



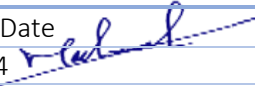
Backup and Recovery Process


Doc. Control Number	Version
SNL-32	0.2



Document Reference

Item	Description
Title	Backup and Recovery Process
Department	Cybersecurity department
Version No	0.2
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	5/29/2023	Muhaned Ali	First Release
0.2	29 May 2024	Muhaned Ali	The document has been reviewed



Contents

1. Purpose.....	4
2. Scope	4
3. Backup and Recovery Process	4
4. Backup Technology	5
5. Rules and Responsibilities	5

1. Purpose

The purpose of this plan is to provide a successful procedure for backup and recovery of critical data. These procedures are in place to assist and guide the SNLC Information Technology Staff. Backup and recovery methods are essential to data protection and security. Any loss of data due to file corruption, virus, security, or human error is a loss of time and money. Furthermore, loss of data can impact the company. An effective backup and recovery plan is crucial to the company.

2. Scope

The scope of these procedures extends to the back-up of all important information and data regardless of the form it takes - including the recovery of IT systems and supporting infrastructure.

3. Backup and Recovery Process

3.1 A backup procedure must include the following elements:

- a) Objective
Clearly outline the goal and objectives of the backup procedures policy to ensure that everyone understands the reasons why backups are required.
- b) Frequency
Set up a regular schedule for backups based on the criticality of the data. For example, critical data may require daily backups while less critical data may require weekly or monthly backups.
- c) Backup Type
Define what type of backup should be performed. The options include full backups, incremental backups, and differential backups.
- d) Backup Media
Determine the media to be used for backups. For example, Online or Offline
- e) Backup Retention
Define how long the backups should be retained to ensure that critical data is available in the event of data loss or corruption.
- f) Backup Testing
Establish a regular process to test the effectiveness of backups and ensure that data can be recovered successfully.
- g) Backup Security
Implement measures to ensure that backups are secure and not accessible to unauthorized personnel.

3.2 A recovery procedure must include the following elements:

- a) Identify Critical Information Assets
The first step of a recovery plan is to identify critical information assets. This includes data and documents that are essential to your business operations such as financial records, customer data, employee information, and legal documents.
- b) Define Recovery Time Objectives
Define how quickly you need to restore your data after a disaster occurs. Based on the criticality of each information asset, different RTOs are set. Typically, critical data has a shorter RTO than less important data.
- c) Determine Recovery Point Objectives
Is how much data loss being acceptable in the event of a disaster. For critical information assets, an RPO of near-zero data loss may be necessary, while less critical data may have a higher RPO.
- d) Create a Recovery Plan

A recovery plan outlines the steps to be taken to recover information assets in case of a disaster. This plan includes backup procedures, restoration procedures, and failover procedures.

e) Test the Recovery Plan

Testing the recovery plan ensures that the plan is effective and can be put into action when needed. The testing process should include all key stakeholders. Any errors found during the testing process should be documented and rectified.

f) Review and Update the Recovery Plan

The recovery plan should be reviewed on a regular basis.

3.3 The RPO must be determined by the data owner.

3.4 To decide the PRO, the IT Manager will contact the data owner.

3.5 The scope will be determined based on data requirements, whether online or offline.

3.6 Ensure the confidentiality, integrity, and availability of backups in adverse situations (e.g., using encryption, protection of backups via physical security)

3.7 Regularly review and update the backup and procedures plan to ensure it is up to date and effective.

4. Backup Technology

4.1 This section describes the technology used for backup infrastructure, as of May 2023.

a) Hardware (**WD my Cloud Ex4100 18Tb**)

5. Rules and Responsibilities

5.1 The backup and recovery procedure are managed by the IT staff.

5.2 The Security team is responsible for ensuring backup confidentiality, integrity, and availability in emergency scenarios.

5.3 Data Backup detail are as follows:

Type	Data	Backup Frequency	Backup media	Responsible
VM Server	System	Weekly incremental	VM Datastore Local Storage Ex4100	Backup administrator
Network Devices (FW's, Routers, Switches, PBX)	Configuration Files	Weekly incremental	Local Hard disk Local Storage Ex4100	Backup administrator
Workstations, Laptops	Files and Folders	Weekly incremental	Local Storage Ex4100	Backup administrator

Table 1 Backup details