PHYSICAL SECURITY & ENVIRONMENTAL SECURITY

General Overview

Physical security elements are safeguards enacted to ensure only authorized individuals have access to various physical locations, such as corporate facilities, data warehouses, computer operation centers, and any other critical areas. Additionally, physical security also consists of the various measures put in place for protecting organizational assets, ranging from people, property, to any number of tangible goods, services or products. And with many organizations today outsourcing critical functions to data centers, managed services providers, and document storage facilities - just to name a select few - physical security has now become a critical component of one's risk assessment and risk management framework. Knowing where your assets are and how they are protected is paramount. But it's just as important to have physical security controls in place at one's corporate office, satellite offices, and any other important locations.

And another important component of physical security are the supporting environmental security controls in place. Specifically, environmental security elements are the essential measures utilized to protect physical surroundings from damaging elements, such as fire, water, smoke, electrical surges, spikes, and outages, along with any other hidden dangers. Environmental safeguards are critical in that they - along with physical security, ensure the safety of the employees, company property, and all other pertinent physical elements near the facility.

The subsequent Physical Security & Environmental Security policy and procedures document includes all necessary measures for ensuring adequate safeguards are in place at all facilities considered critical from an organizational perspective. The scope of this policy and procedure document includes the following types of facilities:

- Corporate office and regional, satellite offices.
- Data centers, co-location facilities, and managed service providers, document storage providers, warehouses, etc.
- Any other physical facility for which the subsequent policy, procedures, and checklists could be adapted to, and ultimately used for.

Physical Security & Environmental Security Policy and Procedures

Title	**[company name] Physical Security & Environmental Security Policy and Procedures**
Version	Version 1.0
Date	TBD
Language	English
Individual and/or Department Responsible for Distribution of Document	[company name] Information Technology Department
Individual and/ or Department Responsible for Timely Update of Document	[name and title]
Developed by:	[company name]
Subject	Use of Software
Approval Date	TBD
Purpose of Document	To implement comprehensive Physical Security & Environmental Security policies, procedures, and practices whereby all employees and other intended parties are readily aware of the organization's Physical Security & Environmental Security policies.
Distribution of Document	Disbursed to all employees of [company name] and available by request to all other intended parties.

1.0 Overview

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal Physical Security & Environmental Security policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 Purpose

This policy and supporting procedures are designed to provide [company name] with a documented and formalized Physical Security & Environmental Security policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of the [company name] I.T. system resources and all supporting assets. Assets are defined as the following: Something that is deemed to be tangible or intangible and that is capable of being owned, operated, maintained, and controlled to produce a stated value.

1.0 Scope

This policy and supporting procedures encompasses all system resources and supporting assets that are owned, operated, maintained, and controlled by [company name] and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (and the operating systems and applications that reside on them, both physical and virtual servers) and any other system resources and supporting assets deemed in scope.

- External system resources are those owned, operated, maintained, and controlled by any entity other than [company name], but for which these very resources may impact the confidentiality, integrity, and availability (CIA) of [company name] system resources and supporting assets.

1.0 Policy

[Company name] is to ensure that the Physical Security & Environmental Security policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Construction

The applicable facilities are to be constructed in a manner that ensures the adequate protection of all [company name] system resources and supporting assets. Specifically, this requires that the following elements meet and/or exceed all local, state, federal and country | region specific mandated guidelines pertaining to construction of a commercial facility:

- Designed and built with the use of approved architectural, mechanical, electrical and/or engineering drawings.
- Safe and secure foundation and footing that meets all stated zoning requirements.

- Proper utilities in place, such as sewer, water, gas, electric, fire protection | fire prevention, and other applicable utilities as warranted.
- Appropriate insurance in place, such as general liability, workers compensation, and other applicable insurance coverage.
- Architecturally and structurally sufficient to meet all needs of [company name].

If necessary, authorized personnel within [company name] are to contact the appropriate party for confirmation of the aforementioned elements.

Physical Security Protection Measures

The applicable facilities are to have adequate physical protection measures in place consisting of the following elements, as applicable:

- Location: Geographically located in a secure area, with appropriate markings and indications commensurate with its use. Note: Some facilities require clear identification as to what they are and their purpose, while others facilities deliberately hide their identification. Ultimately, this determination is to be made by management of the applicable facility.

- Construction: Solid construction with minimal or no physical openings that could weaken the physical structure and/or allow unauthorized access. Additionally, all doors and main entry and egress points (windows, bay doors, roof entry points, underground access points, shipping and receiving entry areas, etc.) are to be deemed of adequate physical construction.

- Physical Barricades: Physical elements that serve as barricades for protecting the physical grounds. This is a requirement for any data center or co-location facility for which [company name] system resources and supporting assets reside in. Additionally, appropriate gates, fences and other physical devices are to be utilized as necessary.

- Access Control Protection: One or more of the following protection measures regarding physical access: Electronic Access Control (ACS), biometrics (i.e., iris, palm reader, facial recognition), and/or traditional lock-and-key measures. Note: For any windows, bay doors, roof entry points, underground access points, shipping and receiving entry areas, and any other entry and egress areas that do not utilize ACS, biometrics, or lock-and-key, they are to be secured with adequate protection measures, such as using internal locks, latches, or other approved devices or mechanisms. Additionally, all access control points are to be securely closed and locked when not in use or are unattended. Access via Electronic Access Control (ACS), and biometrics (i.e., iris, palm reader, facial recognition) is only granted to authorized individuals - those who have gone through the proper provisioning process.

- Customer Information: An important component of ensuring that adequate physical security protection measures are in place is keeping track of all personnel that enter and leave a facility. Thus, all critical customer information, such as vital statistical information (i.e., name, company affiliation, contact information, date and time of entrance and departure, etc.) is to be captured, recorded, stored, and archived.

- Manned Access Control Points: For areas where individuals enter, register, and leave the applicable facility, actual personnel are to be stationed for aiding and facilitating these processes. Additionally, visitor and employee provisioning and de-provisioning systems are to be in place that documents all essential access information.

- Placing of Equipment: For all system resources and supporting assets located at a facility that handles (i.e., storing, processing and/or transmitting) sensitive data, they should be located in physically secure areas, and isolated as necessary, to avoid unauthorized access. Additionally, controls are to be in place for helping minimize the many physical and environmental threats as discussed throughout this stated policy and procedures document.

Vegetation
All vegetation (i.e., grass, shrubs, plants, etc.) is to be appropriately maintained at all time by either a licensed, bonded, and insured landscaping company or by [company name] landscape personnel. Adequate maintenance of vegetation not only improves the appearance of a facility, it also ensures that intruders or other suspicious people or elements cannot conceal themselves as easily.

Security Alarm System
A security alarm system is to be in place, operational at all applicable times as necessary, hard-wired and wireless monitoring (where applicable) for all entry and egress points throughout the facility, and other areas deemed vulnerable. Additionally, response and resolution services for the security alarm are to be a licensed, bonded, and insured third-party security alarm company and/or local police. Moreover, an appropriate party at [company name] is to be immediately notified anytime an alarm has passed its maximum threshold whereby the third-party security alarm company and/or the local police have been contacted.

Alarm Points
Both hard-wired contact points and wireless-alarm points (where applicable) are to be utilized for ensuring the security alarm system is connected to all critical entry and egress points throughout the facility and other areas deemed vulnerable. The use of glass breakers, motion detectors, voice recognition elements, if used, are to be tied into the security alarm system using approved measures.

Cameras | Monitoring | Surveillance | Recording | Archival
Cameras are to be strategically placed throughout the facility as deemed necessary and capable of capturing and recording all activity. Additionally, this requires the use of monitoring devices whereby authorized personnel can view all activity in real-time, while also recording such activity. During non-business hours or when personnel are not available for real-time viewing, recording is to be in place that allows for capturing any activity. Moreover, archival measure are to be in place (minimum of 90 days) for retention of data caught on camera.

Threat Conditions Policy
Because of the growing threats facing organizations, a threat conditions policy is to be in place which consists of documented responses and initiatives to undertake in the event of an actual threat. This may include, but is not limited, to the following:

- Threats of terrorism or hostage situations.

- Physical or environmental conditions resulting in the structural integrity of a facility being compromised which could ultimately endanger the lives of all occupants.
- Power outages, utility issues.
- Technology threats and data compromises, such as Distributed Denial of Service Attacks (DDoS), etc.

Badge Identification | Equipment Checks
Any persons entering or leaving a facility are to be checked at anytime, and at the discretion of authorized personnel, for properly identifying who they are and for items deemed suspicious that may be in their possession. Because many system resources and supporting assets can be small in size, and also costly, bag checks, body searches, pat downs, and any other checks deemed necessary, are to be employed.

Removal of Property and Security of Equipment
All property removed from a facility is to be done so with approved methods only, one that allows for documented process that records vital statistical information for such property, whether it leaves indefinitely or is being returned at a later date (for which it will then be required to be checked-in through a documented process also). Specifically, property may only be removed if approved by authorized personnel and is required to be returned (if applicable) under an agreeable and predetermined timeframe. Additionally, property, while still under the legal binding ownership of the applicable facility, is to be safeguarded at all times, must adhere to manufacture's operating policies (if applicable), with appropriate insurance in place for protecting such property.

Cages | Cabinets | Vaults
System resources, such as computer and networking systems (both the hardware | software, and supporting assets) are to be placed in secure cages, cabinets, or vaults that meet or exceed strength, rigidity, and general safety standards as required by law and/or customers. Additionally, physical access controls, such as electronic access control systems (ACS), combination locks, punch key locks, and/or traditional lock and key are to be used for protection of the applicable system resources.

Security Department and Security Staff
As necessary, the applicable facility is to have in place a formalized security department consisting of the following:

- Operates 24x7 and is responsible for controlling and monitoring facility access and ensuring compliance with access procedures.
- Is responsible for controlling the movement of materials taken out of the facility main entry and exit points, issuing photo id access badges and visitor badges and retrieving them also, along with administering the computerized access control system to permit and terminate access.
- Dedicated on-site security staff 24x7 who are responsible for proper operations and maintenance of the physical security systems, loss prevention, material movement, and security policy and procedures compliance.
- Dedicated on-site security staff 24x7 who perform the following functions:

    - Response and resolution to security alarms.
    - Customer assistance for cage lockouts and escorts.
    - Scheduled and unscheduled security inspections.

  - Enforcement of no food or drinks in certain areas.
  - Enforcement of no unauthorized photography policy.
  - Fire and safety patrol inspections.
  - Monitor intrusion security alarm systems.
  - Dispatch mobile security officers to emergencies.
  - Monitoring to prevent unauthorized access, such as tailgating.
  - Assist all individuals who have authorized access to enter the facility.
  - Controlling access to the data center by confirming identity. Issue and retrieve access badges.
  - Respond to telephone and radio communications.

Local Law Enforcement Contact Information

The posting of local law enforcement contact information (other than 911 or other emergency numbers) is to be in place whereby authorized personnel can contact authorities as necessary. This information should be made available to security staff and posted accordingly in an area where it can be easily viewed by such security staff (such as their security room).

Mantrap

Mantraps, which are common in any facility that require entrance into sensitive areas, are to be used as necessary. This often includes facilities such as data center, co-location entities, managed services providers and other related entities.

Facility Access

Only authorized personnel (i.e., employees, visitors, contractors, and other third party.) are allowed access to the applicable facility, with one's access rights commensurate for his | her roles and responsibilities. Additionally, a documented identification, provisioning and de-provisioning process and related procedures are to be in place consisting of the following measures:

- The use of a software utility, ticketing system, in conjunction with a hard-copy log report that captures all vital statistical access rights information, such as full name, contact information, company affiliation, along with date and time of entry and departure to and from the facility, and any other vital statistical information.

- For individuals who have been granted an actual access control badge - thus allowing to bypass many of the provisioning steps in place for visitors, contractors, and other third party individuals - the software utility that allows access is to be reviewed on a regular basis. The regular review is to ensure that all terminated users do not have access and access for current users is commensurate with their roles and responsibilities.

- Assignment of badge, card reader, or some of other clearly labeled form of visible identification that indicates the type of personnel they are (i.e., employees, visitors, contractors, and other third party), the type of access, duration of access (if applicable). Note: The requirement for a "clearly labeled form of visible identification" prevents unauthorized access and allows anyone within the facility to identify unescorted visitors, ultimately helping in determining if access controls have been breached. Thus, visitors, contractors, and other third party individuals are to be escorted at all times, when applicable.

- For areas deemed restricted, sensitive, classified, or any other designation whereby access is allowed only to select, authorized personnel, additional access control measures are to be in place (i.e., two-factor authentication, biometrics, etc.) for protecting [company name]'s system resources and supporting assets.

Because many facilities have shipping, receiving, delivery, and loading areas that are used on a daily basis, these areas are to have secure access control mechanisms in place, such as those described earlier under "Physical Security Protection Measures." Additionally, for facilities that have shipping, receiving, delivery, and loading areas, the following provisions are to be in place:

  - Access restricted to authorized personnel.
  - Areas that are confined for only their applicable use, with no access allowed to other parts of the facility without undertaking process access control measures.
  - Incoming and outgoing goods and products are to be inspected, tagged and labeled accordingly, recorded, and registered with an approved method.
  - Goods and products arriving at the facility are to be stored in designated areas, such as bins, holding rooms, or some other type of approved method.
  - Goods and products leaving the facility are to have correct transportation labels on them, and are to be stored in designated areas before being picked up.
  - All goods and products entering and leaving the facility are to be physically inspected for any possible security threats.
  - For a facility that receives good and products for a customer, a notification process is to be in place whereby customers are immediately contacted and informed of packages.

- The entire identification, provisioning, and de-provisioning process is to be recorded and archived for purposes of producing audit records as needed, such as for access control breaches, daily operational review activities, and for regulatory compliance requirements.

Access Control System

Access control systems, while important for physical security protection measures, ultimately ensure that only authorized individuals have access to a particular facility, with access rights being commensurate with one's roles and responsibilities. As such, access control systems are to be provisioned and deployed for any area requiring physical access into a facility - or within the facility - access to additional areas. Additionally, the access control systems are to be maintained by authorized individuals only.

Biometrics

Biometrics, while also important for physical security protection measures, ultimately ensure that only authorized individuals have access to a particular facility, with access rights being commensurate with one's roles and responsibilities. As such, biometric devices are to be provisioned and deployed for any area requiring physical access into a facility - or within the facility - access to additional areas. Additionally, the biometric devices are to be maintained by authorized individuals only. Example of biometrics include, but are not limited, to the following:

- Fingerprint and Palm Readers
- Voice Recognition

- Iris Scanners
- Signature Recognition
- Body Movement and Weight Verification Devices

Identification

Proper identification ensures that only authorized individuals are allowed access to a facility. Because of the importance of identification, only the following types are to be accepted for anyone seeking entry into a facility:

- Current, valid driver's license issued by a local, state, or federal agency.
- Current, valid identification card issued by a local, state, or federal agency.
- Current, valid military identification card.
- Current, valid government issued passport or government issued passport card.
- Current, valid facility issued identification card.

Termination Procedures

For personnel that have had their employment terminated and/or for visitors or other individuals who have had their access rights revoked, they are to be properly de-provisioned from any access to systems for which they previously had. Ultimately, this requires a documented termination process whereby authorized personnel remove users from all systems, thus denying access to any critical system resource or access to said facility.

Secure Areas

Many facilities have needs for secure areas whereby undisclosed activities are undertaken as necessary. Specifically, secure areas could be developing new formulas, working with hazardous materials, testing new technologies, or any other type of function. Because of this, only authorized individuals are to be aware of these secure areas, along with having access to them. Additionally, no devices are to be permitted into secure areas that allow for the capture and recording of events, unless authorized. This means that cellular phones, cameras, recording devices, and other similar items are not to be allowed into secure areas. Moreover, all secure areas are to be physically secured at all times with appropriate access controls, such as electronic access controls, traditional lock-and-key, biometrics, etc. Access to secure areas requires a documented approval and provisioning process, as does termination of access rights to secure areas.