




Cloud Services Policy


Doc. Control Number	Version
SNL-25	0.3




Document Reference

Item	Description
Title	Cloud Services Policy Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	1 June 2024
Revision-Date	1 June 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	6/1/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	6/1/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	6/1/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	7 June 2022	Muhaned Ali	First Release
0.2	1 June 2023	Muhaned Ali	The policy has been updated
0.3	1 June 2024	Muhaned Ali	The policy has been reviewed



Contents

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

1. Purpose

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards for protecting SNLC's information and technology assets on Cloud Computing Services and Hosting. This is to ensure that cyber risks are addressed or reduced by focusing on the basic objectives of protection: confidentiality, integrity, and availability of information.

2. Scope

This policy covers all information and technology assets of SNLC on cloud computing services that are hosted, processed, or managed by third parties, and this policy applies to all SNLC employees.

3. Policy

3.1 General clauses

- 1- All third-party cybersecurity requirements in the Third-Party Cyber Security Policy apply to all cloud and hosting providers.
- 2- The Information Security Department must verify the efficiency and reliability of the cloud computing and hosting services provider, in addition to obtaining a license and having an official record in the Kingdom of Saudi Arabia.
- 3- Cybersecurity requirements for cloud computing and hosting services shall be implemented in accordance with SNLC's regulatory policies and procedures and relevant legislative and regulatory requirements.
- 4- The SNLC must conduct a cybersecurity risk assessment of hosting applications or services in the cloud before selecting a cloud and hosting provider.
- 5- The location of hosting sensitive systems, or any part of their technical components, must be within SNLC, or in cloud computing services provided by a government agency, or a national company that has complied with the controls of the National Cybersecurity Authority related to cloud computing and hosting services.
- 6- SNLC GRC Team will Conduct a risk assessment in accordance with the Cybersecurity Risk Assessment and Information Protection prior to adopting cloud services.
- 7- The Information Security Department shall develop, document, and approve procedures for the use of cloud services.
- 8- Contracts for cloud computing and hosting providers must include, at a minimum, the following:
 - Cyber security requirements and Service Level Agreement terms (SLA).
 - Non-disclosure Clauses, including deletion and destruction of data in an agreement between the service provider and SNLC based on the classification of that data and subject to the data classification policy.
 - Business continuity and disaster recovery requirements.
 - Cloud computing and hosting provider contracts must include the ability for SNLC to terminate service without justification or stipulations.
- 9- The implementation of cyber security requirements with cloud computing and hosting service providers should be reviewed periodically, at least once a year.

3.2 Cyber security requirements related to data hosting/storage

- 1- Data must be classified before being hosted/stored with cloud computing and hosting providers.
- 2- Cloud computing and hosting providers must return the data (in a usable format) and delete it irretrievably upon termination/termination.

- 3- The location, hosting, and storage of SNLC information must be within the Kingdom of Saudi Arabia, subject to the regulations and legislative aspects that such data is not subject to any other country's laws.
- 4- The Information Security Department must ensure that the SNLC environment (including virtual servers, networks, and databases) is separated from other third-party environments in cloud computing services.
- 5- Information Security department approval must be obtained to host sensitive systems or any part of their technical components.
- 6- SNLC shall ensure that data privacy requirements are applied to data hosted in the cloud.
- 7- Data and information transmitted to, stored in, or from the Cloud Services must be encrypted in accordance with the relevant legislative and regulatory requirements of the SNLC.
- 8- SNLC shall ensure that the cloud computing and hosting service provider performs regular backups and protects the backups in accordance with the SNLC-approved backup policy.
- 9- The SNLC shall ensure that the hosting and cloud computing service provider cannot access the stored data and that the service provider's access is limited to the authority necessary to carry out its hosting service management and maintenance activities, or as business requirements.
- 10- The cloud computing and hosting service provider shall restrict access to SNLC's cloud services to authorized users only and use means of user identity verification in accordance with SNLC's Authorized Access and Permissions Management Policy.
- 11- The cloud computing and hosting service provider shall provide the technologies and tools necessary for SNLC to manage and monitor its cloud services.
- 12- The Information Security Department and the Legal Department shall include the provisions of cybersecurity requirements related to data hosting in the contract with the cloud computing service provider.

3.3 Other requirements

- 1- SNLC must ensure event logs are enabled on hosted information assets.
- 2- SNLC must ensure event logs are enabled on hosted information assets.
- 3- SNLC must ensure that the Clock Synchronization of the cloud service infrastructure is synchronized with the timing of SNLC.
- 4- The KPI should be used to ensure the continuous development of the protection of information and technology assets on cloud computing services.
- 5- The cybersecurity requirements for cloud computing and hosting services should be reviewed periodically.
- 6- This policy must be reviewed once a year; at least.

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: IT Department, Cyber Security Department.

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.