TechSture
Technologies

Physical and Environmental Safety

Document No – TT-ITP/11

Document Release Note

Document Version	1.0	**Release Date**	

Prepared By		**Approved By**
Pathik Patel		**Chetan Patel**

Document Revision History

Version	Date	Change Description	Modified By	Reviewed By	Approved By
1.0					

Purpose

This policy defines the methodology for Physical and Environmental Security.

Scope

This policy applies to all employees.

Policy

To prevent unauthorized access, loss, damage and interference to business premises and information. Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference.

Physical Security

- IT equipment supporting critical or sensitive business activities will be located in secure areas with restricted access. Local network equipment/file servers and net terminating equipment will always be located in secure areas and/or lockable cabinets. Such facilities should be protected by a defined security perimeter with appropriate entry controls and security barriers with CCTV monitoring e.g. lock and key, to guard against unauthorized access, damage and interference.

- Facilities where person identifiable information is stored, including offices, should be secured when unattended. Procedures must be in place to allow access in cases of emergency.

Entry Controls

Secure areas should be protected from unauthorized access by controls such as:

- Controlled access to the central computer facilities/local network equipment/file servers and net terminating equipment will be confirmed to the designated staff, whose job function requires access to that area/equipment. The IS officer or IT Director may give restricted access to other staff where there is a specific job function needed for such access.
- No individual will be given access to any of the TechSture (Company)'s networks or systems unless that individual has been formally authorized to have access by the IS Officer or IT Director.
- All company vendors, visitors will be required to register at the reception of the Techsture office with their ID captured. They should be allowed to visit only designated area of the office which strictly excludes Electronic and IT Development section.
- Regular review and update of access rights to secure areas.
- Controls for visitors:
  - Supervision or clearance for specific, authorized purposes.
  - Instructions on emergency procedures and security requirements.

- Recording their date and time of entry and departure.

Securing Offices, Rooms and Facilities

- A secure zone may be a locked office, or several rooms inside a physical security perimeter, which may be locked or contain lockable cabinets or safes.
- The selection and design of a secure area should take account of the possibility of damage from fire, flood, explosion, and other forms of natural or man-made disaster. Account should also be taken of relevant health and safety regulations and standards. Consideration should be given also to any security threats presented by neighbouring premises, e.g. leakage of water from other areas.

Following points are considered to controls the secure zones:

- Locating important facilities away from public access.
- Lock unattended doors and windows.
- Locate support functions and equipment such as photocopiers in a secure area so that information cannot be compromised. All prints has to be monitored and log has to be kept.
- Restricted public access to directories and internal telephone books that identify the location of "sensitive" facilities.
- Fall-back equipment and back-up media should be sited at a safe distance to avoid damage from a disaster at the main site.
- Suitable intruder detection systems installed to professional standards and regularly tested should be in place to cover all external doors and accessible windows.

Key Control Procedure

- Locking of office as well as individual cabins and labs is practiced.
- Keys (for all the cupboards & drawers) are deposited to Facility/Process Owner after the closing hours, which are kept in lock & key by Facility Personnel.
- Main door i.e. entrance key is either taken care by the Facility/Process Owner.

A location wise/department wise list of keys is being prepared (refer asset inventory register) & kept with Office Administrator locker. Keys can be availed only to the authorized persons. In case of any emergency key can be availed to other person only after taking permission from the management/authorized person.

In case of loss of key, immediate intimation to be given to receptionist/admin for taking necessary actions & further communications.

Equipment Security

Equipment should be physically protected from security threats and environmental hazards. Protection of equipment (including that used off-site) is necessary to reduce the risk of unauthorized access to data and to protect against loss or damage. This should also consider equipment and disposal. Special controls may be required to protect against hazards or unauthorized access, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

Equipment Sitting and Protection

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and reduces the opportunities for unauthorized access by human threats. The following controls should be considered:

- Equipment should be sited to minimize unnecessary access into work areas.
- Information processing and storage facilities handling sensitive data should be positioned to reduce the risk of overlooking during their use.
- Items requiring special protection should be isolated to reduce the general level of protection required.
- Use of particularized 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.
- Eating, drinking, smoking or other activities in the vicinity of equipment/information processing facilities is not allowed.
- Environmental parameters should be monitored for conditions, which could adversely affect the operation of information processing facilities.
- The impact of a disaster happening in nearby premises, e.g. a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street should be considered.

Power Supplies and Supporting Utilities

Equipment should be protected from power failures, telecommunications failures, and other disruptions caused by failures in supporting utilities such as AC, water supply and sewage. A suitable electrical supply should be provided that conforms to the equipment manufacturer’s specifications.

Control includes:

- Multiple feeds to avoid a single point of failure in the power supply.
- Uninterruptible power supply (UPS).
- Assuring that the supporting utilities are adequate to support the equipment under normal operating conditions.

Equipment Maintenance

Equipment should be correctly maintained to ensure its continued availability and integrity.

Control includes

- Equipment should be maintained in accordance with the supplier's recommended service intervals and specifications.
- Appropriate preventive maintenance.
- Documentation of all maintenance activities, including scheduled preventive maintenance.
- Documentation of all suspected or actual faults, and associated remediation.
- Maintenance only by authorized employees or 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 being maintained;

Cabling Security

Power and telecommunications cabling carrying sensitive data or supporting information services are protected from interception or damage.

Control includes:

- Physical measures 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.
- Clearly identified cable and equipment markings, except where security is enhanced by removing/ hiding such markings.
- Documentation of patches and other maintenance activities.

Secure Disposal or Re-Use of Equipment

All equipment containing storage media should be checked to ensure that sensitive data and licensed software has been removed or securely overwritten prior to disposal.

Control includes:

- Use of generally accepted methods for secure information removal, appropriate to the sensitivity of the information known or believed to be on the media.
- Secure information removal by appropriately trained personnel, or verification of secure information removal by appropriately trained personnel.

Removal of Property

Equipment, information or software should not be taken off-premises without prior authorization/ gate pass.

Control includes:

- Limitations on types/amounts of information or equipment that may be taken off-site.
- Recording of off-site authorizations and inventory of equipment and information taken off-site.
- For persons authorized to take equipment or information off-site, appropriate awareness of security risks associated with off-premises environments and training in appropriate controls and counter-measures.

Records

- Entry Logs
- Disposal Records
- Transfer records (encryption details to be addressed)

Effective Measures

No. of incidents reported in a quarter.