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.

Cybersecurity Event Logs and Monitoring 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 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 event logs and monitoring management systems of <organization name> in order to minimize the cybersecurity risks resulting from internal and external threats 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

This policy covers all event logs management and cybersecurity monitoring systems of <organization name> and applies to all personnel (employees and contractors) In <organization name>. This standard must follow the NCA's operating model for cybersecurity operation centers and NCA's regulatory cybersecurity requirements.

Policy Statements

1- General requirement

1-1 Risk level monitoring systems must be aligned with NCA' regulatory cybersecurity requirements, in order to collect and analyse event logs, and to collect cyber event logs for information assets, systems and applications, databases and networks, and protection systems in <organization name>. These logs must contain the following information as a minimum:

1-1-1 Event type.

1-1-2 Source of event (IIS, EDR, AV, Sysmon, security logs, etc...).

1-1-3 System from which the event was performed (e.g. mail server).

1-1-4 Date and Time of Event.

1-1-5 The user or the tool used to perform the event.

1-1-6 Event status or outcome (Success vs. Failure).

1-2 Activate and combine Event Logs, Audit Trial and Login of all relevant technical assets as per risk log of <organization name>, including CTS, Critical Systems, OT, Tele work systems and Social Media Accounts Information Assets pursuant to the relevant legal and regulatory requirements.

1-3 Protect cybersecurity event logs against unauthorized change, disclosure, destruction, access and release. Also, event logs of all activities must be protected to support digital forensics processes, if needed, as per the relevant legal and regulatory requirements.

1-4 Use Automatic Control Means necessary to monitor event logs.

1-5 Monitor Access Control Points between network boundaries and external communications.

1-6 Monitor all cybersecurity events 24/7/365 by specialized teams.

1-7 Monitor social media accounts and login attempts to ensure operation of systems 24/7/365, and collect relevant log.

1-8 The systems to be monitored must activate event logs when one of the following events at least occurs:

1-8-1 Cybersecurity events on all technical components of the systems to be monitored, including OT, data bases, storage, applications, and networks.

1-8-2 Cybersecurity events of industrial network and associated communications.

1-8-3 Events related to accounts that have privileged and critical access to information assets.

1-8-4 Events related to DNS Logs, Internet Connection, and Wireless Network.

1-8-5 Events related to remote access.

1-8-6 Events related to Cloud computing and hosting events.

1-8-7 Events related to information transfer through external storage media.

1-8-8 Events related to making changes to logs, critical systems files through File Integrity Management (FIM) techniques.

1-8-9 Events related to system, network, or service configuration changes, including downloading patches, or other changes to installed software.

1-8-10 Events related to suspicious activities, such as activities detected by Intrusion Prevention System (IPS).

1-8-11 Events related to User Behaviour Analytics (UBA).

1-8-12 Events related to multiple and unsuccessful access attempts.

1-8-13 Events related to connection of new or unauthorized devices to the critical system networks and industrial control systems (OT/ICS).

1-9 Key performance indicators (KPI) must be used to ensure the continuous improvement as well as proper and effective use of Cybersecurity Event Logs and Monitoring Management requirements.

Roles and Responsibilities

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

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

3- **Policy Implementation and Execution:** <information technology 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.