This is a guidance box. Remove all guidance boxes after filling out the template. Items highlighted in turquoise should be edited appropriately. Items highlighted in green are examples and should be removed. After all edits have been made, all highlights should be cleared.

Insert entity logo by clicking on the outlined image.

Data Loss Prevention Standard Template

Choose Classification

DATE	Click here to add date
VERSION	Click here to add text
REF	Click here to add text

Replace <organization name> with the name of the organization for the entire document. To do so, perform the following:

- Press “Ctrl” + “H” keys simultaneously
- Enter “<organization name>” in the Find text box
- Enter your organization’s full name in the “Replace” text box
- Click “More”, and make sure “Match case” is ticked
- Click “Replace All”
- Close the dialog box.

Disclaimer

This template has been developed by the National Cybersecurity Authority (NCA) as an illustrative example that can be used by organizations as a reference and guide. This template must be customized and aligned with the <organization name>'s business and relevant legislative and regulatory requirements. This template must be approved by the head of the organization (Authorizing official) or his/her delegate. The NCA is not responsible for any use of this template as is, and it affirms that this template is solely an illustrative example.

Document Approval

Role	Job Title	Name	Date	Signature
Choose Role	<Insert job title>	<Insert individual's full personnel name>	Click here to add date	<Insert signature>

Version Control

Version	Date	Updated By	Version Details
<Insert version number>	Click here to add date	<Insert individual's full personnel name>	<Insert description of the version>

Review Table

Periodical Review Rate	Last Review Date	Upcoming Review Date
<Once a year>	Click here to add date	Click here to add date

Table of Contents

Purpose

This standard aims to define the detailed cybersecurity requirements related to the data loss prevention of <organization name>'s data to minimize cybersecurity risks resulting from internal and external threats at <organization's name> in order to preserve confidentiality, integrity and availability.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This standard covers all <organization name>'s enterprise data and applies to all <organization name> personnel (employees and contractors).

Standards

1	Data and information type and vector definition
Objective	To define the types of data and information to be monitored and the vectors by which such data and information can leak from the organization
Risk implication	A poor, or no definition, of the types of data and information and vectors to be monitored may mean that data loss approaches are not designed and implemented correctly, allowing data and information to leave <organization name>
Requirements	
1-1	The types of data and information to be monitored must be defined by asset owners and the <head of cybersecurity function>, with input from other stakeholders, at <organization name>.
1-2	The type of data and information to be monitored must include:

	a) all data and information that must be monitored due to legal and regulatory obligations applicable to <organization name> b) all data and information classified as “Restricted” or above (see Data Classification Policy) c) all data and information that are considered as personal d) all data and information that must be monitored to meet operational and commercial obligations with third parties and suppliers
1-3	A Data Loss Prevention (DLP) register of the types of data and information to be monitored must be identified, documented, and approved.
1-4	The legal, regulatory, operational and commercial obligations placed on <organization name> must be reviewed at least once a year.
1-5	Where required, the DLP register of data and information to be monitored must be updated to reflect changes identified in the review.
1-6	The vectors by which data and information can exit/transfer from <organization name> must be investigated. The investigation must prioritize the data and information listed in the DLP register.
1-7	A list of the vectors such as network (email clients, file transfer protocol (FTP) clients and similar), systems (data recorders, printers, removable storage and similar) and applications by which data and information contained in the DLP register can exit/transfer from <organization name> must be created and maintained.
1-8	The list of vectors must be reviewed at least once a year.
1-9	Where required, the list of vectors must be updated to reflect changes identified in the review.

2	Data Loss Prevention (DLP) tool
Objective	To deploy a DLP tool to monitor and control the movement of data and information listed in the DLP register
Risk implication	Not automating the monitoring of data and information will result in <organization name> having to use manual processes (or no process at all) to find and stop data and information leakage, reducing the effectiveness and efficiency of data leak prevention approaches
Requirements	
2-1	The DLP tool must be managed centrally.
2-2	Access to the DLP tool must be restricted and limited to authorized employees, using physical and logical access controls in accordance with <organization name> approved Physical Security Policy and Identity and Access Management Policy.
2-3	An owner for the DLP tool must be appointed in accordance with relevant policies approved by <organization name>.
3	DLP tool configuration
Objective	To configure a DLP tool to monitor and control the movement of data and information listed in the DLP register
Risk implication	Incorrect configuration of the DLP tool may result in data and information being leaked outside <organization name>
Requirements	
3-1	The DLP tool must be configured to identify all data and information listed in the DLP register, where technically feasible.

3-2	DLP tool must be configured to monitor and control the movement of data listed in the DLP register using technical DLP policies, defining a set of DLP tool rules, including: a) what data can and cannot be sent, posted, uploaded, moved or copied and pasted. b) where data can be transmitted. c) how data can be shared.
3-3	The DLP tool must be configured to scan known vectors of data loss.
3-4	The DLP tool must be configured to use one or more of the following detection techniques: a) content matching b) indexing or fingerprinting c) optional character recognition d) other detection techniques as provided by the tool
3-5	The DLP tool must be configured to enforce the DLP tool rules by one or more of the following mechanisms: a) blocking the transmission of data and information listed in the DLP register b) quarantining messages before transmission c) blocking copy and paste to external storage devices d) logging all violations
3-6	The DLP tool must be configured to provide alerts to authorized employees when a breach of the DLP tool rules occurs.
3-7	Responses to alerts from the DLP tool must occur within an agreed timeframe.
3-8	The DLP tool must be configured to inform users of a breach of the DLP tool rules.
3-9	The DLP tool configuration must be reviewed at least once every six month.

3-10	Where required, the DLP tool must be updated to reflect changes identified in the review.
3-11	Where possible, the DLP tool must be integrated with the SIEM tool.
4	DLP Logging
Objective	To collect information on the functioning of the DLP tool and to ensure the tool is functioning as intended.
Risk implication	Lack of logging may result in poor understanding of how the DLP tool is performing, whether the tool is performing as desired or expected and a lack of data for assurance and audit purposes.
Requirements	
4-1	The DLP tool must log all actions and activities.
4-2	The DLP tool logs must be stored in a secure location, with access limited to authorized employees, using physical and logical access controls.
4-3	The DLP tool logs must be retained according to retention requirements in accordance with related policies approved by <organization name>.
4-4	The integrity of DLP tool logs must be protected and assured (e.g. by using encryption, digital time stamps or other tamper-evident methods of integrity protection).
4-5	The logs produced by the DLP tool must be reviewed and analyzed at least once a month.
4-6	Where required, information from the DLP tool logs must be used to improve DLP tool functioning, provide evidence of data and information loss, provide evidence of success in stopping data and information loss, or to highlight new vectors of data and information loss.

5	Information Asset Data Loss Prevention
Objective	To reduce the likelihood of data and information in physical format being lost.
Risk implication	Loss of information in physical format can lead to exposure or breach, resulting reputational damage, and depending on the information asset lost, in legal and regulatory investigations and fines.
Requirements	
5-1	Classified information assets in physical format (papers, hard copies, contracts, etc.) classified as “Restricted” or above must not be removed by individuals from <organization name> premises.
5-2	Classified information assets in physical format (papers, hard copies, contracts, etc.) considered as personal data must not be removed by individuals from <organization name> premises.

Roles and Responsibilities

1- **Standard Owner:** <head of the cybersecurity function>
2- **Standard Review and Update:** <cybersecurity function>
3- **Standard Implementation and Execution:** <information technology function>
4- **Standard Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard at least once a year or in the event of fundamental technical changes in the infrastructure or in case

any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1- The <head of the cybersecurity function> will ensure compliance of <organization name> with this standard on a regular basis.

2- All personnel at <organization name> must comply with this standard.

3- Any violation of this standard may be subject to disciplinary action according to <organization name>'s procedures.