

5.1.1 Protection of Physical Information Assets Policy

Contents

1. Definitions	2
2. Purpose	2
3. Scope	2
4. Policy	3
5. Non-compliance	4
6. References	4

Version	Adjustment Date	Approved By	Approval Date
1.0	4/7/2024	Saud Alsulami	7/7/2024

1. Definitions

For purposes of this "Protection of Physical Information Assets Policy" the following definitions apply:

- **Physical Information Assets:** refer to tangible items, documents, records, media, and equipment that contain or store sensitive or confidential information, including paper documents, backup tapes, servers, and hardware devices.
- **Security Zones:** are designated areas within physical facilities that have controlled access and security measures in place to protect information assets from unauthorized access, damage, or theft.
- **Offsite Premises:** Offsite premises refer to locations outside the organization's main facilities where physical information assets may be stored, including disaster recovery sites, remote offices, or third-party storage facilities.
- **Delivery and Loading Areas:** Delivery and loading areas are specific locations within an organization's premises where shipments, deliveries, and loading/unloading activities take place.
- **Environmental Threats:** encompass various risks posed by natural or man-made factors that can damage physical information assets. These threats may include fires, floods, power failures, equipment malfunctions, and other environmental hazards.
- **Alarm Systems:** security mechanisms that generate audible or visual alerts in response to specific security events or breaches, including unauthorized access, intrusion, or environmental hazards.
- **Motion Sensors:** Motion sensors are devices that detect physical movement within a defined area and trigger alarms or alerts when unauthorized motion is detected
- **Secure Transport Protocols:** Secure transport protocols are established procedures and measures used to ensure the safe and secure transportation of physical information assets, including packaging, tracking, and secure transportation methods.

2. Purpose

The purpose of the Protection of Physical Information Assets Policy is to establish guidelines and requirements for safeguarding physical facilities, assets, and resources that host, store, or transport information assets. This policy aims to mitigate risks associated with physical threats and environmental hazards

3. Scope

The scope of the Protection of Physical Information Assets Policy encompasses all physical facilities, on-site and off-site, that host, store, or transport information assets, including measures to safeguard against physical threats and environmental hazards to ensure the integrity and availability of information resources.

4. Policy

- 4.1. All physical facilities that host information assets, including data centers, server rooms, and storage areas, must be adequately secured and monitored.
- 4.2. Access to these facilities shall be restricted to authorized personnel only, with access controls, electronic authentication, and surveillance systems in place.
- 4.3. Physical access privileges are granted by the branch manager or the CEO, with the technical support department being responsible for their implementation.
- 4.4. Environmental controls (e.g., temperature, humidity, fire suppression) shall be implemented to protect equipment and information assets from physical damage.
- 4.5. Physical information assets stored or located on offsite premises, such as disaster recovery sites or remote offices, must receive the same level of security and protection as assets on the main premises.
- 4.6. Security measures, including access controls, alarms, and surveillance, shall be implemented to safeguard these offsite locations.
- 4.7. Periodic assessments and audits of offsite facilities shall be conducted to ensure compliance with security standards.
- 4.8. Delivery and loading areas at all organizational premises shall be controlled and monitored.
- 4.9. Loading areas shall be restricted to authorized personnel, and access shall be logged and monitored.
- 4.10. When physical information assets need to be transported, secure transportation methods and procedures shall be followed to prevent loss, theft, or unauthorized access.
- 4.11. Personnel responsible for transporting information assets shall undergo security training and adhere to secure transport protocols.
- 4.12. Physical protection measures against environmental threats, such as fire, flood, earthquake, and extreme weather conditions, shall be in place. This includes fire detection and suppression systems, environmental monitoring, disaster recovery plans, and secure storage to protect physical information assets.

- 4.13. Procedures for responding to physical security incidents, including breaches, thefts, or environmental emergencies, shall be established and documented.
- 4.14. Cables shall be secured against interception, interference, or damage, and proper cable management practices (e.g., labeling, color coding) shall be followed.
- 4.15. Physical information assets shall be operated in accordance with manufacturer-specified requirements, including controlling the working atmosphere (e.g., temperature, humidity, air quality, water, light).
- 4.16. Protection against unauthorized access shall include surveillance through CCTV, alarm systems, motion sensors, and access controls.
- 4.17. Physical information assets shall reside within appropriate security zones and be securely stored during non-operational hours to prevent unauthorized access, tampering, or theft.

5. Non-compliance

Non-compliance with this policy may result in disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

6. References

- ISO 27002
- ISO 27011
- NIST
- National Cybersecurity Authority's (NCA) ECC standards

