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 outlined image.

Corporate Cybersecurity Policy 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 policy aims to document the overall corporate cybersecurity requirements of <organization name>, to achieve the main objective of this policy which is to be the base for all cybersecurity policies, procedures, and standards, as well as an input to <organization name>'s internal processes, such as the processes of human resources, vendor management, project management, change management, etc.

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

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

Policy Statements

1 <cybersecurity function> must define and develop cybersecurity policies, technical standards, regulatory frameworks, and procedures and methodologies, based on the results of risk assessments, and in a manner that ensures circulating cybersecurity requirements and the compliance of <organization name> with them as per its business regulatory requirements in <organization name> and other relevant legal and regulatory requirements. These policies must be approved by <head of organization> and circulated to <organization name>'s concerned personnel and relevant parties. The above includes**:**

1-1 **Cybersecurity Strategy** to create cybersecurity action plans, objectives, initiatives, programs, and projects and ensure their effectiveness within <organization name> to achieve strategic objectives and meet the relevant legal and regulatory requirements.

1-2 **Cybersecurity Policies and Procedures** to ensure the documentation and circulation of cybersecurity requirements and the <organization name>'s compliance with them as per its business regulatory requirements and other relevant legal and regulatory requirements.

1-3 **Cybersecurity Roles and Responsibilities** to ensure that roles and responsibilities are clearly defined for all the parties involved in implementing cybersecurity controls in <organization name>.

1-4 **Cybersecurity Risk Management Methodology** to ensure that cybersecurity risks are methodically managed to protect <organization name>’s information and technology assets as per <organization name>’s regulatory procedures and policies and other relevant legal and regulatory requirements.

1-5 **Cybersecurity Awareness and Training Program** to ensure that <organization name>'s personnel have the necessary cybersecurity awareness and understand their cybersecurity responsibilities while ensuring that they are provided with the skills, qualifications, and specialized training that fit their field of work in <organization name> and that are required in the field of cybersecurity, to protect <organization name>’s information and technology assets and carry out their cybersecurity responsibilities.

1-6 **Cybersecurity in Information Technology Projects Policy** to ensure that cybersecurity requirements are included in <organization name>’s project management methodology and procedures to protect the confidentiality and integrity of its information and technology assets in <organization name> and ensure their accuracy and availability, as well as ensure the implementation of cybersecurity standards in application and program development activities, as per <organization name>’s regulatory procedures and policies and other relevant legal and regulatory requirements.

1-7 **Cybersecurity Regulatory Compliance Policy** to ensure that <organization name>'s cybersecurity program is aligned with the relevant legal and regulatory requirements.

1-8 **Cybersecurity Periodical Assessment and Audit Policy** to ensure that <organization name>'s cybersecurity controls are applied and follow <organization name>’s regulatory procedures and policies, as well as other relevant national legal and regulatory requirements, and the international requirements applicable to <organization name>.

1-9 **Cybersecurity in Human Resources Policy** to ensure that the cybersecurity risks and requirements relating to <organization name>’s personnel are effectively addressed before, during, and at the end of their employment, as per <organization name>’s regulatory policies and procedures and other relevant legal and regulatory requirements.

1-10 **Asset Management and Asset Acceptable Use Policies and Standard** to ensure that <organization name> has an accurate and up-to-date inventory of assets detailing all information and technology assets available to <organization name> to support its operational processes in <organization name> and cybersecurity requirements, to preserve the confidentiality, integrity, accuracy, and availability of <organization name>'s information and technology assets.

1-11 **Identity and Access Management Policy and Standard** to ensure the cybersecurity protection of logical access to <organization name>'s information and technology assets to prevent unauthorized access and restrict access to what is needed to accomplish <organization name>’s business.

1-12 **Information System and Processing Facilities Protection Policy** to ensure the protection of <organization name>'s information systems and processing facilities, including workstations and infrastructures, against cybersecurity risks.

1-13 **Email Protection Policy and Standard** to ensure that <organization name>'s email is protected against cybersecurity risks.

1-14 **Networks Security Management Policy and Standard** to ensure that <organization name>'s networks are protected against cybersecurity risks.

1-15 **Server Security Policy and Standard** to ensure that <organization name>'s servers are protected against cybersecurity risks.

1-16 **Patch Management Policy and Standard** to ensure the management of patches for <organization name> systems, applications, databases, network devices, and information processing devices, and mitigate cybersecurity risks and protect the organization against internal and external threats.

1-17 **Mobile Devices Security Policy and Standard** to ensure the protection of <organization name>'s mobile devices (including laptops, smartphones, and smart tablets) against cybersecurity risks, and the safe handling and protection of <organization name> classified and business information during transmission, storage, and removal, and when using the personal devices of <organization name> personnel (BYOD principle).

1-18 **Data and Information Protection Policy and Standard** to ensure the protection of the confidentiality, integrity, accuracy, and availability of <organization name>’s data and information, as per its regulatory procedures and policies and other relevant legal and regulatory requirements in <organization name>.

1-19 **Cryptography Policy and Standard** to ensure the proper and effective use of cryptography to protect <organization name>’s information and technology assets, as per its regulatory procedures and policies in <organization name> and other relevant legal and regulatory requirements.

1-20 **Database Security Policy and Standard** to ensure that <organization name>’s databases are protected against cybersecurity risks and internal and external threats.

1-21 **Backup and Recovery Management Policy and Standard** to ensure the protection of <organization name>’s data and information and its system and application in <organization name> configuration from damages caused by cybersecurity risks, as per its regulatory procedures and policies in <organization name> and other relevant legal and regulatory requirements.

1-22 **Vulnerabilities Management Policy and Standard** to ensure the timely detection and effective remediation of technical vulnerabilities to prevent or minimize the probability of exploiting them to launch cyberattacks against <organization name>, as well as minimizing potential impacts on <organization name> business.

1-23 **Penetration Testing Policy and Standard** to assess the effectiveness of the monitoring team and systems in detecting and testing potential threats against <organization name>, by simulating actual cyberattack techniques and methods, discovering unknown vulnerabilities, and assessing the effectiveness of the monitoring systems and team in detecting potential threats, which may lead to <organization name>’s cyber penetration, as per the relevant legal and regulatory requirements.

1-24 **Cybersecurity Event Logs and Monitoring Management Policy and Standard** to ensure automatic and timely collection, analysis, storage, and monitoring of cybersecurity event logs, for the early detection of potential cyberattacks and effective management of risks to prevent or minimize potential negative impacts on <organization name>'s business.

1-25 **Cybersecurity Incident and Threat Management Policy and Standard** to ensure the timely identification and detection and effective management of cybersecurity incidents, and the proactive handling of potential cybersecurity threats, to prevent or minimize potential negative impacts on <organization name>'s business.

1-26 **Anti-Malware Security Policy and Standard** to ensure that the workstations, mobile devices, and servers of <organization name> are protected against malware.

1-27 **Physical Security Policy and Standard** to ensure that <organization name>'s information and technology assets are protected against unauthorized physical access, loss, theft, and destruction.

1-28 **Web Application Security Policy and Standard** to ensure that <organization name>’s internal and external web applications are protected against cybersecurity risks.

1-29 **Cybersecurity Resilience Aspects of Business Continuity Management Policy** to ensure the inclusion of cybersecurity resilience requirements within <organization name>’s business continuity management, and to remediate the impacts of the disruptions affecting critical e-services and minimize them for

<organization name> and its information processing systems and devices as a result of disasters caused by cybersecurity risks.

1-30 **Third-party Cybersecurity Policy** to ensure the protection of <organization name>'s information and technology assets against third-party cybersecurity risks, including information technology outsourcing and managed services, as per <organization name>'s regulatory procedures and policies and other relevant legal and regulatory requirements.

1-31 **Cloud Computing and Hosting Cybersecurity Policy** to ensure addressing cybersecurity risks and properly and effectively implementing the cybersecurity requirements related to cloud computing and hosting, as per <organization name>'s regulatory procedures and policies, legal and regulatory requirements, and relevant orders and resolutions. This policy also ensures the protection of <organization name>'s information and technology assets on cloud computing services that are hosted, processed, or managed by a third party.

1-32 **Cybersecurity Industrial Controls Systems Policy** to ensure that cybersecurity is properly and effectively managed, and protect the availability, integrity, and confidentiality of <organization name>'s Operational Technologies (OTs)/Industrial Control Systems (ICS) and protect them against cyberattacks (e.g., unauthorized access, destruction, spying, and manipulation) as per <organization name>'s cybersecurity strategy, cybersecurity risk management, regulatory cybersecurity requirements that are legally applicable to <organization name>.

2 <cybersecurity function> has the right to access the needed information and collect the necessary evidence to ensure compliance with the relevant legal and regulatory requirements**.**

3 Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and effective and efficient use of the protection requirements of information and technology assets.

Roles and Responsibilities

1- To ensure the commitment and support of <organization name>'s authorized official regarding the management and implementation of cybersecurity programs and related requirements in <organization name>, the following list represents the needed roles and responsibilities to approve, implement, and adopt cybersecurity policies, procedures, standards, and programs:

1-1 **Authorized official's responsibilities, <organization name's head or his/her representative>, include the following:**

1-1-1 Establish a cybersecurity steering committee with <head of cybersecurity function> as a member.

1-2 **<cybersecurity supervisory committee>'s responsibilities include the following:**

1-2-1 Approve <organization name>'s cybersecurity policies and requirements.

1-3 **<legal organization>'s responsibilities include the following:**

1-3-1 Ensure that cybersecurity terms and requirements and non-disclosure clauses are legally binding in the contracts of the personnel in <organization name> and in third parties.

1-4 **<internal audit and assessment organization>'s responsibilities include the following:**

1-4-1 Review cybersecurity controls and audit their implementation as per the generally accepted auditing standards and other relevant legal and regulatory requirements.

1-5 **<Information Technology organization>'s responsibilities include the following:**

1-5-1 Implement the cybersecurity requirements related to technology assets in <organization name>.

1-6 **<human resources organization> responsibilities include the following:**

1-6-1 Implement the cybersecurity requirements related to <organization name>'s personnel.

1-7 <cybersecurity function>'s responsibilities include the following:

1-7-1 Develop cybersecurity policies, obtain the approval of <organization name's head or his/her representative> on cybersecurity policies, ensure that the stakeholders are informed of them and implement them, and review and update them periodically.

1-8 **Responsibilities of other heads include for example:**

1-8-1 Support cybersecurity policies, procedures, standards, and programs, and provide all required resources to achieve the desired goals and serve <organization name>'s public interest.

1-9 **The responsibilities of the personnel include the following:**

1-9-1 Knowing <organization name>'s cybersecurity requirements for the personnel and complying with them.

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- The authorized official <organization name's head or his/her representative> must ensure compliance with the cybersecurity policy and related requirements.

2- <head of cybersecurity function> will ensure the compliance of <organization name> with cybersecurity policies and related requirements on a regular basis.

3- All personnel of <organization name> must comply with this policy and related requirements, unless there is an official prior exception from the

<head of cybersecurity function> or the Cybersecurity Supervisory Committee, provided that such exception does not conflict with the relevant legal and regulatory requirements.