




Incident Management Policy

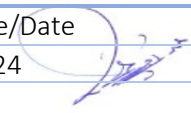
Doc. Control Number	Version
SNL-20	1.0



Document Reference

Item	Description
Title	Incident Management Policy
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	31 March 2024
Revision-Date	31 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	31/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	31/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	31/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	19 August 21	Muhaned Ali	First Release
0.2	19 August 22	Muhaned Ali	Updated and converted to a new format
0.3	31 May 2023	Muhaned Ali	The policy has been reviewed
1.0	31 March 2024	Muhaned Ali	The policy has been reviewed



Contents

1. Overview	4
2. Purpose	4
3. Scope.....	4
4. Policy.....	4
5. Information Security Incident Identification.....	5
6. Information Security Incident Reporting	5
7. Incident Response Training.....	5
9. Approval.....	6
Appendix A - Cybersecurity Incident Response Instructions	6

1. Overview

Incident Management policy shall enable the response to a major incident or disaster by implementing a plan to restore the critical business functions of SNLC. The number of computer security incidents and the resulting cost of business disruption and service restoration rise with the increase in dependence on IT-enabled processes. Implementation of sound security policies, blocking of unnecessary access to networks and computers, improvement in user security awareness, and early detection and mitigation of security incidents are some of the actions that can be taken to reduce such risks and decrease the cost of security incidents.

2. Purpose

The purpose of the incident management policy is to provide organization-wide guidance to employees on the proper response to, and efficient and timely reporting of, computer security-related incidents, such as computer viruses, unauthorized user activity, and suspected compromise of data. It also addresses non-IT incidents such as power failure. Further, this policy provides guidance regarding the need for developing and maintaining an incident management process within SNLC.

3. Scope

This policy applies to all SNL Employees, Contractors, and Third-Party Employees, who use, process, and manage information from individual systems or servers.

4. Policy

4.1 Incident Reporting

- a) Any information security compromise, attempt to compromise, presence of security vulnerability, violation of security policies, or unauthorized access of data, shall be reported to Infosec immediately upon detection and the same shall be responded to by SNL Infosec as per this policy.
- b) All employees and authorized users are required to report any suspected or confirmed cybersecurity incidents immediately to the designated incident response team or contact.

4.2 Incident Classification

- a) Incidents will be classified based on their severity and potential impact on the organization's confidentiality, integrity, and availability of information assets.

4.3 Incident Response Plan

- a) Develop and maintain a comprehensive incident response plan that outlines the roles and responsibilities of the incident response team, communication channels, escalation procedures, and incident containment strategies.

4.4 Incident Detection and Assessment

- a) Implement monitoring mechanisms to detect and identify potential cybersecurity incidents in real-time.
- b) Conduct thorough assessments to determine the nature and scope of the incident, as well as the potential impact on the company.

4.5 Incident Containment and Mitigation

- a) Take immediate action to contain and mitigate the impact of the incident to prevent further harm and data loss.
- b) Engage relevant technical experts and stakeholders to assist in the containment and mitigation efforts.

4.6 Incident Communication

- a) Establish clear communication channels for reporting and disseminating information about incidents to relevant stakeholders, including internal teams, management, legal, and regulatory authorities, as required.

4.7 Incident Investigation and Analysis

- a) Conduct a thorough investigation to understand the root cause of the incident and identify any vulnerabilities or weaknesses in the company's security controls.

4.8 Incident Documentation

- a) Maintain detailed records of all incidents, including their timeline, actions taken, lessons learned, and recommendations for improvements.
- b) Incident management policy and plan must be documented, maintained, and communicated to management and appropriate team members.
- c) SNLC must track, classify, and document all cybersecurity Incidents.

4.9 Coordination with Authorities

- a) Cooperate with law enforcement agencies and regulatory authorities when required by law or regulatory obligations.

4.10 Incident Recovery and Lessons Learned

- a) Develop and implement strategies for restoring affected systems and services to normal operations.
- b) Conduct a post-incident analysis to identify lessons learned and areas for improvement in the incident response process.

5. Information Security Incident Identification

An Information Security Incident is any event that threatens or has the potential to adversely affect the Confidentiality Integrity or Availability, of the information systems/services, of SNLC. Some of the examples of Information Security Incidents include but are not limited to the following:

- a) Unauthorized access or modification of Data or network or systems or services or programs.
- b) Loss or Theft of equipment on which data is stored (Ex: Hard Disk, Removable Media, Servers... etc.).
- c) Denial of Service (DoS) or Distributed Denial of Service (DDoS).
- d) Violation of SNLC policies, processes, and guidelines.
- e) Social Engineering (Ex: Phishing, Spam, Spoofing ...etc.)
- f) Ransomware Infection.
- g) Malware/Virus/Trojan/Worm.
- h) Data Exfiltration (Unauthorized Copying/Transferring of data to external network/internet).
- i) Disclosure of sensitive data in the public domain.

6. Information Security Incident Reporting

- a) If any user detects or observes any of the Information Security incidents mentioned in Section 5, of this Policy. Then the same shall be reported by him/her, to SNL Infosec immediately.
- b) Notify SAUDI ARAMCO, CST within twenty-four (24) hours of discovering the Incident.
- c) Follow the Cybersecurity Incident Response Instructions set forth in Appendix A.

7. Incident Response Training

- a) Conduct regular training to test the Incident Response process for its effectiveness (e.g., testing communication channels, response times).
- b) Evaluate the response of the team members to determine if they followed the incident response process. Assess the effectiveness of the communication channels, response times, and other aspects of the process.
- c) Monthly incident response training is required.

8. Policy Review

- a) This policy will be reviewed on a periodic basis to ensure its continued relevance and effectiveness. Any updates or modifications to this policy shall be communicated to all relevant employees and stakeholders.

9. Approval

Entity	Name	Signature	Date
V.P	Abdullah Al Shuhail		31/3/2024

Appendix A - Cybersecurity Incident Response Instructions



1. Notify

- Notify Saudi Aramco, and CST of the Incident
 - Initial Notification of Incident: The Company must notify Saudi Aramco, CST Security Operations Center (SOC) within twenty-four (24) hours of discovering any Incident.
 - All notifications must be communicated to SOC via the Saudi Aramco Security Hotline at: +966 (13)-880-0000, CST at 0114619999.
 - Subsequent Notification of Incident: After the Initial Notification of the Incident, the Company must notify Saudi Aramco, and CST of all Incidents stemming from the initial Incident via the communication method agreed by SOC during the initial notification.

2. Review and Identify

- Immediately review all recent changes and modifications to information system users and access privileges for unauthorized modifications.
- Conduct a thorough review of the Company's information systems for evidence of compromise.

3. Reset Affected Passwords

- Immediately change every password on information systems that are compromised or suspected to be compromised due to the Incident.

4. Report (Interim)

- Provide Saudi Aramco and CST with reports detailing the Incident. The Company must communicate its ongoing efforts to mitigate and resolve the Incident every twenty-four (24) hours until the time of Incident resolution. The Incident must be classified according to the below classification:

Severity	Description
Low	<p>Incident that:</p> <ul style="list-style-type: none"> • Adversely impacts a very small number of systems or individuals. • Disrupts a very small number of network devices or segments. • Has little or no risk of propagation or causes only minimal.
Medium	<p>Incident that:</p> <ul style="list-style-type: none"> • Adversely impacts a moderate number of systems and/or people. • Adversely impacts a non-critical organization system or service. • Adversely impacts a business unit system or service.
High	<p>Incident that:</p> <ul style="list-style-type: none"> • Threatens to have a significant adverse impact on many systems and/or people. • Poses a potentially large financial risk or legal liability to the organization. • Threatens the confidentiality of data. • Adversely impacts an organization system or service critical to the operation of a major portion of Saudi Aramco. • Has a high probability of propagating to many systems and causing significant damage or disruption?

5. Examine and Analyze

Upon request by Saudi Aramco and CST, provide access to information or equipment associated with the reported Incident for the purpose of conducting a forensic analysis. This includes but is not limited to hard disk drives, volatile memory dumps, and logs.

6. Investigate

Submit (or provide access) to Saudi Aramco SOC, and CST, any malicious software/program, supporting binaries, and files associated with the Incident for forensic analysis purposes. The suitable submission method will be defined by Saudi Aramco and CST upon receiving the first Interim Status Report.

7. Report (Final)

The company will provide two Final Reports of the Incident:

- Business Report: High-level report for Top Management within three (3) business days of resolution or a determination that the problem cannot be resolved within such time. Copy to Saudi Aramco and CST.
- Technical Report: detailed report for Saudi Aramco and CST cybersecurity team within ten (10) business days of resolution or a determination that the problem cannot be resolved within such time.

8. Preserve

- Preserve images of all known affected information systems for at least ninety (90) days from the submission of the Final Report.