Logging and Monitoring Policy

Doc. Control Number	Version
SNL-45	0.2

Document Reference

Item	Description
Title	Logging and Monitoring Policy
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	28 May 2024
Revision-Date	28 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/28/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/28/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/28/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	28 May 2023	Muhaned Ali	First Release
0.2	28 May 2024	Muhaned Ali	The policy has been reviewed

Contents

1. Purpose

This policy establishes the framework for logging and monitoring activities within SNLC. The objective of this policy is to ensure the consistent collection, analysis, and retention of logs from various systems and assets to detect and respond to security incidents, anomalies, and unauthorized activities. This policy outlines the importance of logging and monitoring, the requirements for implementing an effective logging and monitoring system, and the responsibilities of relevant stakeholders.

2. Scope

This policy applies to all information systems, assets, networks, and services within SNLC that generate logs.

3. Policy

3.1 Log Collection and Retention

a) Implement logging mechanisms to capture relevant events, including user activities, system events, security incidents, and configuration changes.

b) Establish clear retention periods for logs based on regulatory requirements, industry best practices, and the company's needs.

3.2 Log Analysis and Review

a) Routinely analyze logs to identify abnormal patterns, anomalies, unauthorized access, and potential security breaches.

b) Conduct regular reviews of logs to ensure the accuracy and completeness of recorded events.

c) Privileged accounts activity must be logged and monitored on a regular basis.

3.3 Log Access and Protection

a) Define access controls to ensure that only authorized personnel have access to log data.

3.4 Incident Detection and Response

b) Implement automated alerting mechanisms to notify the incident response team of critical events, security incidents, and anomalies.

c) Establish procedures for analyzing and responding to alerts in a timely manner.

3.5 Log Integrity and Authentication

a) Implement measures to ensure the integrity of logs, including digital signatures, cryptographic hashes, and secure storage.

b) Authenticate log sources to prevent unauthorized systems from injecting or altering log data.

3.6 Log Archiving and Backup

a) Maintain secure and reliable archives of logs to support forensic analysis, investigations, and compliance requirements.

b) SNLC must retain all audit logs from information systems and applications storing, processing, or transmitting Saudi Aramco data for one (1) year.

c) Regularly back up log data to prevent data loss in case of system failures.

3.7 Log Monitoring Tools

a) SNLC must monitor technology assets, systems, and applications to identify unauthorized access, or unauthorized activity.

b) Utilize appropriate log management and monitoring tools to centralize log collection, analysis, and visualization.

c) SNLC must periodically aggregate and correlate data from multiple systems and critical applications such as Firewalls, IDS/IPS, and anti-virus in a central repository for event monitoring and analysis purposes.

d) The SIEM solution utilized at SNLC is Wazuh.

3.8 Compliance and Auditing

a) Use logs to meet regulatory compliance requirements and support internal and external audits.

4. Policy Review

4.1 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.

SNLC Cybersecurity Standard Appendix A

Information Systems must be capable of auditing the events listed below.

No.	Event Type
1	System starts
2	System shutdown
3	System restart
4	Successful login attempts (Logon Types must be included)
5	Failed login attempts
6	Service creation
7	Additon of user account
8	Deletion of user account
9	Escalation/modification of account privileges
10	Modification of security configuration/policies
11	Deletion of user accounts
12	Activities of privileged accounts
13	Logs cleared
14	Attempt/Failure to access removable storage
15	Session connected, reconnected, and disconnected
16	Plug and Play driver install attempted (System Log)
17	Encryption keys access

No.	Event Attributes
1	Timestamp
2	User ID
3	Event name
4	Event category
5	Event severity
6	Host name
7	Source IP address
8	Destination IP address
9	Source Port
10	Destination Port