VU VISHWAKARMA UNIVERSITY

Maximising Human Potential

Physical and Environmental Security Policy

Vishwakarma University

Ver. No	Release Date	Owner	Approved By	Change details
1.0	19-07-2020	CISO	Vice Chancellor	Initial

Table of Contents

1. Purpose

Purpose of this policy is to physically manage controls implemented to protect information systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

2. Scope

This policy applies to information systems and related supporting infrastructure at; Vishwakarma Main Building, VU-1, Survey No 2, 3, 4, Laxmi Nagar, Kondhwa, Pune, Maharashtra-411048"

3. Objective

To Detect, prevent and control unauthorized physical access, damage, and interference to the organization's premises and information.

4. Policy

a. Appropriate physical and environmental security controls shall be implemented at all VU's Information processing facilities to protect people, property and information system resources.
b. VU shall adopt risk management approach when identifying physical and environment controls for facilities.

4.1. Physical Entry Controls

- Physical entry controls shall restrict the entry and exit of personnel, from an area, such as an office building, secure areas.

- An entry/ exit log of staff and visitors shall be maintained, with date, time and assets.
- Access to areas where confidential information is stored or processed shall be restricted by proper access control and allowed only to authorize persons.
- A physical log book or electronic audit trail of all access shall be securely maintained & monitored.
- External party support service personnel shall be granted restricted access to secure area only after authorization & monitoring measures in place.
- Access rights to secure area shall be regularly reviewed, updated & revoked when necessary.

4.2. Securing Offices, Rooms and Facilities

- Servers, Networking devices & Computers shall be sited to restrict and control the access.
- The server room shall be protected from eavesdropping.
- Confidential files and important restricted and confidential documents shall be kept at a safe place, with lock and key
- CCTV camera shall be implemented for surveillance

4.3. Protecting Against External and Environmental Threats

- Smoke detectors shall be implemented at appropriate places for early fire detection.
- Fire extinguishers shall be kept at appropriate places.
- AMCs for fire detection & prevention utilities shall be in place & regularly monitored.

4.4. Working in Secure Areas

- The personal (staff) shall only know the existence, or activities in a secure area on a need-to-know basis.
- The secure area shall always be monitored, for safety reason and to prevent opportunities for malicious activities.
- Secure areas which are vacant shall be locked and inspected regularly.
- Office area shall be monitored by CCTV and the footage shall be retained.

4.5. Delivery and Loading Areas

- Delivery from outside of the building shall be restricted to authorized and identified personals only.
- All the incoming material shall be checked for any hazardous material.
- A register shall be maintained for all incoming material in accordance with the asset management.
- All incoming & outgoing material shall be checked for any tampering and shall be reported if observed via proper incident management procedure

5. Equipment Security

This category aims to prevent loss, damage, theft or compromise of assets or interruption to the VU's activities.

5.1. Equipment Siting and Protection

- Equipment's shall be sited to minimize unnecessary risks and to reduce the need for unauthorized access to sensitive areas.

- Isolate item which requires special protection to increase the general level of protection required.
- use specific controls as appropriate to minimize physical threats -- e.g., theft or damage from vandalism, fire, water, dust, smoke, vibration, electrical supply variance, or electromagnetic radiation;

5.2. Supporting Utilities

- Supporting utilities shall be adequate to support the equipment under normal operating conditions
- Reasonable provision shall be made for backups (e.g., a UPS) in the event of supporting utility failure

5.3. Cabling Security

- Physical measures shall be implemented to prevent unauthorized interception or damage, including additional protections for sensitive or critical systems;
- Alternate/backup routings or transmission media where appropriate, particularly for critical systems shall be identified
- Markings and labeling requirement for Cable and equipment shall be clearly identified

5.4. Equipment Maintenance

- Appropriate preventive maintenance schedule shall be prepared ;
- Documentation of all maintenance activities, including scheduled preventive maintenance shall be maintained;
- Documentation of all suspected or actual faults, and associated remediation shall be maintained;

- Maintenance shall be conducted only by authorized staff and contracted third parties
- Appropriate security measures, such as clearing of information or supervision of maintenance processes, appropriate to the sensitivity of the information on or accessible by the devices shall be maintained

5.5. Security of Equipment Off-Premises

- Security controls for equipment in transit and in off-site premises, appropriate to the setting and the sensitivity of the information on or accessible by the device shall be implemented;
- Adequate insurance coverage, where third-party insurance is cost-effective; shall be procured
- Staff and contractor shall be made aware of their responsibilities for protecting information, devices, and risks of off-site equipment.

5.6. Secure Disposal or Re-Use of Equipment

- Best practices shall be adopted for secure information removal, appropriate to the sensitivity of the information known or believed to be on the media;
- Information removal shall be performed by appropriately trained personnel

5.7. Removal of Asset

- Information asset/ equipment going in/out of office premises shall be inspected and recorded
- recording of off-site authorizations and inventory of equipment and information taken off-site shall be maintained;

- Users authorized to take equipment or information off-site shall be made aware of security risks
- External party users who have the authority to permit off-site removable of assets shall be identified & appropriate security measures shall be implemented to address risk associated with the assets

6. Enforcement

Any staff found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. Reference Document

- Third- party agreement
- Acceptable use of information assets.
- HR IT policy
- Secure Disposal of media

8. Distribution List

The following users have access to this policy:

- All staff, Contractors, Vendors of Vishwakarma University

9. Acronyms / Definitions

1. VU: Here it refers to Vishwakarma University
2. Staff: Here it refers to Teaching Staff/ Non-Teaching Staff/ Office Staff/ Peons
3. AMC: Annual Maintenance Contract for periodic check & maintenance off supporting utilities
4. Secure area: here it refers to Server room & DVR system place