

# Environmental Risk Management and Security Policy

(Classification and Handling -Safeguarding Sensitive and Confidential Information)

Version: 1.2

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:

Version	Date	Author	Changes Made	Reviewed By	Approval Status
1	1/1/2021	Gyan Singh	Initial creation of Environmental Security Policies and Procedures.	P.Sahoo	Approved
1.1	1/1/2022	Gyan Singh	Added flood prevention and backup power measures.	P.Sahoo	Approved
1.2	1/1/2023	Gyan Singh	Revised incident response procedures and added training requirements.	P.Sahoo	Approve

### 1. Purpose

The purpose of this **Environmental Security Policy** is to ensure the physical protection of the company's infrastructure, including systems, data storage facilities, and other sensitive equipment. This policy defines the procedures for safeguarding physical assets from environmental threats such as theft, unauthorized access, natural disasters, and other security breaches that could compromise the confidentiality, integrity, or availability of company data and operations.

### 2. Scope

This policy applies to:

- All company premises where critical infrastructure, servers, networking equipment, and storage devices are located.
- All employees, contractors, and third parties involved in accessing or managing environmental security controls.
- Physical spaces such as data centers, server rooms, and office buildings.

### 3. Definitions

- **Environmental Security:** The protection of the physical environment from external threats or hazards that may disrupt operations or compromise the confidentiality, integrity, or availability of data.
- **Critical Infrastructure:** Physical assets such as servers, storage devices, and networking equipment essential for business operations.
- **Access Control:** Mechanisms used to restrict unauthorized entry into secure physical locations.
- **Environmental Hazards:** Physical threats like fire, water damage, and electrical failures that could potentially damage company assets.

### 4. Guidelines for Environmental Security

- **Access Control:**
  - Physical access to critical infrastructure, including server rooms, data centers, and storage areas, must be restricted to authorized personnel only.
  - Use access control systems (e.g., key cards, biometric scanners) to monitor and control access.
  - Visitor access must be logged, and they must be accompanied by authorized personnel at all times.

- **Physical Barriers:**
  - Secure entry points to critical areas with locks, gates, and fences where necessary.
  - Use barriers like fireproof doors and reinforced walls for data storage and server rooms.
- **Surveillance:**
  - Implement security cameras and surveillance systems to monitor sensitive areas.
  - Security footage should be recorded and stored for at least 30 days/weeks for auditing purposes.
- **Alarm Systems:**
  - Install intrusion detection and alarm systems to alert staff of unauthorized access attempts or security breaches.
  - Set up environmental alarms (e.g., smoke detectors, temperature sensors) in areas housing critical infrastructure to prevent or mitigate damage from natural hazards.
- **Environmental Controls:**
  - Implement temperature and humidity control systems in data centers and server rooms to maintain optimal operating conditions.
  - Use fire suppression systems (e.g., sprinklers, gas-based systems) to reduce the risk of fire damage.
  - Ensure backup power systems (e.g., UPS, generators) are in place and tested regularly to maintain operations during power outages.

## 5. Risk Mitigation for Environmental Threats

- **Fire Safety:**
  - Install fire alarms and fire extinguishers at strategic locations within the organization's critical areas.
  - Ensure that fire suppression systems are in place, especially in areas containing servers or other sensitive equipment.
  - Regularly conduct fire drills and ensure employees are trained in fire emergency protocols.
  -
- **Flood Prevention:**
  - Prevent flooding by ensuring proper drainage around key infrastructure areas.
  - Place critical equipment above flood levels and install water detection systems in server rooms and storage areas.
  -
- **Power Failures:**
  - Backup power sources (e.g., generators, uninterruptible power supplies) should be tested regularly.
  - Ensure that critical infrastructure has redundancy in power sources to maintain operation during outages.
  -
- **Temperature and Humidity Control:**
  - Set and monitor optimal temperature and humidity levels for all data storage and server rooms.
  - Use monitoring systems to provide alerts in case of temperature or humidity deviations from set thresholds.

## 6. Incident Management and Response

- **Incident Reporting:**

- - Any environmental security incidents (e.g., fire, unauthorized access, power failure) must be reported immediately to the IT and Security teams.
  - The Security team will assess the incident, take appropriate action, and log the event for future review.

- **Response Plan:**

- Establish a response plan for environmental security incidents, including emergency procedures, communication protocols, and escalation paths.
- Ensure that the response plan is tested regularly (e.g., through table-top exercises or live drills).

- **Recovery:**

- Implement a disaster recovery plan (DRP) that includes physical and environmental considerations, such as data restoration from backup and the relocation of critical infrastructure if necessary.

## 7. Enforcement

- **Non-Compliance:**

- Any violations of this policy may result in disciplinary action, including suspension of access to certain areas, or termination, depending on the severity of the breach.

- **Policy Audits:**

- The Environmental Security Policy will be subject to regular audits to ensure its effectiveness and compliance with security standards