deemed necessary, further isolate the environment |
| Appoint communications co-ordinator, perform initial communication to relevant internal parties |
| Advise external parties (if required) |
| Determine action plan for resolution. Include review points and communication points |
| Commence implementation of resolution |

##

## Recovery Progress Checklist

|  |  |
| --- | --- |
| Incident |  |
| Date |  |
| Logged By |  |
| Milestone |  |
| Review the steps taken so far. Have they had the anticipated affect? Has the outcome or any additional information changed what they have to do next? |
| Has the problem changed in dimension (got bigger or smaller)? Do we need to change approach? |
| Have we appraised key stakeholders of progress? |
| Have we reviewed/documented outstanding actions? Can any of these be deferred to post-incident? |
| Are we in a position to stand down IRT? |

## Cyber-Security Incident Close Checklist

|  |  |
| --- | --- |
| Incident |  |
| Date |  |
| Logged By |  |
| Have all immediate risks to business been mitigated |
| Have business functions returned to acceptable operations |
| Have third party services been able to resume required level of service delivery |
| Have we collated all relevant action and event logs |
| Have all identified outstanding actions been documented and are they in a position to handover to operations teams for completion |
| Are all members of the IRT satisfied that the incident has been dealt with, and any remaining actions can be handled operationally |
| Has all IRT documentation been completed and collated? |
| Have respective risk registers been updated (if required), to reflect any new or changed business risk as a result of this cyber-incident |
| Has the COO approved the Team to stand down |

##

## Definitons

| Term | Definition |
| --- | --- |
| Australian Privacy Principles | Are legally binding principles under the Privacy Act that sets out standards, rights and obligations in relation to handling of Personal Information. |
| Data Breach | Means,for the purpose of this Data Breach Response Plan, when Personal Information held by <CLIENT NAME> is lost or subjected to unauthorised access, use, modification, disclosure, or other misuse. |
| Personal Information | Means information or an opinion about an identified individual, or an individual who is reasonably identifiable: Whether the information or opinion is true or not; and Whether the information or opinion is recorded in a material form or not. |
| Privacy Act | Means the *Privacy Act 1988* (Cth) which regulates the handling of Personal Information about individuals. This includes the collection, use, storage and disclosure of Personal Information, and access to and correction of that information. |
| Privacy Commissioner | Means the Privacy Commissioner that forms part of the Office of the Australian Information Commissioner (OAIC) and has responsibility for regulating and providing advice on the operation of the Privacy Act and other privacy-related legislation. |
| Sensitive information | As a subset of Personal Information and is defined as: • Information or an opinion (that is also Personal Information) about an individual’s: Racial or ethnic origin;Political opinions;Membership of a political association; Religious beliefs or affiliations; Philosophical beliefs or membership of a professional or trade association;Membership of a trade union; Sexual preferences or practices; orCriminal record; • Health information about an individual;• Biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or • Biometric templates. |
| Tax File Number Information | Means information, whether compiled lawfully or unlawfully, and whether recorded in a material form or not, that records the tax file number of a person in a manner connecting it with the person’s identity. |