INCIDENT MANAGEMENT POLICY

DOCUMENT CONTROL PAGE

Document ID	SCG/IMP/019/1.0
Security Classification	Confidential
Date Issued	30-Jul-2025
Version	1.0
Project Name	NA
Author	AJ KHAN

VERSION HISTORY / CHANGE HISTORY

Version	Date Issued	Issued to	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

REVIEWERS

Version	Review Date	Reviewed By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

APPROVERS

Version	Date Approved	Approved By	Comments
0.1	30-Jul-2025		Issued for internal review
1.0	30-Jul-2025		Final version

DISTRIBUTION LIST

Date	Name / Distribution List	Comments
30-Jul-2025	Customer_DL_ABC	Published to Customer ABC

DOCUMENT CONTROL PAGE

RELATED DOCUMENTS

DOC_ID	DOC Version#	DOC Link	Comments
SCG/BASEINS/005/1.0			Base Template Instructions
SCG/PXF/008/1.0			Policy Exception Form
SCG/RXT/037/1.0			Risk Exception Template

CONFIDENTIALITY STATEMENT

This document is the exclusive property of [SecureCyberGates]. This document contains proprietary and confidential information. Duplication, Redistribution, or use, in whole or in part, in any form, requires consent of [SecureCyberGates].

[SecureCyberGates] may share this document with auditors under non-disclosure agreements [NDA] to demonstrate Security Audit requirement compliance.

Contents

1) Objective

Our Incident Response Policy serves as guidance for establishing and maintaining a capability to guide [SecureCyberGates] response when security-related incidents occur.
This Incident Response Policy establishes the standards that promotes fairness in maintaining an information security incident handling capability that includes adequate preparation, detection, analysis, containment, recovery and reporting activities.

2) Roles &Responsibilities

Roles	Responsibilities
CISO	Accountable - Overseeing the implementation and enforcement of this policy [Review and Approve this Policy]
IT/Security Team	1. Responsible for ensuring Incident management requirements are in place 2. Responsible for enforcing these Incident management requirements
BU Heads or Project Managers	Ensuring that employees under their supervision comply with this policy. [Review and Approve this Policy]
Employees / Contractors	1. Read this Policy 2. Ask questions /Provide Feedbacks 3. Report possible or actual violations of this Policy.

3) Scope

This Policy applies to anyone who conducts business for or on behalf of [SecureCyberGates] including:

- All employees
- Management and company owners
- External business partners who act on [SecureCyberGates]'s behalf or in our interest as Third Party Representatives

It is important to note that every situation may not be addressed in this Incident Management Policy; if you are unsure how [SecureCyberGates] standards or values apply in a given situation, please ask questions and seek further guidance from the Support and Security team.
Each and every one of us are responsible for ensuring that we follow these guidelines, and we will be held accountable for upholding our commitments to this Incident Management Policy.

4) Incident Response Operations

This SOP applies to all events in which a Employee/vendor/subcontractor are guided on how to respond to an incident across[SecureCyberGates] systems.

4.1) Objective

The organization develops, implements, and governs processes and documentation to facilitate the implementation of an enterprise-wide incident management policy, as well as associated standards, controls, and procedures.

4.2) Standard

[SecureCyberGates] is required to develop enterprise-wide incident response controls that at a minimum include:

- A formal, documented Incident Response Plan (IRP); and
- Processes to facilitate the implementation of the incident response processes and associated controls.

4.3) Guidelines

The objective is to ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

5) Incident Handling

5.1) Objective

The organization:

- Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.
- Coordinates incident handling activities with contingency planning activities; and
- Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training and testing / exercises and implements the resulting changes accordingly.

5.2) Standard

[SecureCyberGates] management and IT staff are required to:

a) Investigate notifications from detection systems;
b) Identify and assess the severity and classification of incidents;

c) Define appropriate actions to take in response to the incident; and
d) Respond with appropriate actions to minimize impact and ensure the continuation of business functions.

Organizations recognize that incident response capability is dependent on the capabilities of organizational systems and the mission / business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design and development of mission / business processes and systems. Incident-related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user / administrator reports and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission / business owners, system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices and the risk executive (function).

6) Incident Response Plan

6.1) Objective

The organization:

a) Develops an incident response plan that:
   - Provides [SecureCyberGates] with a roadmap for implementing its incident response capability;
   - Describes the structure and organization of the incident response capability;
   - Provides a high-level approach for how the incident response capability fits into the overall organization;
   - Meets the unique requirements of [SecureCyberGates] which relate to mission, size, structure, and functions;
   - Defines reportable incidents;
   - Provides metrics for measuring the incident response capability within [SecureCyberGates].
   - Defines the resources and management support needed to effectively maintain and mature an incident response capability; and
   - Is reviewed and approved by designated officials within [SecureCyberGates]
b) Distributes copies of the incident response plan to incident response personnel (identified by name and / or by role) and organizational elements;
c) Reviews the incident response plan on an organization-defined frequency;
d) Revises the incident response plan to address system / organizational changes or problems encountered during plan implementation, execution or testing; and
e) Communicates incident response plan changes to incident response personnel (identified by name and / or by role) and organizational elements. As needed, revise the risk profile to address necessary changes.

6.2) Standard

[SecureCyberGates] management and IT staff are required to establish processes and technical measures to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures. This includes, but is not limited to:

a) Be prepared to respond immediately to information security-related incidents;
b) Create the Incident Response Plan (IRP) to be implemented in the event of a system breach.
c) Test the IRP at least annually;
d) Designate specific personnel to be available on a 24 / 7 basis to respond to alerts;
e) Provide appropriate training to staff with security breach response responsibilities;
f) Include alerts from intrusion detection, intrusion prevention and file integrity monitoring systems;
g) Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments;
h) Ensure the plan addresses the following, at a minimum:
    - Roles, responsibilities, and communication and contact strategies in the event of a compromise;
    - Specific incident response procedures;
    - Business recovery and continuity procedures;
    - Data backup processes;
    - Analysis of legal requirements for reporting compromises;
    - Coverage and responses of al critical system components; and
    - Reference or inclusion of incident response procedures from legal or contractual sources, if applicable.;
i) Review Incident Response Plans (IRPs) at least once a year; and
j) Initiate corrective actions, as necessary.

6.3) Guidelines

It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational systems.

6.4) Risk Assessment

At least once per year or upon significant changes to the networks, [SecureCyberGates] is required to conduct a formal information security risk assessment for the enterprise that, at the very least, covers the following:

a) Identifies:
   I. Critical assets;
   II. Potential natural and man-made threats;
   III. Vulnerabilities;

b) Documents known vulnerabilities in a formal risk assessment;

c) Considers data governance:
   I. Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure;
   II. Compliance with defined retention periods and end-of-life disposal requirements; and
   III. Data classification and protection from unauthorized use, access, loss,
   IV. destruction, and falsification;

d) Assesses current controls affecting the confidentiality, integrity, and availability of critical data; and

e) Assesses current controls affecting safety-related risks for embedded technology.

For more details please refer Risk Management Policy , **Document ID : SCG/RMF/015/1.0**

6.5) Incident Detection and Response

Incidents are identified through a number of methods including:

- Customers Inform [SecureCyberGates] of Possible Attack.
- Discovery Suspicious Server Activity (High CPU usage, High Network usage, DDOS attack, strange software installs
- File Monitoring (Tripwire) or Intrusion Detection System or threat detection Triggers
- Alerts us or customer IT
- Failed Login Detection
- Alerts from SOC[Security Operation center] team

6.6) Incident Detection and Response

1) [SecureCyberGates] will assign security & technical lead to identify severity level (based on SLA) and coordinate efforts. Customer will be briefed once confirmed it is not a false alarm.

2) If there are cyber attacks, first level/network support will be assigned to block source IP(s) of attacks and other mitigation efforts.

3) Based on severity and how many software/network components are affected, a response team with the appropriate skills is assembled.

4) Response team will assess the nature of the incident, including point of compromise, determine mitigation/repair procedures and assess extent of any damage/compromise, and define a remediation checklist.

5) On confirmation of a breach, team will inform customer within 72 hours.

6) Apply relevant mitigations and fixes decided by response team.

7) Security review of other potential compromises or backdoors that might have been inserted by any cyber-attack (if any) and mitigation procedures.

8) Review by legal and relevant parties if any data privacy breaches have occurred.

9) Final test and review to ensure that all relevant holes and vulnerabilities discovered are closed and fixed.

6.7) Incident classification

Incidents will be classified into various types, including but not limited to:

- Data breaches
- Unauthorized access
- Malware infections
- Insider threats
- Ransomware attacks
- Advanced Persistent Threats (APTs)
- Zero-day vulnerabilities

6.8) Incident Response Team

Team	Description	Responsibilities
IT Team	Network and Hardware Infrastructure team	Manage firewall, network and infrastructure, block any intrusions, monitor and trace log files. Also, first responder for network issues.
Application Support	Software support team, in charge of 1 and 2nd level customer support.	First responder to threats and attacks if related to [SecureCyberGates] Software applications.
QRT [Quick Response	Emergency Response Team outside working	First responder to problem after working hours

Team]	hours.	
Legal	Legal team	Assess whether there are any legal and regulatory requirements for the incident Notifications will be made promptly and in accordance with applicable laws
Architect Team	Leaders team	Handles mission critical code patches. Also, for 3rd level customer support.
Security Team	Handles security reviews and attacks.	Discover if any security issue occurred, or if false positive. Coordinate actions with different teams for resolution. Planning for long term fixes.

7) Incident Reporting

7.1) Control Objective

The organization:

a) Requires personnel to report suspected security incidents to organizational incident response personnel within organization-defined time-periods; and
b) Reports security incident information to designated authorities.

7.2) Standard

For actual or suspected information security incidents:

a) Users are responsible for reporting system weaknesses, deficiencies, and / or vulnerabilities through appropriate management channels as quickly as possible;
b) Information security events should be reported through appropriate management channels as quickly as possible; and
c) If a breach occurs, breach notification procedures must occur without unreasonable delay, except:
    - When a law enforcement agency has determined that notification wil impede a criminal investigation; or
    - In order to discover the complete scope of the breach and restore the integrity of the system.

7.3) Guidelines

The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for regulatory agencies. The types of security incidents reported, the content and timeliness of the reports and the designated reporting authorities reflect applicable laws, policies, regulations, standards, and guidance. Good faith acquisition of PII by an authorized user or authorized agent for [SecureCyberGates] purposes does not constitute a security breach, provided that the PII is not used or subject to further unauthorized disclosure

8) Incident Monitoring and Tracking

8.1) Control Objective

The organization documents, monitors and reports information security and privacy incidents.

8.2) Standard

Mechanisms shall be put in place to monitor for information security incidents. This includes, but is not limited to monitoring:

a) Aggregating and correlating event data multiple sources and sensors; and
b) Helpdesk / service desk incidents.

8.3) Guidelines

Documenting system security incidents includes, for example, maintaining records about each incident, the status of the incident and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring and user / administrator reports. All Incidents should be logged in [JIRA] application.

9) Root Cause Analysis and Lessons Learned

Incident response personnel are required to:

a) Perform a Root Cause Analysis following events that trigger usage of the Incident Response Team ; and
b) Incorporate lessons learned in updates to Incident Response Plans.

10) Employee Training and Awareness

10.1) All [SecureCyberGates] employees SHOULD undergo training and assessment on this policy during their initial induction [Onboarding].

10.2) Security team to conduct periodic trainings **ATLEAST ONCE** a year.

11) Compliance and Monitoring

11.1) Compliance with this policy is **MANDATORY**. Employees violating this policy will be subject to disciplinary action up to and including termination.

11.2) Third-party users, contractors, and vendors who **FAIL** to comply with this policy may

have their access to [SecureCyberGates]systems , Application and networks revoked or suspended until compliance is achieved. Repeated or severe violations may result in the termination of their contracts or business relationships with [SecureCyberGates].

11.3) Periodic Audits and Assessments : [SecureCyberGates]'s IT department, in collaboration with the Information Security team, will conduct periodic audits and assessments to evaluate compliance with this security policy.

12) Escalation Matrix

12.1) In case of any policy violations issues, the following escalation structure shall be followed to ensure timely resolution and appropriate accountability:

Level	Role	Contact
Level 1	Team Lead /Reporting Manager	First-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 2	Group Manager / Senior Managers	Second-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]
Level 3	CISO	Final-level escalation: Email / Any Ticketing Tool [info@securecybergates.com]

12.2) Employee SHOULD provide sufficient evidences and details , Clear description of the issue.

12.3) Security team to define issue severity and proper SLA for issue resolution as per severity.

13) Policy Exceptions

13.1) There may be requirements where Employee needs policy exception for legitimate reasons, In such cases, employee should follow POLICY EXCEPTIONS template and approval process. **[Kindly refer Policy exception form [Document ID SCG/PXF/008/1.0]]**

14) Policy Review and Updates

14.1) This policy shall be periodically reviewed **[Atleast Once in a YEAR]**and updated to ensure its effectiveness, relevance, and alignment with [SecureCyberGates]objectives,legal requirements and industry best practices.

14.2) Feedback from employees, stakeholders, and external audits shall be solicited and considered for continuous improvement of the policy and associated procedures.

14.3) Regular audits and inspections shall be conducted to assess compliance with this policy and associated procedures, with non-conformances addressed through corrective actions and preventive measures.

14.4) Any updates or revisions to this policy will be communicated to all employees and relevant stakeholders through appropriate channels. Employees are responsible for familiarizing themselves with the latest version of the policy and adhering to its requirements.

15) Conclusion

By implementing and adhering to this comprehensive Incident Management policy, [SecureCyberGates]aims to resolve incident ASAP and protect its sensitive information, intellectual property, and critical systems from unauthorized access and data breaches. This policy aligns with industry best practices and incorporates robust requirements for password construction, protection, management, and system development standards.

SECURE CYBER GATES

THANKYOU!
FOR CYBER-SECURITY RELATED UPDATES, KINDLY FOLLOW BELOW PAGES...

https://www.linkedin.com/in/aj57/
https://www.linkedin.com/company/securecybergates
https://securecybergates.com/services
https://www.youtube.com/@SecureCyberGates
https://hackerone.com/crypto-khan
https://x.com/securecybergate
securecybergates@gmail.com

SECURE CYBER GATES