SECURITY SOLUTIONS
RISK MANAGED SECURITY ASSURED

Security Solutions Security Incident Response Plan

Document Control:

Document Name	Security Incident Response Plan
Document Version	1.0
Author	Murale Belludi
Document Status	Reviewed and signed off
Last Update	Sep 2025
Last Review	Oct 2025
Next Review	Oct 2026
Document Classification	Internal - In-Confidence

Document History:

Version	Date	Author	Comments	Status
0.1	25-09-2025	Murale Belludi	Initial Draft - Derivative from Information Security Team, Policy and procedure	Draft
0.2	25-09-2025	Mathew Johnson	Peer review,	Draft
1.0	10-10-2025	Athar Awan	Release	Final

1 Introduction:

1.1 Purpose

This document describes the overall plan for responding to Security Solutions Services Information Security Incidents. It defines the roles and responsibilities of participants, characterization of incidents , relationships to other policies and procedures, and reporting requirements.

The goal of the Computer Security Incident Response Plan is to detect and react to computer security incidents, determine their scope and risk, respond appropriately to the incident, communicate the results and risk to all stakeholders, and reduce the likelihood of the incident from reoccurring.

1.2 Scope

This plan applies to Security Solutions Services and any person or device who gains access to these systems or data.

1.3 Maintenance

The Security Solutions Services Account Manager acts on behalf of the Security Solutions support team and will ask for cooperation and assistance from managers and employees as required. The Security Solutions Account Manager also works closely with Human Resources. Security Solutions Information Security Team and the legal team in investigations and e-discovery matters, and at their behest may assist Law Enforcement.

2 Definitions

2.1 Event

An event is an exception to the normal operation of IT Infrastructure, systems, or services. Not all events become incidents.

2.2 Incident

An incident is an event that, as assessed by Security Solutions Information Security staff, threatens the confidentiality, integrity, or availability of information Systems or Customer Data. Incidents may be established by review of a variety of sources including, but not limited to Security Solutions monitoring systems, reports from staff or outside organizations and service degradation or outages.

Incidents will be categorized according to potential for restricted data exposure or criticality of resource using a High–Medium–Low designation. The initial severity rating may be adjusted during plan execution. Detected vulnerabilities will not be classified as incidents.

The Security Solutions Support team employs tools to scan the environment and depending on the severity of found vulnerabilities may warn affected users, advice on the disconnection of affected machines will be communicated and the Security Solutions Account Manager will pursue available technology remedies to reduce that risk.

2.3 Personally Identifiable Information (PII)

For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first and last name in combination with one or more data elements that would allow for the identification of that person.

3 Roles and Responsibilities

The incident Response Process incorporates the Information Security Roles and Responsibilities definitions and extends or adds the following Roles.

3.1 Incident Response Manager

The Incident Response Coordinator is the Security Solutions Account Manager who is responsible for assembling all the data pertinent to an incident, communicating with appropriate parties. Ensuring that information is complete, and reporting on incident status both during and after the investigation. This can be transferred/delegated to Security Solutions Information Security Team on a case by case basis depending on the type of incident, scope and resources available.

3.2 Incident Response Management team

The Incident Response Management team comprises at least one representative of each of the following interest groups:

- Principal Consultant
- System Owner
- Legal team
- Human Resources
- Communication

Other interested parties as approved by the Board of Directors

3.3 Security Solutions Information Security Team (IST)

The Security Solutions Information Security Team is responsible for execution of the Incident response plan and in cases where there is a delegation of responsibilities the Incident response management.

3.4 Incident Response Handlers

Incident Response Handlers are employees of the Security Solutions or its subsidiaries, or outside contractors who gather, preserve and analyze evidence so that incidents can be brought to resolution.

3.5 Insider Threats

Insiders are current or former employees, contractors, or business partners who have access to an organization's restricted data and may use their access to threaten the confidentiality, integrity or availability of an organization's information or systems. This particular threat is defined because it requires special organizational and technical amendments to the Incident Response Plan as detailed below.

3.6 Law Enforcement

Law Enforcement includes the police, or other state law enforcement agencies, and government agencies that present warrants or subpoenas for the disclosure of information. Interactions with these groups will be coordinated with the legal team (see below)

3.7 Legal Team

Security Solutions legal team (external outsourced at this stage) is the liaison between the Security Solutions Account Manager and outside Law Enforcement, and will provide counsel on the extent and form of all disclosures to law enforcement and the public.

3.8 Officers

Officers are the staff designated for various regulatory frameworks to which Security Solutions and its subsidiaries are required to comply.

3.9 User

Users are employees of the client, Security Solutions and its subsidiaries or anyone accessing an information System, Data or company networks who may be affected by an incident.

4 Methodology

This plan outlines the most general tasks for Incident Response and will be supplemented by specific internal guidelines and procedures that describe the use of security tools and/or channels of communication. These internal guidelines and procedures are subject to amendment as technology changes. It is assumed that these guidelines will be documented in detail and kept up-to-date.

4.1 Evidence Preservation

The goal of Incident Response is to reduce and contain the scope of an incident and ensure that IT assets are returned to services as quickly as possible. Rapid response is balanced by the requirement to collect and preserve evidence in a manner consistent with the requirements of any rules and statutes pertaining to Civil Discovery, and abide by legal and Administrative requirements for documentation and chain of custody.

Security Solutions Information Security Manager will maintain and disseminate procedures to clarify specific activities in the Security Solutions Services Programme and other related departments with regard to evidence preservation, and will adjust those procedures as technologies change.

5 Service Level Agreements and Objectives

5.1 Governance

Security Solutions and its subsidiaries have Service Level agreements with the customers they serve. Interruption of service is a hardship and the Security Solutions Information Security team will cooperate with these groups to ensure that downtime is minimized. However, Security Solutions Information Security team management supports the priorities of investigation activities where there is significant risk, and this may result in temporary outages and interruptions.

5.2 Staffing for Incident Response Capability: Resiliency

The Security Solutions Account Manager will endeavour to maintain sufficient staffing and third-party augmentation to investigate each incident to completion and communicate its status to other parties while it monitors the tools that detect new events. Insufficient staffing will impact rapid response capability and resiliency, as will degradation of the tools used for detection, monitoring, and response.

5.3 Continuous Improvement:

The continuous improvement of incident handling processes implies that those processes are periodically reviewed, tested and translated into recommendations for enhancements. Staff inside and outside will be periodically trained on procedure for reporting and handling incidents to ensure that there is a consistent and appropriate response to incidents, and that post-incident findings are incorporated into procedural enhancements.

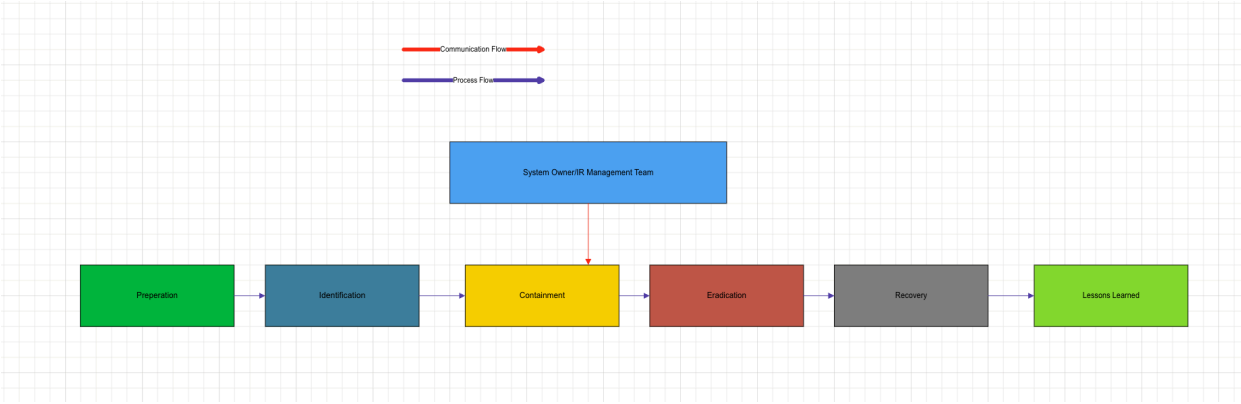
6 Incident Response Phases:

The basic incident response process encompasses six phases:

- Preparation,
- Identification
- Containment
- Eradication
- Recovery
- Lesson learned

The Security Solutions overall incident response process includes detection, containment, investigation, remediation and recovery, documented in specific procedures it maintains. This plan is the primary guide to the preparation phase from a governance perspective; local guidelines and procedures will allow the Security Solutions team to be ready to respond to any incident. Recovery includes re-evaluating whether the preparation or specific procedures used in each phase are appropriate and modifying them if inappropriate.

The dynamic relationship between those phases is highlighted in Figure 1.



6.1 Preparation

Preparation includes those activities that enable the ISO to respond to an incident:

- Policies
- Tools
- Procedures
- Effective governance
- And communication plan

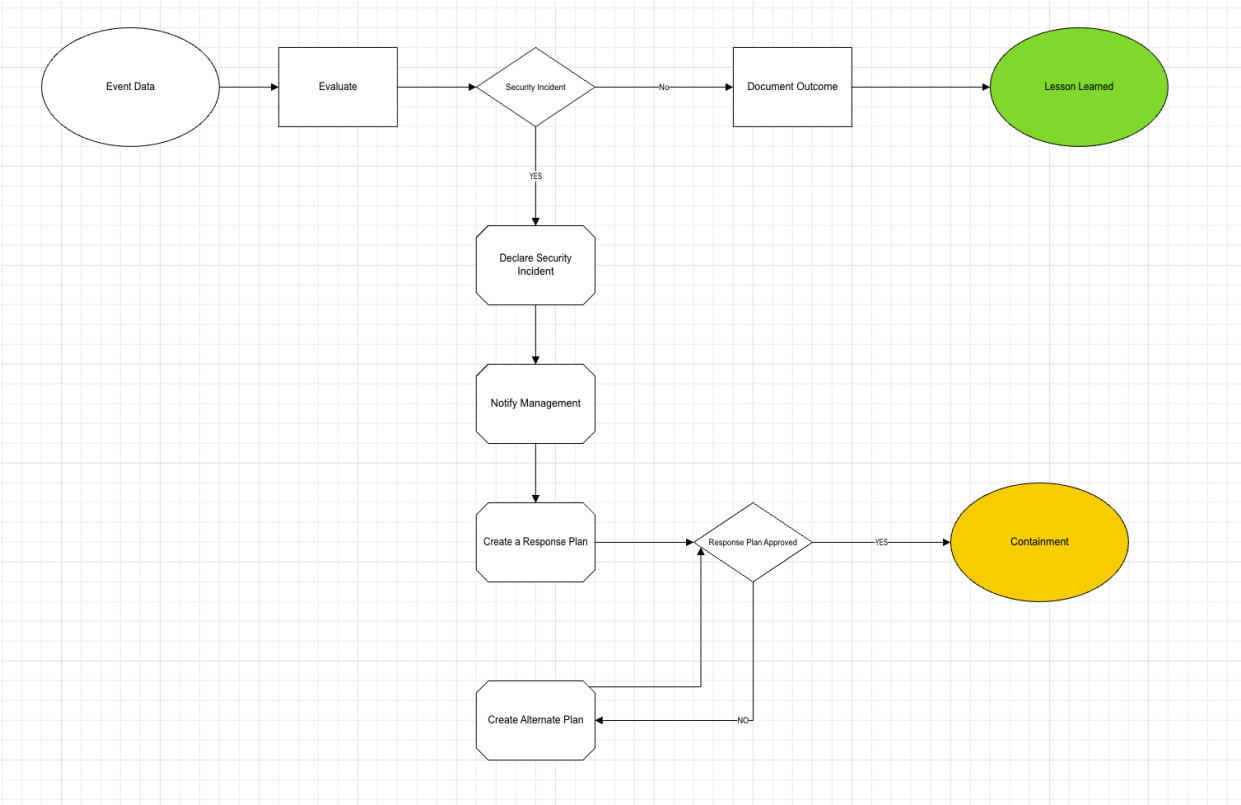
Preparation also implies that the affected groups have instituted the controls necessary to recover and continue operations after an incident is discovered. Post-mortem analysis from prior incidents should form the basis for continuous improvement of this stage.

6.2 Identification Phase:

An event triggers the discovery of the event either with security tools or notification by an internal or external party about a suspected incident. This phase includes the declaration and initial classification of the incident.
There are three phases involved in the identification phase:

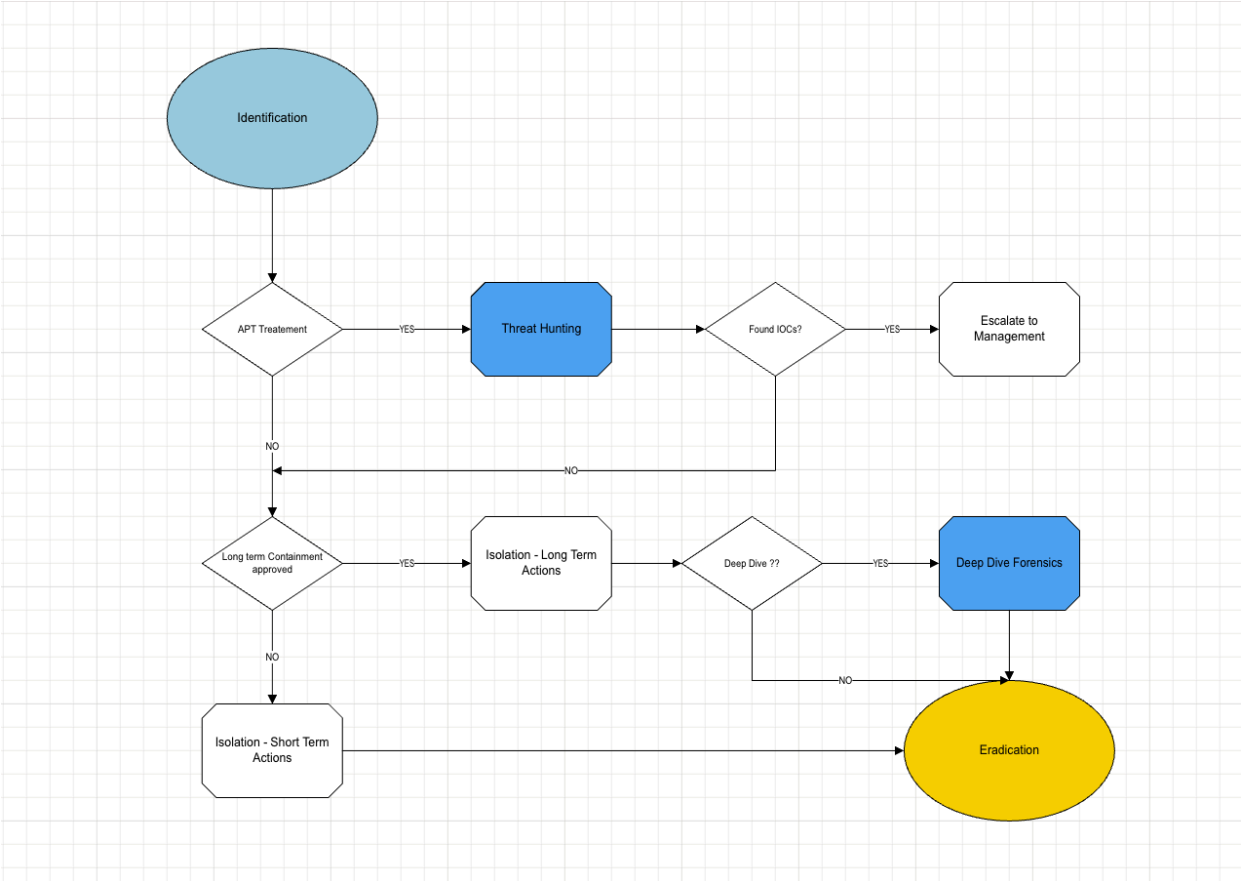
- Evaluation and Assessment
- Declare Incident
- Advise Response Plan

A detailed breakdown follows:



6.3 Containment Phase:

Containment Phase is the phase where the affected host or system is identified, isolated, or otherwise mitigated, when affected parties are notified and investigative status established.



6.4 Eradication:

Purpose: Completely remove the root cause of the incident and prevent re-infection or recurrence.

Key Actions:

1. **Root Cause Analysis (RCA):**
    - Identify the entry point (vulnerability, misconfiguration, compromised credential, phishing vector, etc.).
    - Validate findings with logs, forensic tools, or SIEM data.
2. **System Cleaning:**
    - Remove malicious code, unauthorized users, or persistence mechanisms (backdoors, scheduled tasks, registry changes).

- Patch vulnerabilities or misconfigurations that enabled the incident.

3. **Credential and Access Reset:**
    - Reset passwords, revoke tokens, re-issue certificates, and review privileged accounts.
    - Rotate API keys or encryption keys where applicable.
4. **Infrastructure Validation:**
    - Scan affected systems post-cleaning using EDR, antivirus, or vulnerability scanners.
    - Confirm malicious indicators no longer exist.
5. **Communication:**
    - Update stakeholders (management, legal, affected clients) that the threat is neutralized.
    - Document eradication evidence and actions in the incident record.

6.5 Recovery:

Purpose: Restore normal business operations safely and verify that systems are secure and fully functional.

Key Actions:

1. **System Restoration:**
    - Restore systems from clean backups verified as uncompromised.
    - Rebuild affected servers or environments if integrity is uncertain.
2. **Validation Testing:**
    - Conduct functional and security testing (vulnerability scans, pen test checks).
    - Confirm that patched systems are operational and stable.

3. **Monitoring Intensification:**
    - Increase log monitoring and SIEM alert sensitivity for a defined period (e.g., 30 days).
    - Watch for any signs of re-infection or related activity.
4. **User and Stakeholder Notification:**
    - If personal data or regulated data was affected, initiate **data breach notification** under the **Privacy Act 2020 (NZ)** or **Privacy Act 1988 (AU)**.
        - Notify affected individuals and regulators (e.g., OAIC or OPC NZ) as required by law.
        - Include what data was impacted, what has been done, and guidance for mitigation (e.g., credential changes).
5. **Return to Service:**
    - Formally sign off when systems meet operational and security acceptance criteria.

6.6 Lessons Learned:

Purpose: Capture insights to strengthen the organization's resilience and prevent recurrence.

Key Actions:

1. **Post-Incident Review:**
    - Conduct a formal "hot wash" or debrief with all involved teams within 1–2 weeks.
    - Document what went well, what failed, and what needs improvement.
2. **Root Cause Validation:**
    - Review the accuracy of initial analysis and confirm that corrective actions fully addressed the cause.
3. **Process & Policy Updates:**

- Update incident response playbooks, SOPs, and runbooks.
- Revise risk registers and security controls (patch management, IAM, etc.).

4. **Training & Awareness:**
    - Develop targeted awareness sessions or technical training based on incident type (e.g., phishing, privilege misuse).
5. **Metrics & Reporting:**
    - Include the incident in monthly or quarterly security reports.
    - Track key IR metrics: time to detect, time to contain, time to recover, and recurrence rate.

7. Customer Communication, Support and Regulatory Cooperation

7.1 Customer Support During an Incident

Security Solutions' Terms of Supply and Service Level Agreement (SLA) clearly define the level of support provided to Customers in the event of an information security incident.

- The Incident Response Team will coordinate with the affected Customer's designated contact to provide technical and communication support throughout the investigation and remediation phases.
- Support may include guidance on containment, access to system logs, evidence preservation assistance, and updates on remediation activities until resolution.

7.2 Customer Notification - **Security Breach Notifications**

- Security Solutions will promptly notify affected Customers upon detection or confirmation of any incident that may reasonably impact the confidentiality, integrity, or availability of Customer information or interconnected systems.
- Notifications will include a high-level description of the incident, its potential impact, and immediate containment or mitigation measures taken.

- Where applicable, Security Solutions will coordinate with the Customer's incident or privacy teams to align messaging and response.

7.3 Post-Incident Reporting

- Following closure of an incident, Security Solutions will prepare a **Post-Incident Report** summarizing:
    - Root cause and contributing factors
    - Systems and data affected
    - Corrective and preventive actions taken
    - Lessons learned and process improvements
- This report will be shared with affected Customers to enable them to assess residual risks and make informed decisions about continued use of the GRCLens service.

7.4 Cooperation with Regulatory and Industry Investigations

- Security Solutions will cooperate with any lawful investigation or inquiry by a regulatory body, including but not limited to the Office of the Privacy Commissioner, the Payment Card Industry Security Standards Council (PCI SSC), or other competent authorities.
- Upon request, Security Solutions will provide relevant technical and procedural documentation, logs, and evidence consistent with privacy and contractual obligations.
- Customers will be kept informed of interactions with such bodies where their data or systems are involved.

7.5 Liability, Insurance and Indemnity

- The Terms of Supply specify the limits of liability, indemnity provisions, and insurance coverage applicable to information security incidents.
- Security Solutions maintains appropriate cyber-risk insurance to mitigate potential financial impact resulting from incidents caused by verified vulnerabilities or operational failures within the GRCLens service.

- Compensation or service credits may be provided in accordance with the SLA and subject to the limitations described therein.