|  |  |
| --- | --- |
| [Organization Name] | **No:**  [Policy Number] |
| **IT Standard**:  **Physical and Environmental Security** | **Updated:** 10/28/2024 |
| **Issued By:**  [Policy Authority]  **Owner:**  [Policy Owner] |

# 1.0 Purpose and Benefits

The purpose of the Physical and Environmental Protection Policy is to safeguard the organization’s information technology resources through robust physical and environmental security measures. This policy aims to prevent unauthorized access, theft, tampering, or damage to IT assets by establishing clear guidelines for physical access control, monitoring, and emergency preparedness. By addressing these vulnerabilities, the organization seeks to create a secure environment that protects sensitive information and ensures the operational integrity of its facilities.

Implementing this policy provides numerous benefits, including enhanced security for physical IT assets, which minimizes the risk of data breaches and operational disruptions. By establishing strict access controls and monitoring practices, the organization can detect and respond to physical security incidents more effectively. Additionally, compliance with industry best practices, such as those outlined by the NIST Cybersecurity Framework, helps improve the organization’s overall cybersecurity posture. The policy also promotes a culture of awareness and responsibility among all personnel, ensuring that everyone understands their role in protecting the organization’s physical and information assets.

# 2.0 Authority

This policy is established under the authority of organizational management and is guided by best practices outlined in the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0. While not mandated by law, the organization adopts this framework to enhance its cybersecurity posture and protect its information assets. The authority for enforcement and adherence to this policy is vested in the [Policy Authority], who is responsible for ensuring compliance across all departments.

# 3.0 Scope

This policy applies to all employees, contractors, third-party vendors, and any individuals or entities accessing, using, or managing the organization's information systems, networks, and physical infrastructure, regardless of the medium or format of the information. It covers all electronic, paper-based, and verbal communication, including, but not limited to, data processing systems, cloud services, email platforms, mobile devices, databases, and other digital storage mechanisms that store, transmit, or process sensitive organizational information.

The policy encompasses internal and external users, whether they access the organization's systems on-site or remotely, and includes all physical infrastructure such as data centers, workstations, and hardware that interact with or support the organization's information environment. Additionally, it extends to any devices, both personal and organizational, that connect to the corporate network or handle company data.

All users are responsible for protecting the confidentiality, integrity, and availability of information, complying with this policy and relevant laws, and familiarizing themselves with the organization's security policies and procedures to ensure the protection of organizational assets. Failure to comply with these requirements may result in disciplinary action, including termination of access rights or contractual agreements.

# 4.0 Information Statement

The Physical and Environmental Protection Policy establishes essential measures to protect the organization’s IT resources from physical threats and environmental hazards. It applies to all employees, contractors, and third-party vendors, covering all facilities and information systems. Key components include physical access authorizations, monitoring of access points, emergency power and fire protection measures, and protocols for maintaining environmental controls like temperature and humidity. By adhering to these guidelines, all personnel are responsible for ensuring the confidentiality, integrity, and availability of organizational information, with non-compliance potentially resulting in disciplinary actions.

* 1. Physical Access Authorizations

The [Owner] shall:

1. Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.
2. Issue authorization credentials for facility access.
3. Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.
   1. Physical Access Control

The [Owner] shall:

1. Enforce physical access authorizations by verifying individual access authorizations before granting access to the facility.
2. Control ingress/egress to the facility using [entity defined physical access control systems/devices and/or guards].
3. Maintain physical access audit logs for [entity defined entry/exit points].
4. Provide [entity defined security safeguards] to control access to areas within the facility officially designated as publicly accessible.
5. Escort visitors and monitors visitor activity in [entity specified areas].
6. Secure keys, combinations, and other physical access devices.
7. Inventory [entity defined physical access devices] every [entity defined frequency].
8. Change combinations and keys [entity defined frequency] and/or when keys are lost, combinations are compromised, or individuals are transferred or terminated.
   1. Facility Penetration Testing

The [Owner] shall employ a penetration testing process that includes [entity defined frequency], unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.

* 1. Access Control for Transmission Medium

The [Owner] shall control physical access to [entity defined information system distribution and transmission lines] within entity facilities using [entity defined security safeguards].

* 1. Access Control for Output Devices

The [Owner] shall:

1. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.
2. Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.
   1. Monitoring Physical Access

The [Owner] shall:

1. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.
2. Review physical access logs [entity defined frequency] and upon occurrence of [entity defined events or potential indications of events]; and coordinate results of reviews and investigations with the organizational incident response capability.
   1. Visitor Access Records

The [Owner] shall maintain visitor access records to the facility where the information system resides for [entity defined time period]; and reviews visitor access records [entity defined frequency].

* 1. Power Equipment and Cabling

The [Owner] shall:

1. Protect power equipment and power cabling for the information system from damage and destruction.
2. Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.
   1. Emergency Shutoff

The [Owner] shall:

1. Provide the capability of shutting off power to the information system or individual system components in emergency situations.
2. Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorized activation.
   1. Emergency Power

The [Owner] shall:

1. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; transition of the information system to long-term alternate power in the event of a primary power source loss.
2. Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.
   1. Emergency Lighting

The [Owner] shall:

1. Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
2. Provide emergency lighting for all areas within the facility supporting essential missions and business functions.
   1. Fire Protection

The [Owner] shall:

1. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.
2. This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.
   1. Temperature and Humidity Controls

The [Owner] shall:

1. Maintain temperature and humidity levels within the facility where the information system resides at [entity defined acceptable levels].
2. Monitor temperature and humidity levels [entity defined frequency] to include alarms or notifications of changes potentially harmful to personnel or equipment.
   1. Water Damage Protection

The [Owner] shall:

1. Protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.
2. This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.
   1. Delivery and Removal

The [Owner] shall:

1. Authorize, monitor, and control entering and exiting the facility and maintain records of those items delivered and removed from facility.
2. Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.
   1. Alternate Work Site

The [Owner] shall:

1. Employ [entity defined security controls] at alternate work sites.
2. Assess as feasible, the effectiveness of security controls at alternate work sites.
3. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.
4. Alternate work sites may include, for example, other government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. Staff may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

# 5.0 Compliance

This policy shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the following process.

# 6.0 Policy Exceptions

Requests for exceptions to this policy must be submitted to the [Authority] by the requesting department. Each request should include the scope and justification for the exception, potential risks, proposed mitigation measures, and a timeframe for achieving compliance. The [Authority] will review and discuss these requests with the department.

# 7.0 Definitions of Key Terms

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Information Systems | Any combination of hardware, software, data, and personnel that processes, stores, or transmits information, including but not limited to computers, servers, networks, and applications. |
| Users | Individuals or entities, including employees, contractors, and third-party vendors, who access or interact with the organization’s information systems and data. |
| Mobile Devices | Computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and is portable (i.e., non-stationary). These devices come in the forms such as: smartphones, PDAs, smart watches, tablets, laptops, and wearable devices. |
|  |  |

# 8.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

[Policy Owner’s Contact Info]

[Organization Address]

# 9.0 Review and Revision

This policy should be reviewed at least annually to keep pace with evolving regulations, threat landscapes, and organizational changes. However, more frequent reviews may be necessary following regulatory updates, cybersecurity incidents, significant technology changes, organizational shifts, or compliance audits. This policy should be revised based on these reviews and those revisions noted below.

|  |  |  |
| --- | --- | --- |
| **Date** | **Description of Change** | **Reviewer** |
|  |  |  |

# 10.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-116 – Guidelines for the Use of PIV Credentials in Facility Access](https://csrc.nist.gov/pubs/sp/800/116/r1/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-78-5 – Cryptographic Algorithms and Key Sizes for Personal Identity Verification](https://csrc.nist.gov/pubs/sp/800/78/5/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-76-2 – Biometric Specifications for Personal Identity Verification](https://csrc.nist.gov/pubs/sp/800/76/2/final)

[National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-46 – Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security](https://csrc.nist.gov/pubs/sp/800/46/r2/final)