




Asset Handling Procedure


Doc. Control Number	Version
SNL-39	0.2



Document Reference

Item	Description
Title	Asset Handling Procedure
Department	Cybersecurity department
Version No	0.2
Status	Draft
Type	DOCX
Publish-Date	23 May 2024
Revision-Date	23 May 2025

Authors		
Name	Department	Signature/Date
Muhaned Kamal Ali	Cybersecurity - I. S Specialist	5/23/2024 

Reviewed by		
Name	Department	Signature/Date
Yasir Awad	Head of Cyber Security Department	5/23/2024 

Approved by		
Name	Department	Signature/Date
Abdullah Al Shuhail	V.P	5/23/2024 

Control-Page

Document Amendment Record			
Version-No	Date	Prepared-by	Explanation
0.1	23 May 2023	Muhaned Ali	First Release
0.2	23 May 2024	Muhaned Ali	The document has been reviewed



Contents

1. Overview	4
2. Scope.....	4
3. Asset handling procedure	4
4. Conclusion.....	7

1. Overview

The purpose of this document is to set out the specific controls that must be used when handling information of a particular classification. For details of the criteria for classifying information assets, please see the Information Classification Procedure.

Classified information must not be disclosed to any other person or organization via any insecure method including, but not limited, to the following:

- Paper based methods.
- Fax.
- Telephone.
- Email.
- Verbally.

Where information is disclosed/shared with third parties it should only be done so in accordance with a documented information sharing protocol and/or data exchange agreement.

The disclosure of classified information to an unauthorized person is a disciplinary offence. If there is suspicion that such information has been communicated in a way that could be harmful to the organization or to the data subject, then it is to be reported in accordance with the company's information security incident management procedures.

Any sharing or transfer of classified information with other organizations must comply with all legal, regulatory and organization policy requirements.

2. Scope

This control applies to all systems, people and processes that constitute the organization's information systems, including board members, directors, employees, suppliers and other third parties who have access to SNLC systems.

3. Asset handling procedure

For each security classification level, a set of handling controls must be in place to ensure that the information assets involved are always appropriately protected.

The following sections set out the main procedural components of these controls.

- **Level 0: Public** (or Unclassified)

This classification describes information which is in the public domain or is freely published by the organization.

- Secure processing

In general, there are no specific controls that must be placed on the processing of such information although it should be borne in mind that items such as headed stationery and their electronic equivalents should not be made freely available.

- Storage

Level 0 information may be stored in unsecured areas accessible to the public. However, some controls should be placed on large quantities of such information such as leaflets which could still be subject to theft or misuse.

Information of this classification may be stored on electronic media such as backup tapes, DVDs and CDs without encryption or other forms of protection.

- Transmission

In general, **Level 0** information may be sent in the clear over unencrypted connections or distributed freely in hard copy.

- Declassification

Level 0 information will not be subject to declassification as it is already at the lowest level.

- Destruction

Information falling within the Level 0 classification may be disposed of via normal waste routes without need for controls such as shredding. Where possible, items should be recycled.

- Chain of custody

Level 0 information assets will be freely distributed amongst organization employees, customers, and members of the public where required, without the need to keep records (unless for operational purposes).

- Logging of security-related events

There is generally no need to log security incidents relating to Level 0 classification items unless subject to criminal activity such as large-scale theft of material.

- **Level 1: Internal Use Only**

Level 1 is the lowest level of classification to which protection is applied.

- Secure processing

Information at this level of classification will be subject to access controls involving either physical security or an authorized use logon or both. Access should not generally be granted in public areas and output such as printouts should be to areas where public access is prevented.

- Storage

Information of this classification may be stored on electronic media such as backup tapes, DVDs, and CDs. These media should be subject to secure storage such as in a locked room in an area where there is no public access.

- Transmission

In general, Level 1 information may be sent in the clear over unencrypted connections in small quantities, such as when dealing with an individual customer. However, the use of file encryption is strongly recommended for items such as email attachments particularly where they contain significant quantities of Level 1 data.

- Declassification

Level 1 information may be declassified to “Public” with the permission of the asset owner at which time the controls specified above will apply.

- Destruction

Level 1 information should be destroyed securely so that it cannot be reconstituted e.g., via shredding for paper or full deletion for electronic files.

- Chain of custody

No specific controls are placed on the chain of custody for Level 1 information although reasonable precautions should be taken to ensure that it always stays within the organization.

- Logging of security-related events

Incidents where Level 1 information has been compromised should be recorded and investigated in accordance with the company’s security incident management procedures.

- **Level 2: Restricted**

Level 2 is the second level of classification to which protection is applied.

- Secure processing

Information at this level of classification will be subject to strict access controls involving both physical security and authorized use logon. Access will not be granted in public areas and output such as printouts must be to areas where public and unauthorized employee access is prevented.

- Storage

Information of this classification may be stored on electronic media such as backup tapes, DVDs, and CDs. These media must be subject to secure storage such as in a locked room in an area where there is no access to unauthorized personnel. Procedures must be in place for the management of keys to such areas.

- Transmission

Restricted information may not be sent in the clear over unencrypted connections and the use of file encryption is mandatory for items such as email attachments.

- Declassification

Restricted information may be declassified to “Internal use only” or “Public” with the permission of the asset owner at which time the controls specified in the relevant section above will apply.

- Destruction

Level 2 information must be destroyed securely so that it cannot be reconstituted e.g., via shredding for paper or full deletion for electronic files. Where possible, secure destruction should be verified by a second authorized individual.

- Chain of custody

The chain of custody for Level 2 information should be clearly defined and tracked via formal handovers including signatures for acceptance.

- Logging of security-related events

Incidents where Level 2 information has been compromised should be reported immediately and flagged as a major incident. Such incidents will be recorded and investigated in accordance with the company’s security incident management procedures.

- **Level 3: Confidential**

Level 3 is the highest level of classification to which protection is applied.

- Secure processing

Information at this level of classification will be subject to very strict access controls involving both physical security and authorized use logon with additional security measures in place. Access will not be granted in public areas and output such as printouts must be to areas where only those organization staff who are authorized to the information asset can reach it.

- Storage

Information of this classification must not be stored on removable electronic media such as DVDs and CDs. Backups may be taken as long as this provides no more access than when the information is within the computer system. Backup media must be subject to secure storage such as in a locked room in an area where there is no access

to unauthorized personnel. Procedures must be in place for the management of keys to such areas. Additional controls such as encryption must be used where it is practical. Hardcopy information must not be removed from its home office unless with the express approval of the information asset owner.

- Transmission
Level 3 information must not be sent in the clear over unencrypted connections and the use of file encryption is mandatory for items such as email attachments (although the use of email is to be discouraged).
- Declassification
Confidential information may be declassified to “Restricted”, “Internal use only” or “Public” with the permission of the asset owner at which time the controls specified in the relevant section above will apply.
- Destruction
Level 3 information must be destroyed securely so that it cannot be reconstituted e.g., via shredding for paper or full deletion for electronic files. Where possible, secure destruction should be verified by a second authorized individual.
- Chain of custody
The chain of custody for Level 3 information should be clearly defined and tracked via formal handovers including signatures for acceptance. Where possible, copies of the information should be numbered, and its possession always tracked.
- Logging of security-related events
Incidents where Level 3 information has been compromised should be reported to senior management immediately and flagged as a major incident. Such incidents will be recorded and investigated in accordance with the company’s security incident management procedures.

4. Conclusion

It is important that this procedure is followed in all cases so that the company’s assets are adequately protected in line with the appropriate classification.

The controls described in this procedure must be followed throughout the lifecycle of information assets, including where they are transferred to third parties. Proper handling of assets is fundamental to the correct operation of the ISMS and without it many of the other controls that are in place will not be effective.

All employees and third parties who meet the company’s information assets must be aware of this procedure and the necessary arrangements it specifies.