

# Physical Security Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Proprietary Notice: This document contains proprietary information that is confidential in BPO Convergence Company. Disclosure of this document in full or in part, may result in material damage to BPO Convergence. Written permission must be obtained from BPO Convergence prior to the disclosure of this document to a third party.

## **Document Revision History:**

REVISION DATE	AUTHOR	REVIEWED BY	APPROVED BY	DESCRIPTION
28/06/22	Jyoti Ranjan Nayak	Rajat Ghosh	Mr.Amit Sobti	Approved
15/07/23	Jyoti Ranjan Nayak	Rajat Ghosh	Mr.Amit Sobti	Approved
22/07/24	Jyoti Ranjan Nayak	Rajat Ghosh	Mr.Amit Sobti	Approved

**Purpose:**

The purpose of this Physical Security Policy is to establish a set of guidelines and procedures to safeguard physical assets, protect personnel, and prevent unauthorized access to company facilities and sensitive areas.

**Scope:**

This policy applies to all employees, contractors, and visitors at BPO Convergence Pvt Ltd including all physical assets, premises, and systems.

**1. Access Control**

- **Entry/Exit Points:** All entrances and exits to facilities are secured using access control systems such as key cards, biometrics, or security codes.
- **Visitor Management:** All visitors must sign in at the reception, wear identification badges, and be escorted while in restricted areas.
- **Employee Access:** Employees are only granted access to areas necessary for their roles. Access rights are reviewed periodically.

**2. Physical Security Measures**

- **Surveillance:** Closed-circuit television (CCTV) cameras are placed in key areas, including entrances, exits, and sensitive zones (e.g., server rooms, data centers).
- **Security Personnel:** Onsite security personnel are available during business hours and may be extended based on the facility's needs.
- **Perimeter Security:** Fencing, gates, and other perimeter security measures are maintained to restrict unauthorized entry.

**3. Protecting Sensitive Areas**

- **Server Rooms/ Data Centers:** Access to server rooms and data centers is restricted to authorized personnel only. Visitors are prohibited from entering without prior approval and supervision.
- **Equipment Storage:** All equipment (computers, laptops, hardware, etc.) must be securely stored when not in use to prevent unauthorized access or theft.

**4. Incident Response**

- **Unauthorized Access:** Any unauthorized access attempt or suspicious behavior should be reported immediately to security or management. An investigation will be conducted to determine the cause and prevent future incidents.

- **Emergency Procedures:** Emergency response plans, including evacuation routes and procedures, are communicated to all employees. Regular drills are conducted to ensure readiness.

## **5. Data Protection and Disposal**

- **Physical Data Security:** Sensitive physical records, storage devices, and backups are stored securely in locked cabinets or rooms. Only authorized personnel have access to these items.
- **Secure Disposal:** Any sensitive materials, including hardware (e.g., hard drives, printed documents), must be securely disposed of to prevent data breaches.

## **6. Monitoring and Audits**

- **Regular Audits:** Physical security audits are performed periodically to ensure compliance with this policy. Any security gaps or vulnerabilities identified are addressed promptly.
- **Log Reviews:** Access logs from physical access control systems and surveillance recordings are reviewed regularly to detect potential security incidents.

## **7. Employee Responsibilities**

- **Identification:** Employees must always wear company-issued identification badges while on company premises.
- **Confidentiality:** Employees must not share their access credentials or allow unauthorized persons into restricted areas.
- **Security Awareness:** Employees must adhere to all security protocols and report any suspicious activity to security personnel or management.

## **8. Compliance**

- This policy must comply with applicable local, state, and federal laws, including regulations concerning employee safety, privacy, and data protection.
- Employees who fail to comply with this policy may face disciplinary action, up to and including termination.