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

Insert organization logo by clicking on the outlined image.

Physical Security Standard 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 standard aims to define the detailed cybersecurity requirements related to the physical security of <organization name>'s premises, buildings and assets to minimize cybersecurity risks resulting from internal and external threats at <organization name> in order to preserve confidentiality, integrity and availability.

The requirements in this standard are aligned with the cybersecurity requirements issued by the National Cybersecurity Authority (NCA) in addition to other related cybersecurity legal and regulatory requirements.

Scope

These standard covers <organization name>'s premises, buildings and assets in <organization to add in physical locations as appropriate, such as data centers, offices and warehouses> and applies to all <organization name> personnel (employees and contractors).

Standards

1	Physical Premises Protection
Objective	To protect physical premises from harm.
Risk implications	Physical premises, buildings and assets can be subject to theft or physical damage, resulting in the loss of assets, data and information, or interruption to services provided by the assets.
Requirements	
1-1	The roles of personnel (including employees, visitors and other individuals) who are allowed to access buildings where <organization name> data centers, network devices or application servers are located, must be defined. This

	includes buildings owned or managed by <organization name>, business units and third parties.
1-2	The locations requiring physical access controls must be identified and documented, including all areas classified as critical, or areas containing systems or data classified as critical.
1-3	A process to control access to <organization name> physical premises, buildings and assets must be defined and reviewed periodically.
1-4	The process in 1-3 must include the following minimum requirements: a) personnel requiring access must have a valid employment contract, contractor's agreement, or work order b) how a request for physical access is to be submitted (paper form, email, ticketing system, etc.) c) what the business need is for physical access d) the time frame, schedule or period, required for physical access e) who can request physical access (e.g., <organization name> personnel) f) who can authorize the requested physical access g) how long a request for physical access would take to be approved or denied h) what mechanism would be used to escort or otherwise track the individual granted physical access i) how the request for the physical access is recorded in a secure manner j) how approved physical access requests are stored, and subsequently checked on persons' arrival at a controlled location k) the validity period of access to be granted

1-5	All physical access events to <organization name> physical premises, buildings and assets must be recorded when they occur.
1-6	Physical access rights must be reviewed at least once a year to verify that access to physical premises, buildings and assets remains appropriate and valid.
1-7	A review must be conducted to confirm, change or revoke physical access at least once a year. Collected log data may be used in this review.
1-8	A review must be conducted to confirm, change or revoke physical access to locations hosting critical systems at least once every six months. Collected log data may be used in this review.
1-9	Inactive physical access permissions must be revoked after an agreed time period based on the criticality of the system.
1-10	Visitors who have been granted temporary physical access to physical premises, buildings and assets must be registered and physically supervised by authorized personnel (this includes <organization name> personnel from other <organization name> locations or divisions).
1-11	Physical access controls must be deployed (e.g. use of physical barriers, locks, window bars, reinforced doors, CCTV, restricted access to data centers located in secure buildings, use of ID cards by all visitors) to limit access to <organization name> physical premises, buildings and assets.
2	Environmental protection
Objective	To provide physical premises, buildings and assets with appropriate environmental safeguards.

Risk implication	The operation of IT systems can be adversely affected by poor, or uncontrolled, environments resulting in poor performance, errors or unexpected shutdowns.
Requirements	
2-1	<organization name> physical premises, buildings and assets must be protected by implementing the following minimum environmental control mechanism requirements: a) air conditioning b) humidity controls c) fire detection systems d) fire suppression systems appropriate for the environment.
2-2	Uninterruptible Power Supply (UPS), or similar, systems must be deployed to protect critical IT systems in the event of a power failure.
2-3	Communications and power cabling must be protected, for example by limiting access to switch rooms and network rooms, using armored cabling ducts or concealing cable runs.
2-4	The risk of natural and man-made disasters must be identified and assessed.
2-5	Mitigation measures must be selected and implemented to reduce the impact of natural and man-made disasters (e.g. flood protection, business continuity arrangements, alternative working arrangements, alternative locations) in coordination with the <business continuity function>.
3	Secure disposal
Objective	To ensure that physical IT assets are securely disposed and destroyed.

Risk implication	Insecure disposal and destruction of IT assets may expose any data or information to compromise or breach, resulting in reputational damage and, depending on the data or information exposed, legal and regulatory investigations and penalties.
Requirements	
3-1	Mechanisms must be identified and approved by <organization name> to securely dispose physical IT assets as per its classification and relevant regulatory requirements.
3-2	All physical assets that have reached end-of-life must be disposed of using the approved secure disposal mechanisms.
3-3	Physical copies of backup and storage media for IT assets must be protected from unauthorized access, destruction, or modification.
3-4	A register must be maintained by <organization name> recording all disposal activities of physical premises, buildings and assets, which must be protected from unauthorized access, destruction, or modification.

Roles and Responsibilities

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

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

3- **Standard Implementation and Execution:** <information technology function>

4- **Standard Compliance Measurement:** <cybersecurity function>

Update and Review

<cybersecurity function> must review the standard 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 standard on a regular basis.

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

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