NEOSOFIA

System Backup and Recovery SOP

IT-245-SystemBackupandRecovery

Neosofia, LLC

Version: V004

Effective: 2025-05-10

Table of Contents

1 Purpose

Establish a systematic approach to data backup and recovery to prevent loss, enable rapid restoration and maintain data integrity for all Neosofia IT systems.

2   Scope

This SOP applies to any IT system that manages Neosofia client or corporate data.

2.1   Assets in Scope

Each of the assets below will have an entry in this SOP that outlines the backup and recovery procedures Neosofia employs to protect client and corporate data.

Data/Support Asset	RPO	RP	RTO	OC
Hardware	N/A	N/A	2 hours	N/A
Operating Systems	1 day	7 days	1 hour	1 full + 6 incr.
Virtual Machines	1 day	28 days	1 hour	1 full + 27 incr.
Public DNS Records	N/A	N/A	1 hour	N/A
Source Code	1 week	25 years	1 week	1 full
System Logs	15 min	28 days	1 hour	1 full
Credentials	1 hour	1 year	1 hour	1 full

Neosofia will store one offline copy of each asset above

3   Responsibilities

IT System Administrators will be responsible for

- L4 Architecture, design, implementation, and execution of the procedures outlined in this document.
- L3 System monitoring to determine if restoration procedures need to be executed on
- L2 Documentation of the backup and restoration procedure execution as evidence for auditors
- L1 Provide feedback on this document

IT Managers will be responsible for

- L4 Review of this document no less than once per year
- L4 Respond to and integrate feedback into this document
- L3 Review of this document when new IT systems are procured or retired to determine the system backup and restoration procedures that may require an update
- L4 Advise and mentor IT System Administrators in their responsibilities.

4   Procedures

4.1   Hardware Procedures

Neosofia will maintain a 2% hardware inventory reserve to recover from hardware losses or will define procedures below to enable cloud resources to be used as a temporary replacement for system restoration.

4.2   Operating System Procedures

4.2.1   OS Backup Procedure

When provisioning a new piece of hardware, the OS setup script will automatically set up an OS level backup procedure to be run on a daily basis. Evidence that the script was successfully run can be found in the system backup and recovery section of the evidence portal.

4.2.1.1   Entry Criteria   Rolling OS level backup procedures begin automatically starting at 2AM UTC

4.2.1.2   Backup Procedure and Automated Restoration Test

> [!NOTE] These procedures are executed programmatically on a daily basis and should not be manually executed

1. Create a full OS level snapshot and on-device (USB stick) rescue media needed to restore the system in the event of a hardware failure
2. Reboot the device into the rescue media's automated restoration program
3. Upon system restoration and reboot, upload the restoration logs into the evidence portal

4.2.1.3   Exit Criteria   If the daily OS backup procedure completes without errors, a status report is automatically sent to the evidence portal. If any errors occur, an email is sent to all IT System Administrators with details of the error to be remediated.

4.2.1.4   SLOs

- automated backup and system restoration should take no more than 15 minutes 99% of the time

4.2.2   OS Recovery Procedure

4.2.2.1   Entry Criteria   Upon notification of a system failure or data loss.

4.2.2.2   Procedure

1. Identify and replace defective hardware
2. Start machine into system restoration device (F7 or F11 key for most systems)

3. The restoration procedure should begin automatically. If the restoration procedures requests input due to hardware changes, contact a L3 IT system Administrator or higher for guidance on appropriate inputs.
4. Upon restoration, confirm the restoration evidence was uploaded to the portal.

4.2.2.3   Exit Criteria   if the automated restoration process fails an error email will be sent to all IT System Administrators

4.3   VM Procedures

TBD

4.4   Networking Procedures

TBD

4.5   Source Code Procedures

TBD

4.6   Log File Procedures

TBD

4.7   Credential Procedures

TBD

5   Changelog

Version	Date	Author	Message
V004	2025-04-07	Ben Young	Enhance the PDF Generator (#61)
V003	2025-04-03	Ben Young	add changelog and section numbers to generated pdf documents (#59)
V002	2025-04-02	Ben Young	QMS Doc Generation (#55)
V001	2025-03-18	Ben Young	move to react router ssg (#47)

6   Electronic Signatures

Date	Signature ID/Owner	Actor	Reason
2025-04-07 10:19:52 +0000	B5690EEEBB952194	Ben Young	Author Change 9450889
2025-04-07 10:11:07 +0000	FC3FA4329A10866C	Ben Young	Author Change 1ccc2ac
2025-04-07 14:50:25 +0200	B5690EEEBB952194	Ben Young	Approval