



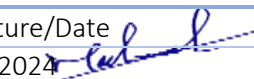
Cybersecurity Audit Policy


Doc. Control Number	Version
SNL-49	0.2



Document Reference

Item	Description
Title	Cybersecurity Audit Policy
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	16 July 2024
Revision-Date	16 July 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	7/16/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	7/16/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	7/16/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	16 July 2023	Muhaned Ali	First Release
0.2	16 July 2024	Muhaned Ali	The policy has been reviewed



Contents

1. Overview	4
2. Scope.....	4
3. Policy	4
4. Review and Revision	4
5. Policy Compliance	4



1. Overview

This policy establishes the guidelines and procedures for conducting independent and periodical cybersecurity audits to ensure the protection of critical systems and data within the organization. It outlines the requirements for the protection and retention of audit records and mandates reporting to top management.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who have access to the SNLC's critical systems and data.

3. Policy

3.1 Independent and Periodical Audits

- a) The company shall conduct independent and periodical cybersecurity audits to assess the effectiveness of its security controls, identify vulnerabilities, and ensure compliance with relevant cybersecurity standards, laws, and regulations.
- b) The frequency of audits shall be determined based on the criticality of the systems, risk assessment, and applicable legal or regulatory requirements.
- c) Critical systems, including those holding sensitive data or supporting critical business operations, shall be audited at least once a year.

3.2 Protection and Retention of Audit Records

- a) Audit records, including findings, recommendations, and supporting evidence, shall be securely stored to maintain their integrity, confidentiality, and availability.
- b) The company shall define and implement appropriate access controls to ensure that only authorized personnel can access audit records.
- c) Audit records shall be retained for a minimum period of 5 years to comply with legal, regulatory, and contractual requirements.
- d) The company shall regularly back up audit records to prevent data loss and implement appropriate disaster recovery measures.

3.3 Reporting to Top Management

- a) The results of cybersecurity audits, including significant findings, recommendations, and remediation plans, shall be reported to top management.
- b) The reporting shall include an executive summary that provides a concise overview of the audit outcomes and highlights critical security risks.
- c) Top management shall be promptly notified of any high-severity vulnerabilities or breaches discovered during audits, enabling timely actions to mitigate risks and minimize potential damage.
- d) The company shall establish a mechanism for top management to review and approve the remediation plans resulting from cybersecurity audits.

3.4 Compliance

- a) All employees, contractors, and third-party vendors shall comply with this policy.
- b) The company's cybersecurity team or designated personnel shall oversee the implementation and enforcement of this policy.

4. Review and Revision

- 4.1 This policy shall be reviewed at least once a year or as deemed necessary by the company's cybersecurity team to ensure its relevance and effectiveness. Any proposed revisions shall be submitted for approval before implementation.

5. Policy Compliance

- 5.1 All employees, contractors, and third-party vendors shall comply with this policy.
- 5.2 The company's cybersecurity team or designated personnel shall oversee the implementation and enforcement of this policy.



5.3 Non-compliance with this policy may result in disciplinary action, including termination of employment or contract.