




Outsourcing Services Policy

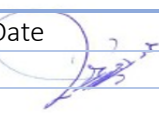
Doc. Control Number	Version
SNL-26	0.3



Document Reference

Item	Description
Title	Outsourcing Services Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	9 July 2024
Revision-Date	9 July 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	7/9/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	7/9/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	7/9/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	28 July 2022	Muhaned Ali	First Release
0.2	9 July 2023	Muhaned Ali	The policy has been reviewed
0.3	9 July 2024	Muhaned Ali	The policy has been reviewed



Contents

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

1. Purpose

This policy aims to define cybersecurity requirements to ensure that SNLC's information and technology assets are protected from cybersecurity risks related to third parties, including IT support services and managed services in accordance with SNLC's regulatory policies and procedures.

2. Scope

This policy applies to all services provided by SNLC third parties and applies to all employees of SNLC.

3. Policy

3.1 General clauses

- 1- Standard procedures for managing SNLC's relationship with external parties before, during, and after the contractual relationship ends must be documented and approved.
- 2- Third-party service providers must be carefully selected and selected in accordance with SNLC's regulatory policies and procedures, and relevant legislative and regulatory requirements.
- 3- A risk assessment should be made of third parties and the services provided and their integrity, by reviewing third-party projects within the SNLC and reviewing the third-party service's cyber event logs (if applicable) before, during, and periodically.
- 4- Contracts and agreements with third parties must be designed to ensure that the third party adheres to the SNLC's cybersecurity requirements and policies and relevant legislative and regulatory requirements.
- 5- Contracts and agreements with external parties must be reviewed by the Legal Affairs Department to ensure that the terms of the agreement are binding during and after the contract period and that its violation exposes the external party to legal accountability.
- 6- Contracts and agreements must include non-disclosure clauses and secure third-party deletion of SNLC data upon termination.
- 7- Cybersecurity requirements with third parties should be reviewed periodically.
- 8- The third-party cybersecurity policy should be reviewed annually, and changes documented and approved.

3.2 Cybersecurity requirements for outsourcing or managed services provided by third parties.

For IT support services or managed services, the third party must be chosen carefully, and the following must be checked:

- 1- Assessing cybersecurity risks and ensuring that there is a guarantee of controlling those risks, before signing contracts and agreements or when changing the relevant legislative and regulatory requirements.
- 2- Operation and monitoring centers of cybersecurity services managed to operate and monitor that use the remote access method must be located entirely within the Kingdom.
- 3- Support services on sensitive systems must be provided by national companies and entities, in accordance with the relevant legislative and regulatory requirements.

3.3 Cybersecurity requirements for third-party employees

- 1- Screening or vetting should be done for support services companies, support services personnel, and managed services working on sensitive systems.

- 2- Cybersecurity responsibilities and Non-Disclosure Clauses must be included in third-party employee contracts (to include during and after termination/termination of the employment relationship with SNLC).

3.4 Documentation and access controls

- 1- Third parties must develop and follow a carefully documented formal process for granting and revoking access to all information and technical systems that process, transmit or store SNLC information in line with the cybersecurity requirements and objectives of SNLC's cybersecurity controls.
- 2- SNLC information must be accessed and processed in a secure and controlled manner.
- 3- Password controls must be applied to all users who have access to SNLC information in line with the cybersecurity requirements and objectives of SNLC's cybersecurity controls.
- 4- A multi-element authentication system must be applied to access sensitive systems that process, transmit, or store information about SNLC.
- 5- Access rights must be revoked immediately upon termination/termination of any third-party employee who has access to SNLC's information or information and technology assets or in the event of a change of employment role that does not require continued access to them.
- 6- Third parties should periodically review access rights in accordance with SNLC's cybersecurity policies.
- 7- All audit records must be stored, maintained, and made available as requested by SNLC.

3.5 Cybersecurity requirements related to change management.

- 1- Third parties must follow a formal and appropriate change management process in accordance with SNLC policies and procedures and in compliance with cybersecurity requirements.
- 2- Changes made to SNLC's IT and technology assets must be reviewed and tested before they are applied to the production environment.
- 3- SNLC stakeholders must be informed of major changes planned and made to SNLC's information and technology assets.

3.6 Cybersecurity Incident Management and Business Continuity Requirements

- 1- The terms of contracts and agreements with third parties should include requirements regarding the reporting of cybersecurity incidents and reporting to SNLC in the event the third-party experiences a cybersecurity incident.
- 2- An appropriate business continuity plan must be developed to avoid the unavailability of services provided to SNLC in accordance with the requirements of the SNLC Business Continuity and Disaster Recovery Plan.

3.7 Data and information protection requirements

- 1- Third parties must process, store, and destroy SNLC data and information in accordance with SNLC data and information protection policy and standards.
- 2- Appropriate cryptographic controls must be in place to protect SNLC data and information and to ensure its confidentiality, integrity, and availability in accordance with the SNLC cryptographic standard.
- 3- Backup copies of SNLC data and information must be made periodically and in accordance with the SNLC Backup Management Policy.

- 4- SNLC data and information contained in sensitive systems and personal data (data privacy), processed by third parties - in a test environment must only be processed, stored, or used after strict controls are used to protect that data such as data masking or data blending techniques (Data Scrambling or Data Anonymization techniques).
- 5- SNLC data and information on sensitive systems that are processed by third parties must not be transmitted.
- 6- SNLC data and information contained in sensitive systems that are processed by third parties must be classified in accordance with the SNLC Data and Information Classification Policy.

3.8 Audit

- 1- SNLC shall conduct an audit of relevant processes and systems as necessary or appropriate.
- 2- All third-party facilities and personnel shall fully cooperate with SNLC's event log review and audit activities, including the audits performed.

4. Roles and Responsibilities

- 4.1 The sponsor and owner of the policy document: Head of Cyber Security Department.
- 4.2 Policy reviews and update: Cyber Security Department.
- 4.3 Policy implementation: Cyber Security Department, IT Department, Department of Legal Affairs, and Department of Procurement.

5. Policy Compliance

5.1 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.

5.2 Exceptions

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

5.3 Non-Compliance

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