



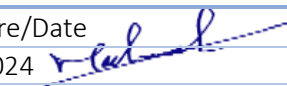
Information Labelling Procedure


Doc. Control Number	Version
SNL-40	0.2



Document Reference

Item	Description
Title	Information Labelling 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. Information labelling procedure	4

1. Overview

The purpose of this document is to set out how information assets will be labelled according to the information classification scheme in place within SNLC. For details of the scheme used and the criteria for classifying information assets, please see the Information Classification Procedure.

The labelling of information assets is a key control which will allow the appropriate level of protection to be applied. Unless information is clearly marked, employees and third parties cannot know whether the information is sensitive or not, particularly as this can change over time.

It is the responsibility of everyone involved in the company to carefully consider how the information they produce, handle, and dispose of can always remain effectively labelled.

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.

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. Information labelling procedure

To ensure that the correct controls are applied to the information assets of the organization, a system of protective marking will be used so that all employees and third parties (where applicable) are aware of how that information must be managed.

- Printed reports

Where possible, a printout of information that carries a security classification will display the security marking as a watermark, clearly visible on every page of the document.

Where this is not possible, one of the following methods will be used:

- The classification will be shown clearly on the front page and in the header of every subsequent page.
- Pre-printed paper showing the security classification will be used.
- A stamp will be used to mark each page with the security classification.

It is expected that the clearest and least labor-intensive method will be selected in each case.

- Screen displays

Computer systems which allow an authorized user access to classified information will include a warning of this fact upon logon which requires user acknowledgement of some form. Where feasible, users should also be warned upon entering an area of the system which contains a higher classification of information than most other areas.

- Recorded media

Strict controls are placed on the use of removable media such as CDs, DVDs, tapes, external hard drives, and USB memory sticks within the organization. Where these are legitimately used to store classified data, they will be labelled externally with the security classification of the most sensitive data on the media, together with the date of creation.

- Electronic messages

Classified information sent within emails must include the classification level and, if being sent externally, a statement of the controls that must be placed on the information by the recipient of the email. Where the information is contained within an attachment, this

must also state the classification clearly at the header of the document, spreadsheet, or other type of file.