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

Insert organization logo by clicking on the outlined image.

Compliance with Cybersecurity Legislation and Regulations 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 legal 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 compliance requirements for <organization name>. The requirements in this policy 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), in addition to other related cybersecurity legal and regulatory requirements.

Scope

This policy covers all systems and procedures in the <organization name> and applies to all personnel (employees and contractors) in the <organization name>.

Policy Requirements

1- Define and document a list of local and international legislation and regulations related to cybersecurity and relevant requirements applicable to <organization name> on a continuous basis once changed or once new requirements are issued. Should there be any locally approved international agreements or obligations that include cybersecurity requirements, they must be added to the list.

2- Comply with all local and international legislation and regulations, as well as clauses of cybersecurity agreements and obligations, that apply to <organization name>.

3- Provide the necessary technologies to verify compliance with the requirements of legal and regulatory authorities related to cybersecurity.

4- Review cybersecurity policies and procedures with cybersecurity legislation and contract clauses annually.

5- Monitor compliance of external service providers with cybersecurity legislation and contract clauses on a continuous and permanent basis.

6- Ensure implementation of cybersecurity policies and procedures annually.

7- Ensure compliance with requirements related to cybersecurity through the use of appropriate tools, including but not limited to:

- Cybersecurity Risk Assessment activities.
- Vulnerability Management activities.
- Penetration Test activities.
- Review of cybersecurity standards.
- Security Source Code Review.
- User surveys.
- Stakeholder interviews.
- Review of privileges on the system and network.
- Review of cybersecurity logs and events.

8- Define and implement the necessary corrective measures to correct the gaps for all compliance requirements by stakeholders.

9- Implement appropriate procedures to ensure compliance with legal and regulatory requirements, related to intellectual property rights and the use of software.

10- <Organization name> Cybersecurity Function must review the implementation of Cybersecurity Controls on a regular basis.

11- Cybersecurity Function must review the implementation of Critical Systems Cybersecurity Controls at least once a year.

12- Review and audit implementation of cybersecurity controls in <organization name> by parties that are independent from the Cybersecurity Function (such as the <internal audit function> at <organization name>). Review and audit must be carried out independently, taking into account the principle of non-conflict of interests, as per the general standards accepted for review and auditing as well as the relevant legal and regulatory requirements.

13- Document and present the results of cybersecurity review and audit to the cybersecurity steering committee and representative of parties independent from cybersecurity function (e.g. <internal audit function> in the <organization name>). As well, results must also include the scope of review and audit, observations, recommendations and corrective measures, as well as feedback remediation plan.

14- Review CSCC implementation by parties independent of the cybersecurity function from <organization name> at least once a year.

15- Use KPI in a proper and effective manner to ensure continuous improvement and proper and effective use of cybersecurity compliance program requirements.

Roles and Responsibilities

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

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

3- **Policy Implementation and Execution:** <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- The <head of the cybersecurity function> will ensure 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 as per <organization name>'s procedures.