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.

Physical Security 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 <organization name>'s physical security in order to minimize cybersecurity risks resulting from internal and external threats at <organization name> and 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 facilities, information and technology assets, equipment and devices in the <organization name> and applies to all personnel (employees and contractors) in the <organization name>.

Policy Statements

1 General Requirements

1-1 All <organization name>'s physical assets and facilities must be inventoried and classified as per <organization name>'s approved Data and Information Classification Policy.

1-2 Access to critical areas (e.g., data centers, recovery centers, data processing centers, monitoring centers, network communication rooms, and supply areas for devices and technical component) must be controlled and restricted to authorized individuals only.

1-3 Suitable operational procedures must be developed, approved, and applied to grant physical access to <organization name>'s facilities based on the principles of Need-to-know, Need-to-access, and Least Privilege. Moreover, access privileges must be reviewed and audited periodically.

1-4 Detectors of metal and hazardous materials must be used for access to critical areas at <organization name>.

1-5 Access to and exit from critical areas must be logged, and records must be retained and protected in accordance with <organization name>'s approved Data Protection Cybersecurity Policy.

1-6 Access to and exit from critical areas must be monitored using technologies such as closed-circuit television (CCTV) according to the legal and regulatory requirements approved by <organization name>, and such access must be monitored continually by specialist personnel.

1-7 Procedures for secure destruction, reuse, and disposal of physical assets containing classified information (including paper documents and storage media) must be developed, and a record of destructed or reused assets must be maintained.

1-8 Infrastructure hardware, in particular storage equipment, must be securely disposed in accordance with the relevant legal and regulatory requirements.

1-9 Security controls must be developed, implemented, and reviewed to protect devices and equipment inside and outside <organization name>'s premises based on their classification.

1-10 Emergency response procedures and evacuation plans for the <organization name>'s buildings and facilities must be developed and implemented in the event of any suspected or actual physical or environmental incidents to ensure the safety of <organization name>'s personnel and critical assets.

1-11 Emergency response procedures and evacuation plans must be reviewed periodically at least once a year.

1-12 Procedures to support and maintain physical assets and equipment must be developed and implemented in accordance with <organization name>'s approved equipment maintenance security standards.

1-13 Cybersecurity security risks must be assessed to detect any security threats, safety threats, and weaknesses that <organization name> may face and address them to protect information assets from being exposed to such threats, as per <organization name>'s approved risk management methodology and the relevant legal and regulatory requirements.

1-14 Physical security capabilities and readiness must be tested <once a year> by conducting simulation drills (e.g., social engineering).

1-15 Attendance of <organization name>'s classified meetings must be restricted to authorized personnel only, and attendees of such meetings must go through security screening and inspection.

1-16 Third parties must only be granted access to <organization name>'s facilities after fulfilling security requirements, and their access must be monitored. They must be escorted wherever required for the duration of their presence.

1-17 Physical access management privileges must be restricted to personnel with specific privileges and must be audited and reviewed periodically in accordance with <organization name>'s approved Identity and Access Management Policy.

1-18 Access, storage, and transmission of backup content of critical systems and media must be secured and protected against unauthorized destruction, modification, or access.

1-19 A Clear Desk Policy must be implemented, and documents, information technology devices, or external storage devices must not be left accessible to unauthorized persons.

1-20 <cybersecurity function> must ensure that all personnel have the required knowledge about physical security best practices, such as the duties and responsibilities assigned to them, and ensure their compliance with such practices.

1-21 Physical assets containing classified information must be securely destroyed.

1-22 Key Performance Indicators (KPIs) must be used to ensure the continuous improvement and efficient and effective use of physical security protection requirements.

2 Controls for the Protection of Audio, Communications, Network, and Power Cables Against Physical Damage

Controls must be implemented to protect audio, communications, network, and power cables against physical damage, after examining potential cybersecurity risks. Such controls must cover the following at a minimum:

2-1 Communication and data network cables must be protected against wiretapping.

2-2 Communication and data network cables must not be installed in areas accessible to third parties.

2-3 Communication and data network cables must be protected and isolated securely to protect them against damage or unauthorized interception and ensure that they are installed through secure and protected areas.

2-4 Electrical and power cables must be isolated from communication and data network cables.

2-5 Uninterrupted Power Sources (UPS) must be used to support the continuous operation of critical systems and sites (e.g., data centers).

Roles and Responsibilities

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

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

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

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

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