US Solutions Pvt Ltd. - Physical Security Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-03-29
- **Author:** IT & Infosec Department - Eleanor Vance
- **Approved By:** Franklin Meyer, Facilities Manager
- **Effective Date:** 2024-04-29
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes the importance of physical security in protecting our information assets, personnel, and facilities. This Physical Security Policy outlines the guidelines and procedures for securing our premises and preventing unauthorized access. All employees, contractors, and authorized visitors ("Users") are required to adhere to this policy.

2. Purpose

The purpose of this policy is to:

- Establish a framework for physical security measures.
- Protect Company facilities and assets from unauthorized access, theft, and damage.
- Ensure the safety and security of personnel.
- Facilitate compliance with applicable laws and regulations.
- Define the responsibilities of personnel regarding physical security.

3. Scope

This policy applies to all Company facilities, including:

- Office buildings.
- Data centers.
- Server rooms.
- Storage areas.
- Any location where Company assets are stored or personnel are present.

4. Access Control

- **Access Badges:**
    - All employees and authorized personnel must wear Company-issued access badges at all times.
    - Access badges must be used to access restricted areas.
    - Lost or stolen access badges must be reported immediately to the Facilities Department.
- **Visitor Management:**
    - All visitors must sign in at the reception desk and be escorted by an authorized employee.

    - Visitors must wear visitor badges at all times.
    - Visitor access must be logged and monitored.
- **Restricted Areas:**
    - Access to restricted areas (e.g., server rooms, data centers) must be limited to authorized personnel.
    - Restricted areas must be secured with access control systems (e.g., card readers, keypads).
    - Access to restricted areas must be logged and audited.
- **After-Hours Access:**
    - After-hours access must be authorized by the User's manager and approved by the Facilities Department.
    - After-hours access must be logged and monitored.

5. Physical Security Measures

- **Surveillance Systems:**
    - CCTV cameras must be installed in strategic locations to monitor premises.
    - Surveillance footage must be retained for a defined period.
    - Surveillance systems must be regularly maintained and tested.
- **Alarm Systems:**
    - Alarm systems must be installed to detect unauthorized entry and other security breaches.
    - Alarm systems must be regularly tested and maintained.
    - Alarm response procedures must be established and communicated to personnel.
- **Lighting:**
    - Adequate lighting must be maintained in all areas of the premises.
    - Exterior lighting must be used to deter unauthorized access.
- **Locks and Security Doors:**
    - All exterior doors and windows must be secured with appropriate locks.
    - Security doors must be used to restrict access to sensitive areas.
- **Environmental Controls:**
    - Data centers and server rooms must be equipped with environmental controls (e.g., temperature, humidity) to protect equipment.
    - Environmental controls must be monitored and maintained.

6. Asset Protection

- **Equipment Security:**
    - Company-owned equipment must be secured to prevent theft.
    - Laptops and mobile devices must be secured when not in use.
    - Sensitive documents and media must be stored securely.
- **Data Center Security:**
    - Data centers must be secured with multiple layers of physical security.
    - Access to data centers must be strictly controlled and logged.
    - Data center equipment must be protected from environmental hazards.
- **Document Security:**

    - Sensitive documents must be stored in locked cabinets or secure storage areas.
    - Documents must be shredded or destroyed securely when no longer needed.
    - Documents must not be left unattended in public areas.

7. Emergency Procedures

- **Emergency Evacuation:**
    - Emergency evacuation plans must be developed and communicated to personnel.
    - Emergency evacuation drills must be conducted regularly.
    - Emergency exits must be clearly marked and unobstructed.
- **Fire Safety:**
    - Fire extinguishers and smoke detectors must be installed and maintained.
    - Fire safety training must be provided to personnel.
    - Fire alarm systems must be regularly tested.
- **Natural Disasters:**
    - Emergency response plans must be developed for natural disasters (e.g., earthquakes, floods).
    - Emergency supplies must be stored on-site.

8. Responsibilities

- **Facilities Department:**
    - Implement and maintain physical security measures.
    - Manage access control systems.
    - Respond to security incidents.
    - Conduct security assessments.
- **IT & Infosec Department:**
    - Provide input on physical security requirements for IT systems.
    - Manage security systems related to IT infrastructure.
    - Investigate security incidents related to IT systems.
- **All Users:**
    - Comply with this Physical Security Policy.
    - Report any security incidents or concerns.
    - Protect Company assets.
    - Follow emergency procedures.

9. Legal and Regulatory Compliance

- This policy complies with all applicable building codes, safety regulations, and data privacy laws.
- Physical security measures must be consistent with legal and regulatory requirements.

10. Training and Awareness

- All Users will receive training on this Physical Security Policy.

- Regular security awareness training will be provided to reinforce physical security best practices.

11. Policy Review and Updates

- This policy will be reviewed and updated annually or as needed to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

12. Monitoring and Enforcement

- The Facilities Department will conduct regular audits to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

13. Acknowledgement

- By accessing Company facilities, Users acknowledge that they have read, understood, and agree to comply with this Physical Security Policy.

This Physical Security Policy is designed to protect US Solutions Pvt Ltd.'s facilities, personnel, and assets. By adhering to these guidelines, Users contribute to a safe and secure work environment.