




HR Information Security Policy

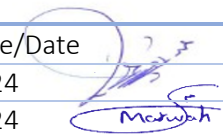
Doc. Control Number	Version
SNL-08	1.0



Document Reference

Item	Description
Title	HR Information Security Policy
Department	Cybersecurity department
Version No	1.0
Status	Draft
Type	DOCX
Publish-Date	5 March 2024
Revision-Date	5 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/3/2024 
Marwah Alsubaiei	HR Department	5/3/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/3/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	13 Jan 2021	Muhaned Ali	First Release
0.2	2 Aug 2022	Muhaned Ali	Policy Update
0.3	11 May 2023	Muhaned Ali	The transfer section has been added.
1.0	5 March 2024	Muhaned Ali	Policy has been reviewed



Contents

1. Overview	4
2. Purpose	4
3. Scope.....	4
4. Policy.....	4
5. Roles and Responsibilities.....	5
6. Policy Compliance	5

1. Overview

SNL holds great amounts of RESTRICTED information. Information security is very important to help protect the interests and confidentiality of SNL and its interested parties. It cannot be achieved by technical means alone and must also be enforced and applied by people, and this policy addresses the same along with Human Resources being the primary objective.

2. Purpose

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards to ensure that cybersecurity risks and requirements related to employees and contractors in the company are effectively addressed before, during, and upon completion/termination of their employment.

3. Scope

This policy covers all systems relating to SNL and applies to all SNL employees.

4. Policy

- 4.1 Cybersecurity requirements for employees must be defined.
- 4.2 Jobs related to sensitive systems in the SNLC must be filled by competent citizens.
- 4.3 HR cybersecurity controls must be implemented during the employee lifecycle in SNL which includes the following stages:
 - a) Prior to Employment.
 - b) During the working period.
 - c) Upon completion/termination of their employment.
- 4.4 SNL personnel must understand and agree to their job roles, terms, and responsibilities related to cybersecurity.
- 4.5 Cybersecurity responsibilities and a Non-Disclosure Agreement must be included in SNL employee contracts (to include during and after completion/termination of their employment relationship with SNL).
- 4.6 Violations related to cybersecurity should be listed on SNL's Human Resources Violations List.
- 4.7 Access to employee information without prior permission is prohibited.
- 4.8 A Performance Measurement Indicator (KPI) should be used to ensure the continuous development of cybersecurity requirements related to human resources.
- 4.9 Prior to Employment
 - a) HR and IT must use the SNL onboarding form.
 - b) Employees must pledge to comply with cybersecurity policies before granting them access to SNL systems.
 - c) The roles and responsibilities of employees must be defined, considering the application of the principle of non-conflict of interest.
 - d) Employee roles and responsibilities related to cyber security should be specified in the job description.
 - e) Cybersecurity roles and responsibilities should include:
 - Protect all SNL assets from unauthorized access or vandalism.
 - Implement all required activities related to cybersecurity.
 - Commit to SNL's cybersecurity policies and standards.
 - Commit to a program to raise awareness of cybersecurity risks.
 - f) A security screening should be conducted for employees in cybersecurity jobs, technical jobs with critical and sensitive powers, and jobs related to sensitive systems.
- 4.10 During the working period
 - a) An awareness program must be presented, related to raising the level of awareness of cybersecurity, including cybersecurity policies and standards, periodically.

- b) The Human Resources Department shall inform the relevant departments of any change in the employees' roles or responsibilities to take the necessary measures related to revoking or modifying the access permissions.
 - c) Ensure that the cybersecurity requirements of human resources are implemented.
 - d) The extent of cybersecurity commitment should be included in the aspects of employee evaluation.
 - e) Ensure that the need-to-know principle is applied in the assignment of tasks.
- 4.11 Upon completion/termination of their work.
- a) Procedures for employment completion or employment termination must be defined in a manner that covers cybersecurity requirements.
 - b) The Human Resources Department must inform the relevant parties if the date of the completion or termination of the job relationship approaches, to take the necessary measures.
 - c) Ensure that all SNLC assets are returned, and access revoked for employees on their last working day and before they receive the necessary clearances.
 - d) Responsibilities and duties that will remain in effect after SNLC personnel terminate service shall be specified, including the confidentiality agreement, provided that such responsibilities and duties shall be included in all personnel contracts.
- 4.12 Internal transfer to other position
- a) If a person must transfer from one position to another, they should follow SNL procedures, complete the internal transfer form, and submit it to HR.

5. Roles and Responsibilities

- 5.1 The sponsor and owner of the policy document: Head of Cyber Security Department.
- 5.2 Policy reviews and update: Cyber Security Department.
- 5.3 Policy implementation: HR Department

6. Policy Compliance

6.1 Compliance Measurement

The Infosec team will verify compliance with this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

6.2 Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

6.3 Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.