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 Cybersecurity Policy Template

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.

Choose Classification

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

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 policy aims to define the cybersecurity requirements related to the data cybersecurity in <organization name> to achieve the main objective of this policy which is minimizing cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

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

Scope

The policy covers all data held by <organization name> and stored, processed and transmitted by information and technology assets; and applies to all <organization name> personnel (employees and contractors).

Policy statements

1- General requirements

1-1 <organization name> must comply with the laws and regulations pertaining to data protection in the Kingdom of Saudi Arabia; and <organization name> policies and procedures.

1-2 <organization name> must set and update, on a regular basis, data cybersecurity requirements.

1-3 <organization name> must ensure data cybersecurity requirements is managed efficiently in accordance with the <organization name>'s Cybersecurity in Human Resources Policy and Asset Management Policy.

1-4 <organization name> must ensure the protection of mobile devices as per the <organization name>'s mobile devices security policy.

1-5 <organization name> must use Data Leakage Prevention technology/solutions.

1-6 <organization name> must prohibit the use of <organization name>'s data in any environment other than the production environment, except after conducting a risk assessment and applying controls to protect that data, such as: data masking or data scrambling techniques.

1-7 <organization name> must identify the techniques, tools and procedures for the implementation of secure data disposal according to the classification level.

1-8 <organization name> must develop and implement exist strategy to ensure means for secure disposal of data on termination or expiry of the contract with the cloud service provider.

1-9 <organization name> must ensure the proper and efficient use of cryptography techniques to protect <organization name>'s data as per the approved <organization name>'s cryptography policy and standard, and related laws and regulations.

1-10 <organization name> must identify roles and responsibilities to ensure data cybersecurity in relevance with legal and regulatory requirements.

1-11 <organization name> must use secure means to export and transfer data and virtual infrastructure.

1-12 <organization name> must prohibit the transfer of any critical systems data from production environment to any other environment.

1-13 <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.

1-14 Key performance indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of cybersecurity requirements for data protection.

2- Classification and Secure Handling of Information

2-1 <organization name>'s data must be classified according to the approved <organization name> Data Classification Policy.

2-2 All <organization name>'s data must be classified in all formats:

1-1-1 Digital (such as word documents, spreadsheets, presentations and databases).

1-1-2 Electronic communications (such as email messages, voice communication services and teleconferencing).

1-1-3 Physical (such as printouts, hard copies of contracts and notebooks).

1-1-4 Spoken (such as meetings, interviews and phone calls).

2-3 Individuals must avoid discussing <organization name>'s data in spoken formats in public areas, or in areas they might be overheard. Spoken discussions should occur in <organization name> premises and in secure locations within the premises.

2-4 All data held by <organization name> on all systems (including critical systems) and cloud systems must be classified and labelled according to all relevant legal and regulatory requirements, as well as the approved Data Classification policy in <organization name>.

2-5 Data owners appointed by <organization name>, working with the relevant stakeholders within <organization name>, must be responsible for classifying data as described in this policy.

2-6 Any violation of this policy and data classification controls must be reported to the relevant stakeholders within of <organization name> immediately.

2-7 Remote access controls on data must be enforced and implemented as per <organization name>'s identity and access management policy.

2-8 Classified data (Secret, Top secret) must not be stored on portable storage devices such as external hard drives or USB sticks, regardless of the level of encryption used on the portable storage device.

2-9 Classified data (Top secret, Secret) must not be input, processed, changed, stored or transmitted on employee-owned devices — termed Bring Your Own Device (BYOD)—, unless that data is the data of the employee.

2-10 Classified data (e.g., Secret, Top secret), that can be accessed, processed, stored or transmitted through telework systems must be protected.

2-11 The subset of classified data (e.g., Secret, Top secret), that can be accessed, processed, stored or transmitted through telework systems must be identified in accordance with the relevant regulations.

2-12 Technology assets for management of <organization name>'s social media accounts must not contain classified data, as per relevant regulations.

3 Retention of records

3-1 <organization name> must retain records of consent given by data owners and must retain records of withdrawal or revocation of consent for the length of time specified by law or regulation.

3-2 <organization name> must keep a record of all secure data disposal operations that have been executed.

3-3 <organization name> must retain data for the length of time specified by law or regulation or until the sensitive information is no longer required for the purpose for which it was collected.

3-4 <organization name> must create a record of processing activities, update it when required and retain copies for the length of time specified by law or regulation.

3-5 Identifying retention period for all systems-associated data, in accordance with relevant legislations. Only required data must be retained in the production environment.

Roles and Responsibilities

1- **Policy Owner:** <head of cybersecurity function>

2- **Policy Review and Update:** <cybersecurity function>

3- **Policy Implementation and Execution:** <data protection function> and <cybersecurity function>

4- **Policy Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the policy at least once a year or in case any changes happen to the policy or the regulatory procedures in <organization name> or the relevant regulatory requirements.

Compliance

1. <Head of cybersecurity function> will ensure the compliance of <organization name> with this policy on a regular basis.
2. All personnel at <organization name> must comply with this policy.
3. Any violation of this policy may be subject to disciplinary action according to <organization name>'s procedures.