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 organization logo by clicking on the placeholder to the

Data Cybersecurity 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 data protection for <organization name>. This standard is intended to define a set of cybersecurity controls to ensure the data protection of <organization name> information assets.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) including but not limited to (ECC-1:2018 and CSCC-1:2019, and DCC-1:2022) in addition to other related cybersecurity legal and regulatory requirements.

Scope

This standard covers all <organization name>'s information technology assets and applies to all personnel (employees and contractors) in <organization name>.

Standards

1	Identity and Access Management
Objective	The objective of this section is to ensure secure logical access to data assets in order to prevent unauthorized access and allow only authorized access.
Risk Implication	Improper management of data access may cause unauthorized access to critical data, which can lead to data damage, data loss, or data theft.
Requirements	
1-1	User authorization must be based on identity and access control principles, which are: • Need-to-Know, • Need-to-Use,

	• Least Privilege. • Segregation of Duties.
1-2	All access to data must be controlled using identification and authentication mechanisms. This access control must: a) Assign privileges to individuals based on the individual's job classification and function. b) Restrict privileges to the minimum needed for the individual or service to perform their duties. c) Deny all access that is not explicitly granted. d) Remove all system access not explicitly required. e) Review user's identities and access rights periodically.
1-3	Device, service, and application accounts must be assigned to an account owner and must not be used by individuals to access the related device, service, or application. These accounts and their associated passwords must be managed by the enterprise privileged account management tool.
1-4	All accounts must be reviewed upon changes in user role and at least annually for user accounts or user groups which handle public and confidential data. Privileged accounts and service accounts, or accounts which handle secret and top-secret levels of data must be reviewed every 6 months.
2	Data and Information Privacy
Objective	The objective of this section is to ensure, that privacy requirements of data and information are implemented.
Risk Implication	Insufficient or lack of data privacy practices may lead to unauthorized access to confidential data, which may result in data leak or data loss.
Requirements	

2-1	<Organization name> must consider privacy at the initial design stages and throughout the complete development process of new systems, applications, databases, products, processes, or services that involve processing personally identifying information (PII).
2-2	Privacy by Design must be embedded into the design and architecture of IT systems processing personally identifying information (PII) to ensure that current, new or changes to the systems that collect, or process personally identifying information (PII) satisfy requirements.
2-3	When applicable, <Organization name> must apply suitable data pseudonymization / anonymization techniques to meet the requirements of Privacy by Design principle.
2-4	The default system settings must be the most privacy friendly (data minimization principle), if a system or service includes choices for data subjects on how much personally identifying information (PII) is shared.
2-5	<Organization name> must put appropriate technical and organizational measures in place to ensure, that only necessary personally identifying information (PII) are processed by default.
2-6	Security controls outlined in this document must be aligned with the privacy requirements. <Organization name> should have a separate policy/standard/requirement for data privacy.

3	Data in Transit Encryption
Objective	The objective of this section is to define the encryption requirements of specific data, based on its classification, risk assessment results, and use case.
Risk Implication	Improper or lack of encryption of data in transit may lead to sending confidential data - Intentionally or unintentionally - to someone who has no legitimate access to it or sharing it publicly.
Requirements	
3-1	<organization name> must use encryption on all critical systems data during transfer (Data-In-Transit), using updated and secure encryption methods, algorithms, and keys in accordance with relevant National Cryptographic Standards.
3-2	Encryption must be used if electronic personally identifiable information (PII) is transmitted (through, but not limited to, e-mail, (SSH) File Transfer Protocol (SFTP), instant messaging, e-fax, Voice Over Internet Protocol (VoIP).
3-3	Encryption (with the use of WPA (Wi-Fi Protected Access) or higher level cryptographic protocol) must be used if connecting to the internal network(s) over a wireless network.
3-4	Encryption must be used if remotely accessing an <organization name>'s internal network(s) or devices over a shared (e.g., Internet) or personal (e.g., Bluetooth, NFC) network. This does not apply to remote access over an <organization name>'s managed point to point dedicated connection.
3-5	Encryption must be used if data is being transmitted with an <organization name> public facing website and/or web services, they are required to utilize Hypertext Transfer Protocol Secure (HTTPS) in lieu of Hypertext Transfer Protocol (HTTP) where technically feasible. Public facing websites must utilize (HTTP)

	Strict Transport Security (HSTS), automatically redirecting (HTTP) requests to (HTTPS) websites where technically feasible.
3-6	<organization name> must use appropriate encryption methods for data in transit including, but are not limited to, Transport Layer Security (TLS) 1.2 or later, Secure Shell (SSH) 2.0 or later, Wi-Fi Protected Access (WPA) version 2 or later (with Wi-Fi Protected Setup disabled) and encrypted Virtual Private Networks (VPNs) as prescribed by NCA in (NCS-1:2020). Components should be configured to support the strongest cipher suites possible.
4	Encryption in Data at rest
Objectives	The objective of this section is to ensure that encryption of data is based on its classification, risk assessment results, and use case.
Risk Implication	Improper or lack of encryption of data at rest may lead to data leaks, unauthorized access to data, public disclosure of confidential information.
Requirements	
4-1	<organization name> must use encryption all critical system data during storage (Data-At-Rest) at the file, database, or specific column level, within the database, using updated and secure encryption methods, algorithms, and keys in accordance with relevant National Cryptographic Standards.
4-2	Encryption must be used on the systems listed below: a) desktops that access or contain personally identifiable information (PII) or sensitive information.

	b) data stores (including, but not limited to, databases, file shares) that contain PII or sensitive information. c) all mobile devices, no matter if they were issued by <organization name> or third-party, that access or contain any <organization name> information or sensitive information. d) all portable storage devices containing any <organization name> information or sensitive information. e) PII is transported or stored outside of the <organization name> facility or sensitive information.
4-3	Full disk encryption must be used for all issued laptops that access or contain <organization name> information. Full disk encryption tools must use either pre-boot authentication that utilizes the device's Trusted Platform Module (TPM), or Unified Extensible Firmware Interface (UEFI) Secure Boot.
4-4	Laptops and third-party laptops that access or contain (PII) or sensitive information must be powered down when outside of the <organization name> facilities, (i.e., shut down or hibernated) when unattended, to mitigate attacks against encryption keys.
4-5	<organization name> must have a process in place for confirming, that devices and media being used have been successfully encrypted using at least one of the following (listed in preferred order): a) automated policy enforcement. b) automated inventory system. c) manual record keeping.
5	Media Disposal

Objective	Information systems which capture, process, and store information using a wide variety of media, including paper may require special disposal, in order to mitigate unauthorized access to data and to ensure its confidentiality.
Risk Implication	Inadequate or lack of data sanitization practices are exposing the <organization name> to the risk of data breach, data disclosure, unauthorized access to confidential information.
Requirements	
5-1	<organization name> must perform the clearing of data with overwriting data as a sanitization method, in case the media will be reused and will not be leaving the <organization name>'s control in order to prevent information to be retrieved by data, disk or file recovery utilities.
5-2	<organization name> must use purging data as sanitization method if the media will be reused and will be leaving the <organization name>'s control, in order to protect confidentiality of information against an attack through either degaussing or secure erase.
5-3	<organization name> must physically destroy data as a sanitization method, if the media will not be reused at all, in order to completely destroy the media.
5-4	It must be documented: ● When the destruction of data took place ● Who executed the destruction of data ● The evidence must be stored in accordance with the agreed retention period.
5-5	<organization name> must decide which sanitization process is being used, based on the classification and associated

	confidentiality level of the information, not the type of media. The type of sanitization must be approved by the Data Owner.
6	Controls Against Financial and Reputational Risks
Objective	To ensure the confidentiality, integrity and availability of <organization name>'s data and information as per organizational policies and procedures and related laws and regulations, in order to avoid financial and reputational damage.
Risk Implication	Stolen and claimed "as genuine" documents (without watermarks), data leakage, and mishandling of sensitive and personal data can cause financial and reputational damage.
Requirements	
6-1	<organization name> must use watermark feature to label the whole document when creating, storing, printing, or displaying the document on the screen and making sure each copy of the document has a traceable number.
6-2	<organization name> must use Data Loss Prevention techniques.
6-3	<organization name> must prohibit the use of sensitive and personal data in any environment other than the production environment. Exception must be only granted after applying strict controls to protect that data of <organization name> by using appropriate techniques, such as: data masking or data scrambling.
7	Other Standards
Objective	The Data Protection must be securely deployed and used appropriately when required.
Risk Implication	Failure to meet all security standards and requirements increases the security risks for data protection.

Requirements	
7-1	The following standards must be implemented in relevance to Data protection: 1. Cryptography Standard 2. Network Security Standard 3. Physical Security Standard 4. Backup and Recovery Standard

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 employees 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.