Document Reference:	Redback-Incident-Form	Effective Date:	3rd December 2023
Document Name:	Incident Form and Tracker Details	Expiry Date:	3rd December 2024

Incident Form and Tracker Details

Cyber Security

Redback Operations

Document Owner:	Joel Daniel	Last Modified By:	Joel Daniel
Next Review Date:	11th March 2024	Last Modified on:	3rd December 2023

Version	Modified By	Approver	Date	Changes made
0.1	Joel Daniel		27th Nov 2023	Initial Draft
0.2	Joel Daniel		2nd Dec 2023	Updated to align with completed Incident Response Plan criteria and requirements.

Table of Contents

1 Purpose and Scope of the Policy

The purpose of this document is to detail the various information that will be collected in order to ensure that data of incidents are accurately and reliably collected. The scope will cover the Incident Form and the Incident Tracker.

2 Incident Tracker

The Incident Tracker contains the basic required data for identifying and managing incidents, which would be handled in the incident sheet.

- Incident Form = https://docs.google.com/forms/d/e/1FAIpQLSew9gGm9P20o3q3Jg_tMQD0oqJJjEDeQ-iOHz-j1b8ZcLWI8Q/viewform?usp=sf_link
- Incident Sheet = https://docs.google.com/spreadsheets/d/12jbbfF7W08v5nt71Yem1DG6xAYcG5v2pxNItIYBle2E/edit?resourcekey#gid=1034913739

2.1. Incident Form (at escalation)

The form has select fields which need to be populated immediately when an incident is being escalated:

- Incident Name/Title = Name of the Incident
- Date and Time of Incident = Immediate Date and Time of Incident occurrence (not date and time of escalation).
- Affected Asset/Username/Data = The targeted entity (multiple entities mention the name of the most sensitive/priority entity followed by etc… [eg:- test@deakin.edu.au, etc….)
- Severity = The severity of the Incident
- Priority = Time period within which the incident needs to be resolved (often aligns with Severity level and/or affected assets)
- Incident Category = Type of Cyber Incident
- Affected Project = The project in the company affected by the incident.
- Incident Escalator = The person reporting the incident.

2.2. Incident Sheet (post escalation)

Alongside the above fields, the sheet storing the collected data contain additional fields that will be filled post escalation directly by the cyber security team/analyst:

- Incident ID = A unique ID to identify incidents.
- Expected Incident Resolution Date and Time = Based on Priority, date and time at which the incident should be resolved.
- Incident Resolved = Yes/No question tracking incident resolution.
- Incident Resolution Date and Time = Date and Time when incident was resolved.
- Resolution Reason = Summarized reason on resolving issue (problem solution).
- Additional Comments = Additional information for noting incident.

In addition, due to information found during investigation analysis, only these fields within the sheet can be changed after escalation by the cyber security team if required:

- Date and Time of Incident
- Incident Category
- *Severity and Priority can be changed only after discussion and agreement with the relevant stakeholders and authority in relation to what's dictated in the Cyber Incident Response Plan, regardless of whether data provided was by accident or not.*

3 Incident Record

The Incident Record provides a comprehensive view on the investigation carried out for the incident, which may continuously, even post resolution, be updated with various findings such as evidence, involved threats, carried out actions etc….

The Incident Record is to be accessed and filled only by the cyber security team and authorized analysts. Other stakeholders (affected project members, company board, legal entities) are allowed to only view the document.

The Incident Record template can be found at https://deakin365.sharepoint.com/:w:/r/sites/RedbackOperations9/Shared%20Documents/Cyber%20Security%20Team/2023%20Trimester%203/Cyber%20Security%20Incident%20Record%20Template.docx?d=w62a6a73bf4fa4110999fc224e3987dfc&csf=1&web=1&e=nc5PPY.

The following information need to be filled:

- Incident ID = Unique code for identifying incidents
- Incident Title = Name of the incident
- Date and Time of Incident = Date and Time of detection of incident
- Date and Time of Escalation = Date and Time of escalation of incident
- Timezone = Timezone of incident when first escalated
- Incident Severity = Severity of the Incident
- Incident Priority = Priority Category of the incident
- Incident Category = Type of cyber incident
  Refer Incident Form and/or Cyber Incident Response Plan for list of Severity, Priority and Category
- Affected Project = Project impacted by the incident
- Affected Assets = Entities owned by the company/project that are impacted by the incident
- Incident Manager = Names of Cyber Security Analyst assigned to incident and Incident Escalator
- Incident Tags = Quick identifiers

- Incident Summary = Brief summary on the cause of the incident and initial actions carried out.
- Incident Timeline = A summarized detail of all events directly related to the incident, including but not limited to; attack events, initial steps taken by employees to contain and eradicate the attack, changes in states of affected assets, compromise times etc…
  - Each event must precede the date and time per line.
- Actions taken in Incident = Actions taken by company members to identify, analyze, contain and eradicate threats in the incident must be mentioned in point form. Chronological order of actions must be maintained as much as possible with comprehensive detail.
- Status of actions required to be taken per playbook/incident response plan = Based on provided playbooks and/or the company incident response plan, select actions are required for incidents. These actions need to be noted down and then answered whether they were carried out and the result (if no, why not must be mentioned).
- Incident Findings = Evidence, Events and other information not initially showcased when incident was escalated and results of investigations are to be placed here.
- Threat Actors and Vectors = Identified responsible parties for the incident (malware family, APT etc….) as well as the mode of delivery (external hardware, Internet, email etc…) and affected vulnerabilities (if any) must be mentioned here. Each line must have a basic detail followed by sub points of extensive information.
- Additional Details = Information regarding the various questions that the Incident Response Plan requires to be answered alongside additional findings such as supporting evidence, involved indirect parties etc…..can be mentioned here.
- Incident Resolution = Date and Time of complete Incident Resolution should be mentioned at the beginning.
  - Steps taken = These are steps taken to resolve and confirm resolution of the incident. Select steps may also be part of the “Actions taken in Incident” section which can involve restoration of operations, restoration of backups, blacklisting etc…
  - Incident Impact and Outcome = The impact of the incident in terms of company loss (financial/data/time/power/operations etc….) must be mentioned. Each impacts corresponding outcome (loss of customers, damaged resources, recreation of system etc….) should be mentioned here. Improvements in system post incident resolution, relevant trainings, even identified potential benefits and opportunities can also be mentioned.

- Legal and Governing Entities = This table contains a series of Yes/No questions regarding escalation to stakeholders and governing bodies. Refer the Cyber Incident Response Plan for required escalations.

It is important to note that select fields may have their data changed over time as incident investigations and analysis continue. However, ensure that the relevant incident data in the record do not conflict with the data of the corresponding row in the incident tracker sheet.

4 Supporting Documentation

- Cyber Incident Response Plan.

5 Additional Comments

- **While the templates documented here and its sections remain the vital areas of answer and overrides other templates provided, it is important to also answer the questions posed by the Cyber Incident Response Plan whenever possible, especially using template for Incident Review and Post Analysis as seen in the Plan's templates.**
- **Legal and Governing bodies informed have select questions that the company security teams will need to answer and possess relevant evidence as detailed in the Cyber Incident Response Plans and other government regulations.**
- Google Forms is the current preferred platform for hosting incident collection form due to its flexibility in collection of required data. Microsoft Forms will require the Pro version.
- Incident Tags will likely be transferred to document metadata section or dropped.