




Information Classification Procedure


Doc. Control Number	Version
SNL-38	0.2



Document Reference

Item	Description
Title	Information Classification 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 classification procedure	4
4. Roles and Responsibilities.....	6

1. Overview

Information can take many forms including, but not limited to, the following:

- Hard copy data held on paper.
- Data stored electronically in computer systems.
- Communications sent by physical post or using email.
- Data stored using electronic media such as USB drives, disks, and tapes.

Personal information is any information about any living, identifiable individual. The organization is legally responsible for this, and its storage, protection and use are governed by national and international law. Details of specific requirements for personal information can be found in the Privacy and Personal Data Protection Policy.

The Company maintains inventories of all-important information assets upon which it relies. However, SNLC recognises that there are risks associated with employees, customers, contractors and other third parties accessing and handling information in order to conduct official Company business.

SNLC has a responsibility to protect the information it holds and processes using controls appropriate to the sensitivity of the information involved.

Only by classifying information according to a documented scheme can the correct level of protection be applied. This procedure sets out the details of the scheme to be adopted and the criteria applied in deciding which level of protection to apply to any given information asset.

2. Scope

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

3. Information classification procedure

On creation, all information assets must be assessed and classified by the owner according to their content. The classification will determine how the document should be protected and who should be allowed access to it. Any system subsequently allowing access to this information should clearly indicate the classification.

3.1 Classification scheme

The SNLC information classification scheme requires information assets to be protectively marked into one of 3 classifications (excluding public information which does not need to be marked). The way the document is handled, published, moved, and stored will be dependent on this scheme.

The classes of information are:

- a) Level 0: Public (or unclassified)
- b) Level 1: Internal Use Only
- c) Level 2: Restricted
- d) Level 3: Confidential

The definitions of these classes of information are described in further detail below. The decision regarding which classification an information asset should fall into is based on the following main criteria:

- a) **Legal** requirements that must be complied with.
- b) **Value** to the organization.
- c) **Criticality** to the organization.
- d) **Sensitivity** to unauthorized disclosure or modification

These areas are considered in the definitions below.

- a) **Level 0: Public/Unclassified** information assets

Much of the information held by the organization is freely available to the public via established publication methods. Such items of information have no classification and will not be assigned a formal owner or inventoried.

It may be necessary however to maintain an awareness of the information that falls within this classification over time as circumstances may change and a need to provide increased protection of previously public information assets may arise.

b) Level 1: Internal Use Only

For information that is not published freely by the organization, some of this may be classified as internal only. This is typically information, which is relatively private in nature, either to an individual or to the organization and, whilst its loss or disclosure is unlikely to result in significant consequences, it would be undesirable.

This classification label applies to information intended for use within the Company, and in some cases within affiliated organizations, such as business partners of the Company. Assets of this type are widely distributed within the Company and may be distributed within the Company without permission from the information asset owner. (e.g., telephone directory, dial-up computer access numbers, new employee training materials, and internal policy manuals.)

The criteria for assessing whether information would be classified as **Internal only** include whether its unauthorized disclosure would:

- Cause distress to individuals.
- Breach proper undertakings to maintain the confidence of information provided by third parties.
- Breach statutory restrictions on the disclosure of information.
- Cause financial loss or loss of earning potential, or to facilitate improper gain.
- Give an unfair advantage to individuals or companies.

c) Level 2: Restricted

The level above Internal only is that of Restricted. This information would be more serious if it were disclosed to unauthorized persons and result in significant embarrassment to the organization and possibly legal consequences.

This classification label applies to the most private or otherwise sensitive information of the Company. Information under this classification shall be strictly monitored and always controlled. (e.g., merger and acquisition documents, trade Secrets, financial records, Government sectors (MOI, BG), and Private sectors (Saudi Aramco, STC, KJO). contractors, and management communication).

The criteria for assessing whether information would be classified as **Restricted** include whether its unauthorized disclosure would:

- Affect relations with other organizations adversely.
- Cause substantial distress to individuals.
- Cause financial loss or loss of earning potential or to facilitate improper gain or advantage for individuals or companies.
- Prejudice the investigation or facilitate the commission of crime.
- Breach proper undertakings to maintain the confidence of information provided by third parties.
- Impede the effective development or operation of organizational policies.
- Breach statutory restrictions on disclosure of information.
- Disadvantage the organization in commercial or policy negotiations with others.
- Undermine the proper management of the organization and its operations.

Information falling into the classification of “Restricted” will typically be handled by middle management and above, with some employees of lower clearance being given access only in specific circumstances.

d) **Level 3: Confidential**

The highest level of classification is that of Confidential. This is reserved for information which is highly sensitive and would cause major reputation and financial loss if it were lost or wrongly disclosed.

This classification label applies to Company information, which is private or otherwise sensitive in nature and shall be restricted to those with a legitimate business need for access. (e.g., employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally generated market research, computer passwords, identity token personal identification numbers (PINs), and internal audit reports).

The criteria for assessing whether information would be classified as Confidential include whether its unauthorized disclosure would:

- Materially damage relations with other organizations (i.e., cause formal protest or other sanction).
- Cause damage to the operational effectiveness or security of the organization.
- Work substantially against organizational finances or economic and commercial interests.
- Impede seriously the development or operation of organizational policies.
- Shut down or otherwise substantially disrupt significant business operations.

Access to information assets defined as “**Confidential**” will be tightly controlled by senior management and in many cases numbered copies of documents will be distributed according to specific procedures.

3.2 Deciding the correct classification

When deciding which classification to use for an information asset, it is recommended that an assessment is conducted to consider the likely impact if the asset were to be compromised. The criteria given above should be used for this purpose.

A correct classification will ensure that only genuinely sensitive information is subject to additional controls. The following points should be considered when assessing the classification to use:

- a) Applying too high a classification can inhibit access, lead to unnecessary and expensive protective controls, and impair the efficiency of the organization's business.
- b) Applying too low a classification may lead to damaging consequences and compromise of the asset.
- c) The compromise of larger sets of information of the same classification is likely to have a higher impact (particularly in relation to personal data) than that of a single instance. Generally, this will not result in a higher classification but may require additional handling arrangements. However, if the accumulation of that data results in a more sensitive asset being created, then a higher classification should be considered.
- d) The sensitivity of an asset may change over time, and it may be necessary to reclassify assets. If a document is being de-classified or the marking changed, the file should also be changed to reflect the highest marking within it.

4. Roles and Responsibilities

4.1 Employees

- a) Employees must manually write the email classification before sending any emails.

4.2 IT Team

- a) The IT team's primary responsibility is to execute data classification, ensure that all data is classified, and assist the business owner in deciding on the appropriate classification.

4.3 GRC Team

- a) The GRC team is in charge of creating policies and processes, classifying data according to business needs, and consulting with business owners to implement the proper controls for protecting data.
- b) Confirming that data at rest, in motion, and in a transit have the data classification implemented correctly.

4.4 SOC Team

- a) Closely monitor and notify the GRC team right away if any unclassified data are found.