



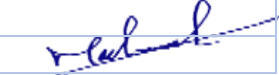
# Cybersecurity Roles and Responsibilities


Doc. Control Number	Version
SNL-29	0.2



### Document Reference

Item	Description
Title	Cybersecurity Roles and Responsibilities
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	23 May 2024
Revision-Date	23 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/23/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/26/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/26/2024 

### Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	23 May	Muhaned Ali	First Release
0.2	23 May 2024	Muhaned Ali	The document has been reviewed

## 1- Roles and Responsibilities

The following outlines specific organizational roles and their respective responsibilities. Clearly defined roles and responsibilities help the organization, and its employees work more efficiently by designating who is responsible for performing certain tasks.

### 1.1 Boards of Directors/Senior Management

The Board of Directors is ultimately responsible for information security. Senior Management is responsible for understanding risks to the Company to ensure that they are adequately addressed from a governance perspective. It is reported that the effectiveness of information security governance is dependent on the involvement of the Board/senior management in approving policy and appropriate monitoring of the information security function.

The major role of top management involves implementing the Board approved information security policy, establishing necessary organizational processes for information security, and providing necessary resources for successful information security.

### 1.2 Chief Executive Officer (CEO)

The Chief Executive Officer is the highest-level senior official or executive in an organization with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations assets, individuals, other organizations, and the Nation that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained.

Responsibilities include, but are not limited to:

- Ensuring the integration of information security management processes with strategic and operational planning processes.
- Making sure that the information and systems used to support organizational operations have proper information security safeguards; and
- Confirm that trained personnel are complying with related information security legislation, policies, directives, instructions, standards, and guidelines.

### 1.3 Cyber Security Committee

Since information security affects all aspects of the company, to consider information security from an SNLC-wide perspective a steering committee of executives should be formed with formal terms of reference. The Chief Information Security Officer would be the member secretary of the Committee. The committee may include, among others, the Chief Executive Officer (CEO) or designee, Director of business development and project, Director of managed services, CFO, Chief Information Officer (CIO)/IT Head, HR.

Responsibilities include, but are not limited to:

- Providing a clear direction and leadership on the company's InfoSec strategies in managing information security.
- Ensuring that information security policies and objectives are implemented accordingly.
- Risk management: setting the tone by defining the risk appetite and supporting the risk treatment plan.

- Ensuring that adequate steps are taken regularly to improve the information security of the company.
- Conducting management review.
- Ensuring that continual improvements are addressed promptly and without delay.
- Demonstrating commitment to supporting top management to achieve the company's strategic goals.
- Direct reporting to top management.

#### 1.4 System Security Engineer

The System Security Engineer is an individual, group, or organization responsible for conducting system security engineering activities.

Responsibilities include, but are not limited to:

- Designing and developing organizational systems or upgrading legacy systems; and
- Coordinating security-related activities with information security architects, senior agency information security officers, system owners, common control providers, and system security officers.

#### 1.5 System Administrator

The System Administrator is an individual, group, or organization responsible for setting up and maintaining a system or specific components of a system.

Responsibilities include, but are not limited to:

- Installing, configuring, and updating hardware and software.
- Establishing and managing user accounts.
- Overseeing backup and recovery tasks; and
- Implementing technical security controls.

#### 1.6 Users

The User is an individual, group, or organization granted access to organizational information to perform assigned duties.

Responsibilities include, but are not limited to:

- Adhering to policies that govern acceptable use of organizational systems.
- Using the organization-provided IT resources for defined purposes only; and
- Reporting anomalies or suspicious system behavior.

#### 1.7 Supporting Roles

- Auditor: Auditors are responsible for examining systems to determine:
  - 1- whether the system is meeting stated security requirements and organization policies; and
  - 2- whether security controls are appropriate. Informal audits can be performed by those operating the system under review or by impartial third-party auditors.
- Human Resources: The Human Resource office is often the first point of contact for managers who require assistance in determining whether a security background investigation is necessary for a particular position. The human resources and security offices generally work closely on issues involving background investigations. The human resources office may also be responsible for security-related exit procedures when employees leave an organization.