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.

Cybersecurity Incident and Threat Management 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 4
Scope 4
Policy Statements 4
Roles and Responsibilities 10
Update and Review 10
Compliance 10

Purpose

This policy aims to define the cybersecurity requirements related to cybersecurity incident and threat management at <organization name> to minimize cybersecurity risks and protect it against internal and external threats by focusing on key security objectives namely; confidentiality, integrity, and availability.

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 (TCC-1:2021), in addition to other related cybersecurity legal and regulatory requirements.

Scope

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

Policy Statements

1- General Requirements

1-1 The <organization name> must establish the required mechanisms to timely identify and detect cybersecurity incidents in <organization name> to effectively manage reports received from personnel or beneficiaries.

1-2 The <organization name> must proactively handle cybersecurity incidents by adopting defensive mechanisms to prevent or mitigate the impacts on confidentiality, integrity, or availability.

1-3 Incident response plan must be documented and approved to establish procedures to address any cyber-attack, defining response team roles and responsibilities, defining decision making authority, and establishing interaction mechanism with internal and external stakeholders as well as incident escalation plan.

1-4 Cybersecurity incident response capabilities, readiness level, and approved plan must be tested periodically through Attack Simulation Exercises.

1-5 Provide organization's personnel (employees and contractors) with the required skills and training to effectively respond to cybersecurity incidents.

1-6 Examples of cybersecurity Incidents shall include but not limited to:

1-6-1 Unauthorized changes in workstations configurations – both desktops and/or laptops and server's configurations.

1-6-2 Malware infections.

1-6-3 Changes in applications in terms of appearance (unusual appearance) in addition to modifications in user's privileges

1-6-4 Unauthorized access to data or modification of data without authorization or user's privileges.

1-6-5 Attempts to gain information that may be used to initiate an attack (Port Scans, Social Engineering attacks, targeted scans across IP range, etc.).

1-6-6 Unauthorized activation of suspended or deleted user accounts.

1-7 Cybersecurity incident response plans must be aligned with the IT incident response plans, crisis management and business continuity plans.

1-8 In case of telework, cybersecurity incident response plans and contact information must be updated within the organization in line with the status of telework, ensuring communication capability and readiness of incident response teams

1-9 In case a cybersecurity incident is detected in <organization name>, the incident response team must immediately take the necessary steps to handle the detected incident by analysing the incident data and determining its impact.

1-10 If a cybersecurity incident is detected, relevant available information such as system and network logs, logs from relevant security products (e.g. logs from malware protection solutions, firewall, and advanced intrusion detection and prevention protection systems) must be analysed.

1-11 Necessary evidence (e.g. evidence collection in accordance with legal constraints and evidence protection against unauthorized tampering) must be handled, documented and maintained securely to preserve its merits. Such evidence must be analysed without damage or modification to its original form.

1-12 In case a cybersecurity incident is detected, the cause of cybersecurity incident must be investigated, supported by specialists, such as digital forensics analysts and cyber incident response teams.

1-13 The incident response plans, capabilities and readiness, must be reviewed at least once a year.

1-14 Cybersecurity incidents must be classified according to severity level and impact on <organization name>'s business

1-15 Cybersecurity incidents must be classified according to the relevant legal and regulatory requirements as per the table below:

TABLE 1: CYBERSECURITY INCIDENTS CLASSIFICATION

Severity Level	Definition	Target Response Time	Target Incident Resolution Time
Catastrophic	Catastrophic failures of services or negative impact on national cybersecurity that result in or threaten to cause serious economic or social complications or lead to death of certain people.	<To be determined by organization> Immediate	<To be determined by organization> Immediate
Critical Incident	Gross threat or damage to image, reputation or credibility of <organization name>, multiple business	Immediate	<To be determined by organization>

Choose Classification

Severity Level	Definition	Target Response Time	Target Incident Resolution Time
	functional units getting severely impacted, location of business critically affected, and business continuity measures would have to be invoked.		2 hours
High Incident	Severe outage affecting single business functional units, key services or location.	<To be determined by organization> 1-2 Hours	<To be determined by organization> 4-5 hours
Medium Incident	Moderate degradation to business functional units, locations, IT assets in addition to moderate to high impact to non-critical business units within in <organization name>.	<To be determined by organization> 2-3 hours	<To be determined by organization> 8-9 hours
Limited Incident	Affecting few resources and the issue can be tolerated for a particular period of time.	<To be determined by organization> 5 hours	<To be determined by organization> 24 hours

1-16 Key performance indicators (KPI) must be used to ensure the continuous improvement as well as proper and effective use of Cybersecurity Incident and Threat Management requirements

2- Cybersecurity Incidents Reporting

2-1 Raise security awareness of <organization name>'s personnel and define their cybersecurity incidents and threats responsibilities to promptly report any cybersecurity incident or threat.

2-2 The <organization name> must establish point of contact (POC) for reporting incidents internally, be it a phone number or email address.

2-3 The <organization name> must specify which incident or threat to be reported, when and to whom they are reported. The parties most commonly notified include <representative>, <head of cybersecurity function>, incident response teams within the <organization name>, and information and technology assets owners.

2-4 Prior to disclosure of information about security incidents to third parties, approvals must be obtained according to the relevant legal and regulatory requirements.

2-5 Report cybersecurity incidents to NCA once detected.

2-6 Share incident reports and breach indicators and reports with NCA.

3- Incidents Response and Recovery

3-1 Incident response team in < organization name> must create a detailed cybersecurity incident report. The report must include incident type and category, personnel who reported it, tools used in detecting the incident, service/assets/information affected, how they were detected, and any relevant supporting documents.

3-2 Analyse and update Root Cause Analysis of cybersecurity incidents and develop plans to address them.

3-3 If needed, involve vendors to resolve the incident and/or restore the service.

3-4 Implement and execute cybersecurity incident and threat recommendations and alerts issued by the sector supervisor or NCA.

3-5 Cybersecurity incident recovery procedures must identify vulnerabilities exploited and apply the necessary remediation technical and administrative measures, including but not limited to

3-5-1 Implement compensating controls.

3-5-2 Deploy updated security patches.

3-5-3 Restore system backup versions.

3-5-4 Reconfigure security devices including firewalls and intrusion detection systems.

3-6 The <organization name> must safeguard incident reports (which includes data about security intrusions and incidents such as information about individuals, organizations, specific systems and/or attack methodology) and restrict access to it.

3-7 The incident, if not resolved and corrected within the pre-defined timeframes, must be escalated as per the classification of security incidents and incidents escalation rules and procedures.

3-8 Any changes to technology components required to resolve an incident, must be performed in accordance with the <organization name>'s Change Management Process.

3-9 The incident response team at <organization name> must hold a "lessons learned" meeting with all involved functions after a major incident to reflect on how to better handle future incidents and how to proactively handle them to prevent or mitigate impacts on <organization name>'s business.

4- Threat Intelligence Feeds

4-1 Subscribe with authorized and trusted cybersecurity resources "Threat Intelligence" to collect information about new cybersecurity threats and incidents and act immediately.

4-2 Store and organize the collected threat intelligence feeds in a knowledge base such as wikis which are quite flexible and suitable for developing working notes and indicator metadata.

4-3 Update Intrusion Prevention and Detection Systems to ensure their capability of detecting such threats based on threat intelligence feeds.

4-4 Subscribe with Telework-related threat Intelligence providers with to collect information and deal with such information periodically.

Roles and Responsibilities

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

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

3- **Policy Implementation and Execution:** <information technology 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- The <head of the cybersecurity function> will ensure compliance of <organization name> with this policy on a regular basis.

2- All personnel of <organization name> must comply with this standard.

3- Any violation of this policy may be subject to disciplinary action as per <organization name>'s procedures.