




Backup and Recovery Management

Doc. Control Number	Version
SNL-21	1.0



Document Reference

Item	Description
Title	Backup and Recovery Management
Department	Cybersecurity department
Version No	1.0
Status	Draft
Type	DOCX
Publish-Date	31 March 2024
Revision-Date	31 March 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	31/3/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	1/4/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	1/4/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	13 Jan 2022	Muhaned Ali	First Release
0.2	11 July 2022	Muhaned Ali	Policy Updated
0.3	29 May 2023	Muhaned Ali	The Policy has been reviewed
1.0	31 March 2024	Muhaned Ali	The Policy has been reviewed



Contents

1. Purpose	4
2. Scope.....	4
3. Policy	4
4. Policy Compliance	6

1. Purpose

The purpose of this policy is to maintain data integrity and availability of the SNLC's IT Resources to prevent loss of data and to facilitate the restoration of the IT Resources and business processes.

2. Scope

This policy applies to all members of the SNLC community including Finance, Human Resources, BD, Managed Services, Secure Communications, Safety Division, and InfoSec.

3. Policy

There is always a risk that systems and/or procedures will fail to result in loss of access to information, data, and systems, despite the implementation of best practices.

The following steps will help ensure the SNLCs information and data are backed up and restored securely in the most efficient manner possible:

3.1 IT System/ Data Backups

- a) The SNLC's IT administrators are responsible for providing system support and data backup tasks and must ensure that adequate backup and system recovery practices, processes, and procedures are followed in line with the SNLC's Disaster Recovery Procedures and departmental data retention policies.
- b) SNLC must establish and follow regular procedures for backup of critical systems and Saudi Aramco's data, software, and websites.
- c) Backup stored at an off-site location must be encrypted using at least AES encryption algorithm, and 256 bits key, except for data classified as public.
- d) To ensure full availability, the IT team must follow the backup and recovery process.
- e) All IT backup and recovery procedures must be documented, regularly reviewed, and made available to trained personnel who are responsible for performing data and IT system backup and recovery.
- f) All data, operating systems/domain infrastructure state data, and supporting system configuration files must be systematically backed up - including patches, fixes, and updates that may be required in the event of system re-installation and/or configuration.
- g) Wherever practicable, backup media (e.g., tape) must be encrypted and appropriately labeled. Any system used to manage backed-up media should enable storage of data/s and codes/markings which enables easy identification of the original source of the data and type of backup used on the media. All encryption keys should always be kept securely with clear procedures in place to ensure that backup media can be promptly decrypted in the event of a disaster.
- h) Copies of backup media must be removed from devices as soon as possible when a backup or restore has been completed.
- i) Backup media which is retained on-site prior to being sent for storage at a remote location must be stored securely in a locked safe and at a sufficient distance away from the original data to ensure both the original and backup copies are not compromised by the same event.
- j) Access to the on-site backup location and storage safe must be restricted to authorized personnel only.
- k) All backups identified for long-term storage must be stored at a remote secure location with appropriate environmental control and protection to ensure the integrity of all backup media.
- l) Backup media must be protected in accordance with the SNLC's Physical and Environmental and Data Protection and Media Handling Policies.
- m) Hard copy paper files containing important information and data should be scanned and stored electronically to ensure digital copies are created which can be backed up by the

SNLC's IT systems. Where this may not be possible, photocopies of paper files must be made and stored in a secure storage location.

- n) Regular tests must be carried out to establish the effectiveness of the SNLC's backup and restore procedures by restoring data/software from backup copies and analyzing the results. Departmental IT Service Relationship managers should be provided with information relating to any issues with the backup testing of their data.
- o) The IT Services Data Centre team should maintain a record of job failures, with the re-running of any failed jobs logged in to the backup software management console.

3.2 User Responsibilities

- a) IT Users also have a responsibility to ensure SNLC data is securely maintained and is available for backup:
 - 1- IT Users must not store any data/files on the local drive of a computer (this excludes the normal functioning of the Windows operating system and other authorized software which require the 'caching' of files locally to function). Instead, Users must save data (files) in their allocated areas.
 - 2- If the SNLC network becomes unavailable for whatever reason and work-related data is at risk of being lost, users have no option but to save the data (files) locally. Once the Corporate Network becomes available again, data (files) should be immediately transferred to the corporate network for it to be backed up safely and local copies of data on the computer or portable storage media should be deleted. This will help to ensure the availability and integrity of data and to avoid duplicate copies of data being stored.
 - 3- Only SNLC purchased and encrypted USB data sticks should be used, and any data stored must be for temporary purposes. All sensitive, business, and personally identifiable information should be removed from the USB data and moved to an appropriate SNLC data network location as soon as possible to ensure the data is made available to the SNLC and can be successfully backed up.
 - 4- Mobile devices/phones must not be used to store sensitive, business, or personally identifiable information. In the event of unforeseen or unavoidable situations leading to important data being stored on mobile devices/phones, the data must be stored at a suitable SNLC network location and removed from the mobile device/phone as soon as possible.

3.3 Data Restores

This section of the policy document outlines the policy for recovery of data relating to SNLC Backup.

- a) Requests to recover data or systems should be submitted to the IT Service Desk. Requests must be made at the earliest possible time following the loss of data or system.
- b) The SNLC IT department cannot accept responsibility for delay by a member department or individual to register requests for data or system restoration.
- c) Data restoration from backup is subject to the retention and granularity periods defined within this backup policy.
- d) Backup policy recovery schedules. Where requests to recover data from the backup are processed the SNLC IT department must endeavor to process such requests as soon as possible following receipt. The following table summarizes recovery schedules for types of backups carried out by the SNLC IT department.

Data Type	Recovery Period (Hours from request receipt)	Type of Recovery	Potential data loss (The period of potential difference [hours]between)
-----------	--	------------------	---



			loss of data & last backup).
Personal Data files stored on SNLC data servers (Not exceeding 5GB)	24 Hours	Permanent recovery to original data location.	24 Hours
Accounting Data	3 Hours	Permanent recovery to original data location.	No data loss is anticipated.
Infrastructure servers, routers.	3 Hours	Initial recovery using system replica. Later Scheduled Permanent recovery to original data location.	12 ours

4. Policy Compliance

4.1 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.

4.2 Exceptions

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

4.3 Non-Compliance

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