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 entity logo by clicking on the image shown.

Cybersecurity Review and Audit Policy Template

Replace <organization name> on behalf of the entity for the entire document. To do this, follow the below steps:

- Press "Ctrl" and "H" keys at the same time.
- Add "< organization name>" in the Find text box.
- Enter the full name of your destination in the "Replace" text box.
- Click on "More" and make sure "Match case" is selected.
- Click "Replace All".
- Close the dialog.

Choose Classification

Date:	Click here to add a date
Version:	Click here to add text
Reference:	Click here to add text

Disclaimer

This template has been developed by NCA as an illustrative example that can be used by entities as reference and a 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 entity 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

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

Document Copies

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 text

Table of Contents

purpose 4
Scope 4
General Items 4
Roles And Responsibilities 6
Update And Review 6
Compliance 6

Purpose:

This policy aims to define the cybersecurity requirements related to the cybersecurity controls review and audit adopted at <organization name> and ensure their implementation and that they are aligned with <organization name>'s policies and regulations as well as relevant legal and regulatory requirements and international requirements imposed as per the regulations on <organization name>.

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 cybersecurity controls in <organization name> and applies to all personnel (employees and contractors) in <organization name>

Policy Statements

1 General Requirements

1-1 The <Cybersecurity function> in <organization name> must review and audit the implementation of cybersecurity controls adopted by <organization name> at least once a year, and review compliance with the cybersecurity controls issued by the National Cybersecurity Authority (NCA) that applies to <organization name>.

1-2 Cybersecurity review and audit procedures must be defined, documented, and applied.

1-3 <organization name> cybersecurity controls implementation must be reviewed and audited periodically by parties of <Cybersecurity function> such as <Internal Audit Function> or third party in accordance with relevant legal and regulatory requirements.

1-4 Implementation of cybersecurity controls for critical systems must be reviewed at least once a year by <Cybersecurity function> and every three years by parties independent of <Cybersecurity function>, such as <Internal Audit Function> or third party in accordance with relevant legal and regulatory requirements.

1-5 The <Cybersecurity function> must review the implementation of data cybersecurity controls (DCC-1:2022) according to their classification. Controls of data classified as (public and restricted) must be reviewed at least once every 3 years. Whereas controls of data classified as (secret and highly confidential) must be reviewed at least once a year in accordance with relevant legal and regulatory requirements.

1-6 Implementation of data cybersecurity controls (DCC-1:2022) must be reviewed by parties that are independent of <Cybersecurity function> but from <organization name> as per the period specified for each level. Implementation of controls for data classified as (public and restricted) must be reviewed once every 5 years at least. Whereas implementation of controls for data classified as (secret and highly confidential) must be reviewed at least once every 3 years in accordance with relevant legal and regulatory requirements.

1-7 The <Cybersecurity function> in <organization name> must review implementation of ICS/OT cybersecurity controls (ECC-1:2018) at least once a year.

1-8 Implementation of ICS/OT cybersecurity controls must be reviewed by parties that are independent of <Cybersecurity function> in <organization name> at least once every 3 years in accordance with relevant legal and regulatory requirements.

1-9 Cybersecurity review and audit results must be documented and discussed with the relevant functions.

1-10 Results must be presented to the cybersecurity steering committee and the representative. Result must include the scope of review and audit, observations, recommendations and corrective actions as well as risk assessment and remediation plan.

1-11 The following RACI Chart must be adopted for implementation of cybersecurity review and audit processes:

	<External Auditor>	<Internal Audit>	<Cybersecurity function>	<Head of the cybersecurity function>	<head of cybersecurity committee at the organization>	<Organization Head>
Cybersecurity Review	R		R	A	I	I
Cybersecurity Audit	R	R	I	I	A	I

Implement corrective actions	C/I	C/I	R	R	A	I

1-12 Key performance indicators (KPI) must be used to ensure the continuous improvement and effective and efficient use of cybersecurity requirements of review and audit requirements.

Roles and Responsibilities

1. **Policy Document Owner:** <Head of Cybersecurity function>.
2. **Policy Review and Update:** <Cybersecurity function>.
3. **Policy Implementation and Implementation:** <IT Function>.
4. **Policy Compliance Measurement:** <Cybersecurity function>.

Update and Review

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

Compliance

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