IT PHYSICAL SECURITY POLICY

Date Added: 09/05/2024

Date Amended:

Status:
Active/Archived

IT Physical Security Policy		
This Policy provides governance to safeguard physical IT infrastructure, data, and related resources from unauthorized access, damage, or theft.	Author	
	Policy #	
	Effective Date	

TEMPLATE INSTRUCTIONS AND NOTE (DELETE BEFORE PUBLISHING)

- Text in red is highlighted for Organization-specific updates

1. Purpose

The purpose of this Policy is to establish <Organization's> expectations for safeguarding physical IT infrastructure, data, and related resources from unauthorized access, damage, theft, or environmental hazards.

2. Scope

This Policy applies to:

1. All Workforce Members, including but not limited to employees, contractors, consultants, officers, board members, and temporary personnel.
2. All IT assets and physical facilities housing IT systems, including data centers, server rooms, workstations, network equipment, mobile devices, and storage media.
3. Third-party vendors and contractors with physical access to IT infrastructure.

<Organization> may create location– or business unit–specific policies, procedures, standards, and processes to address physical security concerns. These additional guidelines are extensions to this Policy and require compliance from all applicable Workforce Members.

3. IT Physical Security Policy

3.1 Access Controls

1. Physical access to IT infrastructure, including server rooms, data centers, and networking closets, shall be restricted to authorized personnel only.
2. Multi-factor authentication (e.g., key cards and PINs) must be required for entry into sensitive IT areas.

3. All access attempts must be logged and monitored for auditing purposes.
4. Visitors must be escorted by authorized personnel and logged in an access register.
5. Access permissions must be reviewed and updated regularly to ensure they align with job responsibilities.

3.2 Facility Security

1. Critical IT infrastructure must be housed in secure, locked rooms with restricted access.
2. Surveillance systems (e.g., CCTV cameras) must monitor entry points and key physical infrastructure areas.
3. Environmental controls (e.g., HVAC systems, smoke detectors, fire suppression systems) must be implemented to prevent environmental hazards.
4. Backup power supplies (e.g., UPS systems) must be in place to ensure continuous operation of critical systems.

3.3 Equipment Security

1. IT equipment must be physically secured to prevent theft, tampering, or damage.
2. Portable devices (e.g., laptops, tablets, USB drives) must be secured when unattended.
3. Devices containing ePHI (electronic Protected Health Information) must be encrypted and securely stored when not in use.
4. Decommissioned IT equipment must undergo secure data wiping or destruction following NIST standards.

3.4 Workstation Security

1. Workstations must be locked or logged off when unattended.
2. Users must not leave sensitive information visible on screens or printed materials.
3. Public or shared workstations must be configured to prevent unauthorized data access.
4. Physical workstation layouts must minimize unauthorized shoulder-surfing risks.

3.5 Incident Response for Physical Security Breaches

1. Incident Response for Physical Security Breaches
2. All physical security breaches or suspicious activities must be immediately reported to the IT Security Team.
3. An incident report must be created and documented for each security event.
4. Physical security incidents must follow the procedures outlined in the Security Incident Response Policy.

4. Responsible Parties

1. <Director of Information Services>: Responsible for overseeing the implementation and enforcement of this policy.
2. <IT/Security Team>: Responsible for monitoring physical security controls and addressing incidents.
3. <Facilities Management Team>: Responsible for maintaining physical infrastructure security and environmental controls.

5. Policy Exceptions

Exceptions to information security policies may be granted in unusual and unique circumstances when it is not possible to comply with a specific policy. Exception requests must be made by submitting a written request to the <Director of Information Services or Responsible Individual>.

The <Director of Information Services or Responsible Individual> must document within the written approval the mitigating controls that must be followed for the exception, along with the reasonable time period for which the exception is granted.

In case of uncertainty as to the ability to approve an exception because of mandatory legal or regulatory requirements, the Exception requests must be made by submitting a written request to the <Director of Information Services or Responsible Individual> must consult with Legal.

6. Compliance

The <Director of Information Services or Responsible Individual> will employ multiple methods, tools, and processes to monitor and assess whether security controls and measures have been implemented and are being followed.

Non-compliance with this policy will result in notifications to the employee and management. Further consequences may include disciplinary action up to and including termination of employment (with cause) and/or legal proceedings to recover any loss or damage to <Organization> and possibly third parties affected.

7. Applicable Laws/Regulations/Legal Requirements

Supports the following regulations and standards:

- HIPAA §164.310(a)(1): Facility Access Controls
- HIPAA §164.310(b): Workstation Use
- HIPAA §164.310(c): Workstation Security
- HIPAA §164.310(d): Device and Media Controls

8. Referenced Documents

Document	Description	Links
Network Security Policy	Defines secure management of network infrastructure.	<insert link>
Acceptable Use Policy	Outlines the acceptable use of information resources, including workstations, information systems, applications, equipment, or other resources that may store confidential information.	<insert link>
Security Incident Response Policy	Outlines the scope, responsibilities and guidelines for responding to security incidents within the organization.	<insert link>

7. Revision History

Version	Date	Author	Description of Change
0.01			Initial draft