**COMPANY Logo**

**Information Security Policies:** Physical & Environmental Management

Effective Date:

**COMPANY Logo**

Revised:

Approved by: CISO (or equivalent) Approved on: 00/00/20

Approved by: COO Approved on: 00/00/20

Approved by: Board of Directors Approved on: 00/00/20

# Purpose

The purpose of the Physical & Environmental Management Policy is to limit unauthorized physical access, damage, and interference to the COMPANY (“COMPANY”) premises and information. It is important that critical or sensitive information processing equipment is housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls commensurate with the identified risks.

# Scope

This policy encompasses all COMPANY sites and the conditions and restrictions necessary to provide physical security and individual secure area access. The term “Users” refers to employees, contractors, vendors, consultants, or other persons having access to COMPANY computing assets or information.

# Roles and Responsibilities

## The RACI Chart below shows the assignment of functional and cross-functional activities. The roles are as follows:

| R - Responsible is the organizational title responsible for doing the work.A - Accountable is the organizational title for who is accountable for the work being done.C - Consulted is the organizational title that provides necessary information.I - Informed is the organizational title that receives information. **Milestone or Task** | Governance / Risk Management | Chief Information Security Officer (or equivalent) | Information Security Organization / IT | Corporate (Physical) Security | Users |
| --- | --- | --- | --- | --- | --- |
| Secure Facilities | I | C | R | A | I |
| Entry Access | I | C | R | A | R |
| Environmental | I | A | R | C | I |
| Device Security | C | A | R | C | I |
| Media & Hardcopy Handling | I | A | R | C | R |
| Securing Work Areas | I | A | R | C | R |
| Removal of Equipment | I | A | R | C | R |
| Secure Disposal or Re-use of Equipment | I | A | R | C | R |
| Equipment Maintenance | I | A | R | C | I |

# Policy Statements

The Physical & Environmental Control Policy is implemented because physical access to COMPANY’s hardware and software resources must be protected and controlled.

This is accomplished via the following:

## Secure Facilities

* + 1. Corporate Security must implement physical security for offices, rooms, and facilities.
    2. Corporate Security must clearly define the security perimeter and ensure it has no gaps or blind spots.
    3. Corporate Security must ensure all external doors have adequate control mechanisms, be alarmed, and have mechanisms in place to ensure closure.
    4. The Information Security Organization must work with Corporate Security to ensure that all facilities that house information processing systems have a physical security perimeter that consists of either a manned entranceway or an automated gate.
    5. The Information Security Organization must work with Corporate Security to ensure that security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) are in place to protect areas that contain information and information processing facilities.
    6. The Information Security Organization must work with Corporate Security to control access points such as delivery and loading areas and other points where unauthorized persons may enter the premises and, if possible, isolated them from information processing facilities to avoid unauthorized access.
    7. The Information Security Organization must work with Corporate Security to ensure that offices located within secure areas remain locked when not in use.
    8. The Information Security Organization must work with Corporate Security to ensure that electronic locks control secure area doors at all times.
    9. The Information Security Organization must review the security of the Server room and other secure areas annually, taking into consideration entry arrangements, fire, cooling and ventilation, electrical capacity, equipment space requirements, data integrity and disaster recovery.
    10. The Information Security Organization must ensure secure area doors are closed after every entry or exit, and never propped open.
    11. The Information Security Organization must work with IT to ensure that new equipment is unpacked outside the secure area and no packing material is taken into the secure area. Additionally, wire clippings and other discarded material are removed from the room after installation of equipment.
    12. The Information Security Organization must work with IT to ensure that no keyboard, peripheral, storage media or access equipment is taken into or used in the secure area without the express permission of the head of the IT Department or nominated deputy. This permission is recorded on the Sign-In Sheet.

## Entry Access

* + 1. Corporate Security must implement authentication controls (e.g. swipe card plus PIN) to authorize and validate all access. An audit trail of all access must be securely maintained.
    2. The Information Security Organization must work with Corporate Security to ensure that visitors to secure areas must be supervised or cleared and their date and time of entry and departure recorded.
    3. The Information Security Organization must work with Corporate Security to ensure that visitors and non-authorized employees sign-in when entering secured areas.
    4. The Information Security Organization must regularly maintain, review, and update access rights to secure areas.
    5. The Information Security Organization must allow Secure Area access only with the express permission of the head of the IT Department or nominated deputy.
    6. The Information Security Organization must allow any COMPANY user, vendor or contractor who is not on the Access List and requires temporary Secure Area access, entrance only with approval from the head of the IT Department or nominated deputy.
    7. The Information Security Organization or IT must accompany temporary entrants to the Secure Area at all times. This precaution is followed both within and outside normal working hours.
    8. Users must ensure that visitors only be granted access for specific, authorized purposes and must be issued with instructions on the security requirements of the area and on emergency procedures.
    9. Users must control access to sensitive information and information processing facilities and restrict access to authorized persons only.
    10. Users must wear some form of visible identification and are encouraged to challenge unescorted strangers and anyone not wearing visible identification.
    11. Users must ensure that visitors are required to wear identification that is clearly visible at all times.
    12. Users must prevent 'tailgating' access by persons who are not (to their knowledge) on the Access List entering the Secure Area.

## Environmental

* + 1. The Information Security Organization must work with Corporate Security to design and apply physical protection safeguards against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster.
    2. The Information Security Organization must work with IT to protect equipment to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.
    3. The Information Security Organization must work with IT to protect equipment from power failures and other disruptions caused by failures in supporting utilities.
    4. The Information Security Organization must work with IT to provide protection from interception or damage to power and telecommunications cabling carrying data or supporting information services.
    5. The Information Security Organization must work with IT to ensure that no food or drink is brought into the Secure Area.
    6. The Information Security Organization must work with IT to ensure that no matches, lighters or other potential incendiary source is brought into the server room or other secure areas.
    7. The Information Security Organization must work with IT to ensure no cleaning materials, solvents or other inflammable material is stored in the server room or other secure areas.

## Device Security

* + 1. IT must protect COMPANY assets under their control through cost-effective physical security measures.
    2. IT must place network devices such as routers, switches, and bridges in secure locations.
    3. IT must place modems in secure locations, preferably a computer room or data center.
    4. IT must store CPUs of all servers in a secure location, preferably a centrally located computer room or data center.
    5. For CPUs with console keys, IT must remove and store the keys in a secure location.
    6. IT must password protect all servers and change the passwords on a regular basis following corporate policy.
    7. IT must use a boot-time password for computers not stored in a secure location.
    8. Where possible, Users must lock workstations in a room or an office after hours.
    9. Users must encrypt sensitive information stored on local disks of computers not stored in a secure location.

## Media & Hardcopy Handling

* + 1. IT must store all source media for operating system software, applications and license keys in a secure location.
    2. Users must protect all COMPANY software, documentation, and information by commensurate physical security controls to prevent unauthorized disclosure, destruction, or modification.
    3. Where appropriate, Users must store paper and computer media in suitable locked cabinets and/or other forms of security furniture when not in use, especially outside working hours.
    4. Users must lock sensitive or critical business information (ideally in a fire-resistant safe or cabinet) when not required, especially when the office is vacated.
    5. User must protect incoming and outgoing mail points and unattended fax machines.
    6. Users must lock (or protect from unauthorized use in some other way) photocopiers outside normal working hours.
    7. Users must immediately clear from printers, sensitive information, when printed.
    8. Users must treat directories, telephone books, and other personnel related documents as sensitive information.

## Secure Work Areas

* + 1. Users must lock away media (paper, disks, and removable devices) containing sensitive information whenever they leave their desk unattended.
    2. Users must ensure all sensitive or critical business information is not left on desks when the office is vacated.
    3. Users must log-off personal computers and computer terminals when unattended and protect by key locks, passwords or other controls when not in use.
    4. Users must set their workstations screens to “blank out” after a 3-minute period of inactivity or, if left unattended, the system must invoke a screen saver or session suspension mechanism. The user must then re-authenticate to deactivate the screen saver and resume the current session.
    5. Users must erase white boards containing Internal Use, Confidential, or Restricted Information, or take other steps to protect the information on the board.
    6. Users must immediately remove or pickup Confidential or restricted information from printers or fax machines.
    7. Users must never leave sensitive information on desk surfaces or in other places where unauthorized persons can read them, especially when leaving the office for the day or an extended period.

## Removal of Equipment

* + 1. IT must apply security to off-site equipment taking into account the different risks of working outside COMPANY’s premises.
    2. IT must ensure the use of any information processing equipment outside COMPANY’s premises is authorized by management.
    3. User must not take equipment, information or software off-site without prior authorization.

## Secure Disposal or Re-use of Equipment

* + 1. The Information Security Organization must work with IT to check all items of equipment containing storage media to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.
    2. The Information Security Organization must work with IT to physically destroy devices containing sensitive information or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

## Equipment Maintenance

* + 1. IT must correctly maintain equipment to ensure its continued availability and integrity.
    2. IT must maintain equipment in accordance with the supplier’s recommended service intervals and specifications.
    3. IT must maintain records of all suspected or actual faults, and all preventive and corrective maintenance.

# Compliance with Policies

# Use of COMPANY’s network, systems, hardware and applications represents the User’s consent to the terms of the policies described here, including consent for COMPANY to monitor and audit content and/or use. A User’s failure to comply with Information Security Policies may lead to disciplinary action to include one or more of the following:

* Oral and/or written warning or notification of violation to User(s) involved and supervisor(s)
* Suspension of network, system or application access or electronic communications privileges permanently or for a set period
* Repossession of electronic devices or hardware permanently or for a set period
* Electronic messages may be blocked or rejected if the message contains inappropriate content
* Written warning to the User’s HR file
* Suspension from work
* Education course related to the infraction paid for by the User
* Regulatory discipline or censure
* Termination of employment

Users consent by reading this policy at time of hiring and at each annual evaluation by signing an *Information Security Policy Acknowledgement* form.

# Questions

Users are encouraged to contact the Chief Information Security Officer (CISO) or the Information Security Organization with any questions or concerns. It is critical for all Users to consult supervisors and/or the Information Security Organization about “red flags” (any suspicious activities giving rise to concerns about whether such activities meet or potentially violate Information Security Policies). All Users are encouraged to raise questions or concerns if they believe an information-security risk or leak is present.

# Disclaimers

COMPANY retains the right to:

* Restrict or revoke any User’s privileges to information, equipment or systems
* Inspect, copy, remove or otherwise alter any information, program, or other system resource that may undermine these objectives
* Take any other steps deemed necessary to protect COMPANY information or information systems

This right may be exercised with or without notice to the involved users. COMPANY disclaims any responsibility for loss or damage to information or software that results from COMPANY exercising its rights under Information Security Policies.

All documents, computing assets, and communications systems assets, including the email and phone systems, physically located at or pertaining to COMPANY are the property of COMPANY. COMPANY reserves the right to examine all information stored in or transmitted by these systems, subject to applicable law. Users should have no expectation of privacy associated with personal information and information stored in, created on, or sent through the COMPANY computer and communication systems.

# Definitions

The following terms are related to this Information Security Policy:

* **Access Control List**: A list that specifies what access privileges individuals have to a facility or other physical location.
* **Authentication Controls**: To verify the identity of an individual, usually using Swipe Cards or PINs.
* **Authorization**: The granting of access to an individual.
* **Identification**: The process that enables recognition of an individual via picture badge or id number.
* **Physical Access Control**: The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.
* **PIN**: A number used to gain access to a facility or other physical location.
* **Swipe Card**: A card that stores authentication and authorization information on a magnetic strip on the card.