Physical Security Policy

Doc. Control Number	Version
SNL-15	0.3

Document Reference

Item	Description
Title	Physical Security Policy
Department	Cybersecurity department
Version No	0.3
Status	Draft
Type	DOCX
Publish-Date	29 May 2024
Revision-Date	29 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/29/2024

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/29/2024

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/29/2024

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	19 July 2022	Muhaned Ali	First Release
0.2	5 May 2023	Muhaned Ali	The policy has been updated
0.3	29 May 2024	Muhaned Ali	The policy has been reviewed

Contents

1. Purpose

The purpose of this policy is to provide cybersecurity requirements based on best practices and standards to ensure that the cybersecurity risks and requirements related to physical security at SNLC are effectively implemented.

2. Scope

This policy covers all SNLC systems, information assets, equipment, and devices and applies to all SNLC employees.

3. Policy

3.1 Protection of Physical Information Assets

a) Protecting Physical Facilities Hosting Information Assets

- **Access Control**: Implement access control mechanisms, such as secure entry points, key card systems, biometric authentication, or security personnel, to restrict access to physical facilities housing information assets.
- **Surveillance**: Install CCTV cameras or other monitoring systems to monitor and record activities in and around the physical facilities.
- **Security Zones**: Establish security zones within the facilities to limit access to authorized personnel only.

b) Protection of Physical Information Assets and Facilities on Offsite Premises

- **Offsite Security Assessment**: GRC team shall conduct a security assessment of offsite premises hosting physical information assets to ensure they meet the required security standards.
- **Contractual Agreements**: Establish comprehensive contractual agreements with third-party providers to outline security responsibilities and compliance requirements.
- **Regular Auditing**: Periodically audit the security measures of offsite premises to ensure ongoing compliance.

c) Delivery and Loading Areas

- **Controlled Access**: Restrict access to delivery and loading areas to authorized personnel only.
- **Inspection**: Implement inspection protocols to verify the contents of incoming and outgoing shipments containing physical information assets.

d) Transportation of Physical Information Assets

- **Secure Transportation**: Use secure transportation methods, such as GPS tracking, or trusted courier services, when transporting physical information assets.
- **Chain of Custody**: Maintain a chain of custody log to track the movement of physical information assets during transportation.

e) Physical Protection Against Environmental Threats

- **Fire Protection**: Install fire detection and suppression systems, such as fire alarms, sprinklers, or fire extinguishers, to mitigate the risk of fire-related incidents.
- **Temperature and Humidity Control**: Implement systems to monitor and maintain appropriate temperature and humidity levels to prevent damage to physical information assets.
- **Water Protection**: Use water-resistant or waterproof storage solutions to protect physical information assets from water-related incidents, such as flooding.

3.2 Controls should be implemented to protect audio, communications, network, and power cables against physical damage, after considering potential hazards. These controls shall, at a minimum, cover the following:

- Protection of communications cables and data networks from the cultivation of wiretapping devices.

- Not extending communications and data network cables in areas that can be accessed by third parties.
- Efficiently protect and isolate communications cables and data networks from damage or unauthorized interception and ensure their extension across secure and protected areas.
- Isolate the power and power cables from the communications and data network cables.
- Using multiple, uninterruptible power sources to support the continuous operation of critical systems and facilities (such as data centers).

3.3 SNLC must logically (e.g., partitioning a physical drive), and/or physically segregate data-at-rest related to Saudi Aramco from the data of other clients or customers.

3.4 Multiple physical security measures must be implemented to prevent unauthorized access to facilities. Entrances and exits must be secured with authentication card key, door locks, and monitored by video cameras.

3.5 Implementation of a physical security risk assessment by the authorities responsible for physical security by analyzing the physical environment and surrounding areas to monitor security and safety threats and identify and address vulnerabilities to protect information assets from exposure to these threats.

3.6 The Safety Department shall develop and approve physical security and safety regulations and procedures for SNLC or any event or event it participates in organizing. It includes a precise definition of duties and tasks, to serve as a general framework for the service of safety, prevention, rescue, firefighting, ambulance, and a guiding guide for the protection of lives, assets, and information.

3.7 SNLC must dedicate an access restricted working area for personnel with access to the Saudi Aramco network.

3.8 Physical access to the facility where information systems reside must be restricted to authorized personnel and reviewed on a regular basis.

3.9 Not to grant external parties' physical access to the entity's facilities except after achieving security requirements, provided that their access is monitored and escorted to places that require this.

3.10 The authority to administer the physical access system should be limited to persons with specific privileges that can be audited.

3.11 Periodically review and update the permissions of physical access to sensitive areas.

3.12 Training the company's employees in best practices related to physical security such as the clean office policy and ensuring their compliance with it.

3.13 A Performance Measurement Indicator (KPI) should be used to ensure the continuous development of cybersecurity requirements related to physical security.

4. Physical Access Management

4.1 Physical Access Authorizations and Control

a) Only authorized individuals with a legitimate need shall be granted access to SNLC's facilities.
b) All systems (routers, switches, servers, and firewalls) must be housed in a communication room and locked rack(s). The access to the communication room must be contingent on security requirements, such as access card readers or biometric devices.
c) Access authorizations shall be assigned based on job roles and responsibilities through a formal approval process.
d) Access to sensitive or high-security areas shall require additional approvals and undergo a higher level of scrutiny.
e) Backup media must be secured to block/inhibit unauthorized physical access.

4.2 Physical Access Control List

a) Maintain a comprehensive and up-to-date Physical Access Control List that includes individuals with authorized access to the SNLC's facilities.
b) Assign unique identifiers (e.g., employee ID numbers or access cards) to authorized personnel for easy identification.
c) Periodically review and update the Physical Access Control List to reflect changes in employee status, job roles, or access requirements.

4.3 Physical Access Management Process
a) Design and implement a Physical Access Management process that outlines the procedures for granting and managing access to physical facilities.
b) Issue appropriate authorization credentials (e.g., access cards, keys) to individuals with approved access.
c) Include a formal request and approval workflow in the process to ensure proper authorization for access.

4.4 Physical Entry Controls for Visitors
a) SNLC must define a process for visitor management. The process should include maintaining and regularly reviewing visitor logs. The visitor log should capture information such as (Visitor identification, Visit Purpose, check in/check out date and time).
b) Establish entry controls for visitors to restrict access to authorized areas only.
c) Issue security badges or temporary access cards to visitors for identification purposes during their stay.
d) Monitor visitors' activities, and escort them when accessing sensitive or restricted areas.

4.5 Continuous Review of Physical Access Control List
a) Conduct regular reviews of the Physical Access Control List to verify the necessity of access for everyone.
b) Remove individuals from the list promptly when access is no longer required due to job changes, termination, or other reasons.

4.6 Monitoring Physical Access Logs
a) Regularly review physical access logs to detect any unusual or suspicious activity.
b) Implement a logging and monitoring system to track access events and potential security breaches.

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: Physical Security Management

6. Compliance and Enforcement

6.1 Compliance with this policy is mandatory for all employees, contractors, and visitors accessing SNLC's facilities.
6.2 Violations of this policy may result in disciplinary action, including but not limited to retraining, suspension, termination, and legal consequences, as appropriate.

7. Policy Review

7.1 This policy will be reviewed on a periodic basis to ensure its continued relevance and effectiveness. Any updates or modifications to this policy shall be communicated to all relevant employees and stakeholders.