Wipro’s

Physical Security Policy

**Document Control**

|  |  |
| --- | --- |
| Function | Global Security Group (GSG) |
| Sub-function | - |
| Policy Owner | Head - Global Security Group |
| Policy Effective Date | August 1, 2002 |

**Purpose**

This policy ensures the protection of the Organization’s information assets from physical and environmental threats.

**Audience**

Organization’s employees, retainers, contractors, and service providers.

**Scope**

This policy applies to the information assets and facilities owned or managed by the Organization.

**Policy Details**

**PS.1** Physical security perimeters or zones shall be defined and implemented.

**PS.2** Physical security risk assessments shall be performed periodically.

**PS.3** The Confidentiality, Privacy and Information Security Addendums, and the Non-Disclosure Agreement (NDA) shall be signed with the physical security contractors, service providers, and suppliers.

**PS.4** Physical access to secure areas shall be controlled and managed using appropriate authentication methods.

**PS.5** Identity and access cards shall be allocated as per business requirements and shall be deactivated upon the user termination or separation.

**PS.6** Physical access shall be granted as per the Physical Security Control Procedure.

**PS.7** Physical access records shall be maintained, protected, and reviewed as per the business requirements.

**PS.8** Electronic physical access controls shall be protected from power failures.

**PS.9** Office premises shall be controlled and monitored for unauthorized intrusion using the Closed Circuit Television (CCTV), guards, and intrusion detectors.

**PS.10** The CCTV recordings shall be protected and retained as per the business requirements.

**PS.11** Visitor entry records shall be maintained, reviewed, and protected as per the business requirements.

**PS.12** Visitors shall be escorted by an employee of the Organization while visiting the office premises.

**PS.13** Photographic, video, or audio devices shall be prohibited inside the secure areas.

**PS.14** Incoming and outgoing material details shall be verified and documented.

**PS.15** Incoming materials shall be inspected before moving inside the office premises.

**PS.16** Any movement of information assets outside Organization’s premises shall be authorized by the designated personnel.

**PS.17** Information assets in transit shall be tracked and monitored.

**PS.18** Information assets shall be placed in secure areas to protect against any physical and environmental threats.

**PS.19** Power supply and communication cables shall be labelled and protected from any electromagnetic interference and damage.

**PS.20** The Organization shall ensure redundancy for power supply and telecommunications.

**PS.21** Temperature and humidity levels shall be maintained and monitored in server rooms and data centres as per the Data Center Security Standard.

**PS.22** The Uninterrupted Power Supply (UPS) systems or generators shall be installed and monitored.

**PS.23** Emergency power shut-off shall be implemented, and access shall be restricted to authorized personnel.

**PS.24** Automatic emergency lighting shall be installed and maintained for use in the event of a power outage or disruption.

**PS.25** Fire detection and fire suppression systems shall be installed and maintained in Organization’s premises.

**PS.26** Fire evacuation drills shall be performed periodically.

**PS.27** The Water Leakage Detection (WLD) system shall be installed and monitored in server rooms and data centres as per the business requirements.

**PS.28** Preventive maintenance of supporting utilities shall be performed periodically.

**PS.29** Physical security audits shall be performed periodically.

**PS.30** Physical security records shall be retained as per the Data Retention Policy.

**PS.31** Physical accesslogging and monitoring shall be enabled as per business requirements.

**PS.32** Security incidents related to physical security shall be reported as defined in the Security Incident Management Procedure.

**Definitions**

|  |  |
| --- | --- |
| **Definitions** | **Description** |
| Information Asset | Software, physical, and virtual assets used to create, store, and process information. |
| Offsite Asset | Organization information assets that are stored or maintained outside the office premises. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Uninterruptible Power Supply | An electrical system or mechanism that provides emergency power when the main power source fails. |
| Water Leakage Detection | Equipment that is used to detect water leaks and send alert to users. It primarily applies to Organizational facilities that contain system resources, including data centers, server rooms, and mainframe computer rooms. |
| Supporting Utilities | Utilities, including electricity, telecommunications, water supply, gas, sewage, ventilation, and air conditioning, which are required to support information processing facilities. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| CCTV | Closed Circuit Television |
| GSG | Global Security Group |
| NDA | Non-Disclosure Agreement |
| UPS | Uninterrupted Power Supply |
| WLD | Water Leakage Detection |

**Reference**

* Data Retention Policy
* Closed Circuit Television (CCTV) Standard
* Data Center Security Standard
* Physical Security Standard
* Identity Badging Procedure
* Physical Security Control Procedure
* Material Movement Procedure
* Asset Management Procedure
* Security Incident Management Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 28th August 2023 | Merged Physical Security Policy, Closed Circuit Television (CCTV) Policy, and Acceptable Mobile Phone Camera and Photographic Device Usage Policy.  Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Sojan O T | Sanjay Sharma | 18th January 2024 |