




Cybersecurity Metrics Procedure


Doc. Control Number	Version
SNL-74	0.2

Document Reference



Item	Description
Title	Cybersecurity Metrics Procedure
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	10 December 2023
Revision-Date	10 December 2024

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	10/12/2023 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	10/12/2023 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	10/12/2023 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	Dec 2023	Muhaned Ali	First Release
0.2	11 Aug 2024	Muhaned Ali	The document has been reviewed



Contents

1. Objective	4
2. Scope.....	4
3. Roles and Responsibilities.....	4
4. Key Performance Indicators (KPIs).....	4
5. Measurement Metrics	4
6. Policy Compliance Rate Metrics.....	4
7. Timeliness of Updates Metrics.....	4
8. Measurement Frequency.....	4
9. Data Sources	4
10. Measurement Process.....	4
11. Continuous Improvement	5
12. Communication	5
13. Review and Audit.....	5
14. Version Control.....	5

1. Objective

The objective of this procedure is to establish a systematic approach for continuously measuring, reviewing, and updating cybersecurity policies in response to changes in policies within the SNL.

2. Scope

This procedure covers all cybersecurity policies within the SNL.

3. Roles and Responsibilities

3.1 Cybersecurity Team:

- a) Define and implement measurement strategies.
- b) Continuously review the effectiveness of cybersecurity policies.

3.2 Policy Owners:

- a) Collaborate with the Cybersecurity Team to ensure policies are up to date.
- b) Communicate changes in policies to relevant stakeholders.

4. Key Performance Indicators (KPIs)

Identify and document key performance indicators (KPIs) related to the continuous measurement and review of cybersecurity policies:

4.1 Policy Compliance Rate: Percentage of policies aligned with the latest version.

4.2 Timeliness of Updates: Average time taken to update policies in response to changes.

5. Measurement Metrics

- a) Select specific metrics under each KPI category, considering relevance, measurability, and alignment with organizational goals.

6. Policy Compliance Rate Metrics

6.1 Regular Audits: GRC must conduct an annual audit in accordance with regulatory requirements.

6.2 Number of Non-Compliance Issues: GRC team must identify, and track issues discovered during audits.

7. Timeliness of Updates Metrics

7.1 Update Cycle Time: The GRC team must annually update and review policies, procedures, standards, and guidelines.

7.2 Adherence to Policy Changes: Percentage of policies updated in response to changes.

8. Measurement Frequency

- a) The GRC Team must ensure that measurement frequency and reporting is done quarterly.
- b) The GRC Team must submit the Cybersecurity Metrics sheet to the head of the Cybersecurity Manager quarterly.

9. Data Sources

- a) The GRC Team must identify and document sources of data for each metric, such as policy documentation, audit reports, and change notifications.

10. Measurement Process

10.1 Data Collection

- a) The GRC Team will collect data on policy compliance, timeliness, and adherence to policy changes on a regular basis.
- b) Collaborate with policy owners to gather relevant information.

10.2 Analysis

- a) GRC team must analyze collected data to identify trends, patterns, and areas for improvement.
- b) GRC team must identify root causes of non-compliance issues, delays in updates, and challenges in adhering to policy changes.

10.3 Reporting

- a) The GRC Team must prepare regular reports on policy compliance, update timelines, and adherence to policy changes.
- b) The GRC Team must present their findings to relevant stakeholders, including management and policy owners.



11. Continuous Improvement

- a) The GRC Team must establish a feedback loop for continuous review and improvement of the Cybersecurity Metrics Process. The GRC Team must periodically reassess and adjust metrics based on evolving organizational needs and the threat landscape.

12. Communication

- a) The GRC Team must regularly communicate measurement results to relevant stakeholders, fostering awareness and accountability.

13. Review and Audit

- a) The GRC Team must Conduct regular internal reviews of the measurement process. Consider external audits to validate the effectiveness and accuracy of the measurement process.

14. Version Control

- a) The GRC team must maintain version control for this procedure and other documents to track changes and updates.