Cybersecurity Policy Templates

Physical Security Management Policy

(Last Updated April 2025)

Purpose

Our Physical Security Policy aims to establish a comprehensive framework for protecting the physical assets, facilities, and infrastructure that house our organization's critical systems, data, and networks. This policy aims to provide clear guidelines and procedures for implementing robust physical security measures, including access controls, surveillance systems, and incident response protocols, to mitigate the risk of unauthorized access, theft, damage, or disruption to our physical assets. By implementing effective physical security practices, this policy seeks to safeguard our information assets' confidentiality, integrity, and availability, minimize the potential impact of physical security incidents, and ensure the continuous operation of our systems and services. Through integrating physical and cybersecurity controls, we strive to create a secure and resilient environment that protects against both digital and physical threats while maintaining the trust and confidence of our stakeholders.

Scope

The Physical Security Policy applies to all employees, contractors, visitors, and stakeholders accessing our organization's physical premises, facilities, and assets. This policy encompasses implementing and maintaining measures to protect the physical infrastructure and assets from unauthorized access, theft, damage, and tampering. It covers areas such as building access controls, video surveillance, visitor management, secure storage, disposal of sensitive information, and the protection of server rooms, data centers, and other critical physical locations. The policy sets guidelines for physical security assessments, incident reporting, and response procedures. Compliance with this policy is mandatory for all individuals within the organization, and any deviations or exceptions require approval from the designated authority responsible for physical security and cybersecurity governance.

Safeguards

To achieve the organization's overall mission, and the purpose of this cybersecurity policy, the organization shall:

PHY-01 Maintain a documented physical security program for the organization that documents the safeguards it will implement to address physical security.

PHY-02 Define a process the organization shall use to monitor and detect violations of the organization's physical security program.

PHY-03 Ensure that the organization's documented physical security program defines safeguards for securely disposing of physical assets.

PHY-04 Ensure that the organization's documented physical security program defines safeguards for perimeter access controls to the organization's facilities.

PHY-05 Ensure that the organization's documented physical security program defines safeguards for authorizing, identifying, and monitoring visitors at the organization's facilities.

PHY-06 Ensure that the organization's documented physical security program defines safeguards for addressing internal physical access controls at the organization's facilities.

PHY-07 Ensure the organization's documented physical security program defines safeguards for securely handling physical access devices (such as keys or cards).

PHY-08 Ensure that the organization's documented physical security program defines safeguards to visibly mark the classification level of the organization's technology assets.

PHY-09 Ensure that the organization's documented physical security program defines environmental safeguards to protect the organization's facilities and technology assets.

PHY-10 Ensure the organization's documented physical security program defines safeguards to address access controls for physical computing devices.

PHY-11 Ensure that the organization's documented physical security program defines safeguards for how individuals can remove technology assets from the organization's facilities.

PHY-12 Ensure that the organization's documented physical security program defines safeguards and how the organization will secure unattended spaces (such as clean desk policies).

PHY-13 Ensure the organization's documented physical security program defines safeguards to secure technology assets such as printers, copiers, or multi-function devices.

PHY-14 Ensure that the organization's documented physical security program defines safeguards for logging physical access to its facilities.

PHY-15 Regularly perform physical penetration tests at each facility to ensure the organization's physical security safeguards operate as expected.

Policy Sanctions

Non-compliance with this policy may result in disciplinary action in line with our corporation's human resources procedures. Consequences may range from mandatory refresher training and written warnings to temporary suspension of remote access privileges and, in severe cases, termination of employment or contractual obligations. Individuals could be subject to legal consequences under applicable laws if violations involve illegal activities. These sanctions emphasize the critical importance of cybersecurity, the individual's role in protecting our digital assets, and the potential risks associated with policy violations. Enforcement will be consistent and impartial, with the severity of the action corresponding directly to the seriousness of the breach.