**Physical and Environmental Security Policy and Procedure**

Doc ID: POL/0.1

Document Classification: Internal

July 2022

**Document Control**

| Document Name | Physical and Environmental Security Policy and Procedure |
| --- | --- |
| Document ID | POL/0.1 |
| Security Classification | Internal |

| **Authorization** | | |
| --- | --- | --- |
| Document Owner | Reviewed by | Authorized by |
|  |  |  |

| **Amendment Log** | | | |
| --- | --- | --- | --- |
| **Version** | **Modification Date**  **DD MMM YYYY** | **Section** | **Brief description of the change** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**TABLE OF CONTENTS**

1.0 Purpose 5

2.0 Scope 5

3.0 Policy 5

3.1 Physical Security 5

3.1.1 Physical Entry Controls 5

3.1.2 Security of Office and Facilities 5

3.1.3 Physical Access for Employees, Consultants, Apprentice and Vendor Employees 6

3.1.4 Access to Third Parties and Visitors 7

3.1.5 Access to Visiting Employees and Visiting Clients 8

3.1.6 Securing Access to Secure Areas 8

3.1.7 Securing the Premises from Visitors and Third Parties 9

3.1.8 Maintenance and Review of Access Logs 10

3.1.9 Banners for Secured Areas 10

3.1.10 Management of Access Cards 10

3.1.11 Securing Information Storage Media 10

3.1.12 Securing Offsite Facilities [Disaster Recovery Site] 10

3.1.13 Security Office Keys 11

3.1.14 Security Inspections 11

3.1.15 CCTV Process 11

3.2 Environmental Security 11

3.2.1 Ensuring Suitable Environmental Conditions 11

3.2.2 Securing Premises from Fire 12

3.2.3 Securing Premises from Floods and Water Damage 12

3.2.4 Risk of Fire 12

3.2.4.1 Server Room 12

3.2.4.2 Fire Alarms 12

3.2.5 Water Damage Risk 12

3.2.5.1 Protection from Floods 12

3.2.5.2 Location of Server Room 13

3.2.6 Miscellaneous 13

3.2.6.1 Flooring 13

3.2.6.2 Switches 13

3.2.6.3 Emergency Lamps 13

3.2.7 Fire prevention steps 13

3.2.8 Maintenance and monitoring 13

3.3 Power Supplies 14

3.3.1 Power Supply Controls 14

3.3.2 Power off Switches 14

3.3.3 Power Supply 14

3.3.3.1 Local Power Supply 14

3.3.3.2 Dedicated UPS for the Server Room 14

3.3.3.3 Generator 14

3.3.3.4 Grounding (Earthing) 14

3.4 Cabling Security 15

3.4.1 Cabling Standards 15

3.4.1.1 Testing and Maintenance 15

3.4.1.1.1 Preventive Maintenance and Protection 15

3.4.1.1.2 Crisis / Emergency Maintenance 15

3.4.2 Heat and Air Pollution 16

3.4.2.1 Temperature 16

3.4.2.2 Humidity 16

3.4.2.3 Dust 16

3.5 Clear Desk Policy 16

3.6 Equipment Security 16

3.6.1 Physical Security of Laptops and Desktops 16

3.6.2 Equipment Maintenance 17

3.6.3 Security of Equipment off Premises 17

3.6.4 Disposal of equipment 17

4.0 Reference Documents 17

# Purpose

This policy and any other associated guidelines apply to the employees of {Company} and any Physical and environmental security policy addresses measures for securing information processing facilities and information assets from unauthorized access, damage or interference, or any natural calamities.

# Scope

This policy and any other associated guidelines apply to the employees of {Company} and any person having access to physical assets of {Company}. This could include apprentices, contractors, consultants, third-party associates, and any temporary employees and covers physical access to computing facilities, hardware, corporate data, and application and systems software. These facilities include server rooms/data centers, network control centers, and other related areas.

This document sets out {Company} arrangements for:

* Preventing unauthorized physical access, damage, and interference to our information and information processing facilities
* Preventing loss, damage, theft, or compromise of assets
* Preventing interruption to our operations

# Policy

The access to office premises is controlled via biometric access/access cards and to secured areas via biometric access/access cards.

All employees, apprentices, consultants, and vendor/contract employees shall be provided with biometric access/access cards with access to the {Company} premises as per their job roles and responsibilities.

Access to vendors, clients, and visitors shall be provided as per business requirements with appropriate records in Visitor Registers. They shall be allowed to carry Laptops and mobile storage devices after recording the same on the Visitor Register. They shall be escorted to the premises by the concerned host department representative.

The work environment in {Company} shall be conducive to service delivery with adequate power and air conditioning of Temperature, humidity dust control, and fire protection.

## Physical Security

### Physical Entry Controls

* {Company} must have a well-defined and secure perimeter.
* All doors shall be locked, when unattended or beyond working hours.
* Security guards shall be placed at all entry doors of the premises at all times.
* Directories and internal books or layout plans identifying locations of organizational information processing facilities should not be readily available or accessible to the public.
* CCTV cameras to be set up and monitored as per the CCTV process defined in subsequent section(s).

### Security of Office and Facilities

* The place where information-processing equipment is located must be secured from theft, physical intrusion, and environmental hazards. If there is any theft of the equipment, then the Incident Management Procedure needs to be followed.
* Support functions and equipment e.g. photocopiers, and fax machines, should be sited appropriately within the secure area to restrict access, which could compromise information. Incoming and outgoing mail (paper mail) points and unattended fax machines must be protected from unauthorized use during and outside normal working hours.
* Any equipment shall be taken outside only after approval from the Department Head / Delivery Head, Head – IT, and the Administration department. An approved gate pass shall be obtained for the same and shall be produced to the security personnel at the time of exit. A gate pass shall be issued for outgoing material. Security personnel at the entry gate shall not allow any material outside without an appropriate gate pass.
* Details of movement of hardware equipment between offices shall be recorded to facilitate easy tracking of inventory, proper depreciation, and identification of hardware for disposal/buyback or write-off.

### Physical Access for Employees, Consultants, Apprentice, and Vendor Employees

* The Human Resources (HR) department should inform the Administration (Admin) department and all support departments through auto-generated mail from MIS about the joining details of employee, apprentice, consultant, and vendor employee along with details of project/support department.
* On the day of joining a temporary access card will be issued to the employee, apprentice, consultant, or vendor employee. Admin department shall replace the temporary card with a permanent access card for employee, apprentice, consultant, or vendor employee by entering all relevant information in the access control software.
* Physical access rights granted to the employees in support services will be governed by the roles and job responsibilities of the support services staff members. Those members providing dedicated services to {Company} operations and the {Company} staff would be granted access to all areas in {Company}
* Physical access rights to the contract/vendor employees for support services shall be governed by the services provided by them as defined in the service level agreements signed with the contractor. The access rights shall be commensurate to those needed by such staff to fulfill their service obligations. However security requirements like signing the non-disclosure agreements and the confidentiality clause will be mentioned in all third-party contracts, agreed upon and signed by the personnel before any physical access is granted.
* The Police Clearance Certificate (PCC) needs to be submitted by all the security guards. The PCC should be submitted by the vendor company within 3 months of deputation. At the time of deputation if the PCC is not available then the vendor company shall submit the undertaking on the company letterhead.
* The government-issued license for electrical works needs to be submitted by the electricians. The deputation letter needs to be submitted by the housekeeping agency for the deputed staff.
* Periodic audits on the records of security guards and housekeeping personnel should be performed.
* On the last working day of an employee/apprentice / consultant or vendor, HR shall forward resignation or termination information through auto-generated mail from MIS to all support departments.
* The resigning employee will return the access card to the Admin and mention the evidence of the return of access card or loss of access card on the exit clearance form. Admin should then disable the card in access control software.
* If an employee/apprentice/consultant/vendor employee forgets to carry his/her access card, he/she shall record the time of entry in a separate register kept at security. He /She shall be given a temporary card for the day. The same shall be returned to the security at the end of the day.
  + - Employees not carrying the Photo ID badges should not be allowed inside the work areas by Security personnel.
      * Defaulted employee has to make an entry in the employee defaulter register which will include the details:
        + Employee Name:
        + Employee Number:
        + Time in:
        + Time out:
        + Reporting Manager’s Name:
        + Issued card number:
        + Employee Signature:
      * Defaulter employee will be issued access card which will be activated for general security zones only.
      * Defaulter employee should return the access card at the time of exit.
      * Reconciliation of badges issued to defaulter employees must be done at the end of each month.
      * Any issue regarding reconciliation should be reported to the Admin department who in turn will report it to the reporting manager of the defaulter employee.
* For any loss of card, the same shall be informed to Admin by the concerned employee by mail or in person. Admin shall disable the same card in the system, recover the cost of the card from the employee, and issue a new card.
* For absconding employees/apprentice/consultants, HR should inform the Administration (Admin) department and all support departments through auto-generated mail from MIS after completion of 10 days of issuing the termination letter to the absconding employees. Admin shall disable the access in the system and recover the dues from the final settlement, wherever applicable.
* For absconding vendor employees, HR should inform the Administration (Admin) department and all support departments through auto-generated mail from MIS after completion of 2 days of receiving information from the concerned project manager. Admin shall disable the access in the system and recover the dues from the final settlement, wherever applicable.
* Employees, apprentices, consultants and vendor employees can take Personal PDAs and Mobile Phones with Cameras / memory. However, no photography will be allowed in Server rooms and pre-identified restricted areas.

### Access to Third Parties and Visitors

* Security personnel at the door must ask visitors the purpose of their visit and whom they wish to meet in {Company}
* Security personnel must ensure that all visitors make an entry and sign the [visitor’s register](#_heading=h.1rvwp1q) maintained at the reception.
* Security personnel must issue a visitor badge and record the visitor’s badge number in the register. Security personnel must instruct the visitor to display the visitor’s badge by wearing it around their neck continuously during their stay on {Company} premises.
* Security personnel should direct the visitor to the reception or instruct the visitor to wait at the visitor bay till the concerned {Company} employee comes and escorts the visitor.
* Third party personnel such as maintenance staff and delivery staff shall only be granted limited physical access to the common areas.
* Security personnel or the person at the reception must inform the concerned {Company} employee about the visitor.
* Security personnel must maintain a record on Returnable Goods Inward Slip of any IT equipment’s or media like tape drives, laptops etc. to be brought in the office premise by the visitor. The serial number of the equipment’s must be noted in visitor register. Security personnel shall verify the details and hand over a copy of the same to the third party / visitor at the time of entry in the premises. The security guard shall also collect the same slip at the time of exit and verify the authorization and details of authorized goods.
* Security personnel must collect the visitor badge and exit time should be logged when the visitor leaves the {Company} premise.
* Security personnel must match the serial number of the IT equipment’s when the visitors enter and leaves {Company} premise. Any deviation should be reported to the Head - Admin or Head – IT.
* Reconciliation of badges issued to visitors must be done at the end of each month. Any deviations found during the reconciliation should be reported to Admin department.
* Security personnel at door must not allow any {Company} owned IT equipment or media to be taken out without a valid gate-pass. The gate pass should be checked for the signature of appropriate signatory.
* Third party personnel (representatives of supplier / vendors) making deliverables of supplies shall be escorted in the premises by concerned department representative.

### Access to Visiting Employees and Visiting Clients

* Visiting employees shall be given the access cards at reception by security personnel when they visit our office on the first day.
  + - Employee has to make an entry in the register kept at the reception which will include the details like:
      * Employee Name:
      * Employee Number:
      * Time In:
      * Issued Card Number:
      * Date of Issue:
    - Expected Date of Return:
* The access card issued to the visiting employees shall be activated for general security zones only.
* For visiting clients, visiting cards (not access enabled) shall be given to the respective hosts of the client from {Company} who in turn shall hand over the same to the client.
* Visiting clients shall be escorted by the host of the client.

### Securing Access to Secure Areas

* All critical servers and communications equipment must be located in secure locked rooms (referred as secure areas) to prevent tampering and unauthorized usage.
* Access to secure rooms shall be restricted by means of access control mechanisms.
* Additional controls shall be in place to secure critical or sensitive information. Access to secure areas must be strictly controlled e.g. access to server rooms must be controlled and restricted to authorized personnel like server and database administrators who need to perform their duties.
* Signs indicating "Authorized Personnel Only" or a similar message shall be prominently posted at all entrances of secure areas.
* IT department shall control physical access to the server rooms / data centers. A list of employees / apprentice / consultants / vendor employees having access to server room shall be created by Admin and handed over to the IT department. Any changes to the list shall be immediately updated by Admin team. The access to server room list shall be reconciled on quarterly basis and / or whenever there are changes to the employee access. A list of personnel authorized to enter the server room must be displayed at the door of server room. (List of Authorized Personnel for Server Room)
* Admin team shall control physical access to the UPS rooms, Stabilizer rooms, Electrician room.
* Knowledge or access of the “secure areas” [example: server room, UPS room, etc.] shall be given to employees or third party on a “need-to-know” basis.
* Secure areas must not be visible or identifiable from the outside; i.e. there should not be any directional signs providing access to such rooms.
* Emergency lighting should be installed in the server rooms and other working areas for use during power outages.
* Visitors and third parties shall be allowed entry to secure areas for authorized and specific purposes only after obtaining the approval from respective stakeholders. Visitors or third parties shall not be permitted unsupervised access to secure areas.
* A separate register shall be maintained at the entry gate of the secure areas (server room, data centers) for recording the entry of the people like employees, vendor, contractors etc. who do not have regular access to the secure areas. Any such entry to the secure areas shall only be provided after making an appropriate entry in the register.
* Wherever access cards are given, Admin team shall reconcile the information of employees, apprentice, consultants, and vendor employees as per MIS with report of live access cards generated from access control software on monthly basis. The reconciliation report shall be reviewed by various stakeholders to check if there have been any physical access violations. Admin team shall carry out monthly check on un-issued cards.
* All equipment movement within and outside the secure rooms should be tracked and continuously monitored to mitigate the risks of unauthorized removal of equipment both by employees or any external personnel.
* Access to tape, disk and documentation libraries should be restricted exclusively to those employees who are responsible for their maintenance.
* Following are the security requirements for {Company} servers at any Data-center:
* 24x7, 365 days, manned security guards
* Secure Access Restriction to the servers. It shall be a combination of:
* Electronic Access Control System.
* Access Restriction via smart-cards.
* Access available only to authorized {Company} personnel.
* Photo identification required for authorized {Company} personnel
* All access will be logged (electronically or manually) and shall be reviewed on a regular basis as per the **Physical Access Review Plan**
* Names of individuals with authorized access to {Company} servers shall be provided to data centers as per access requirement. The access to the data centers will be authorized by the VP-Tech or CTO.
* All visitors who are granted the permission to access {Company} servers and other networking devices are accompanied by {Company}'s personnel or any other person duly authorized by {Company} for the same.
* For access to the Data Center, a photo-identification is a must. This photo-identification will be issued to authorized {Company} personnel.

### Securing the Premises from Visitors and Third Parties

* Employees shall display the Photo ID badge by wearing it around their neck continuously during their stay on {Company} premises.
* Employees not carrying the Photo ID badges shall not be allowed inside the work areas without following the employee ‘defaulter procedure’. Defaulted employee has to make an entry in employee defaulter register. Defaulter employee shall be given an employee ID badge which will have access rights only to the work areas and not secured areas. The employee ID badge number shall be noted down against the related entry in the defaulter register.
* Every visitor (anyone who is not wearing the Photo ID badge) shall be questioned by the security personnel or the receptionist present at the main door.
* The security personnel or the receptionist shall advise the visitor to fill in the details in the visitor register. The visitor register shall contain the details like:
  + Visitor name
  + Company
  + Date
  + Time in
  + Time out
  + Contact details
  + Purpose of visit
  + Whom to meet (Person to be met)
  + Remarks (Details of laptop or any other equipment)
* The details regarding the information processing equipment, if any, carried along should be captured in the visitor register. The materials (laptops, mobile storage devices, I-pods, MP3 Players etc.) must be declared at the security / reception on visitor register.
* A visitor badge shall be allotted to every visitor once the entry is marked in the register. The visitor badge number shall be noted down against the related entry in the register.
* {Company} employee being visited shall be informed about the visit and the details of the information processing equipment in visitor’s possession. Visitors shall always be escorted by the concerned {Company} employee. It is the responsibility of the employee to ensure that the visitor only visits the areas they are authorized to visit. The employee shall be held responsible for all actions / misconducts, if any, of the visitor.
* Visitor’s entry should be restricted to the meeting / discussion rooms only as far as possible.
* {Company} personnel shall question all unescorted strangers.

### Maintenance and Review of Access Logs

* Monthly Reconciliation of the information of employees on rolls as per MIS with report of live access cards generated from access control software must be done on monthly basis.
* The reconciliation report is reviewed to check if there have been any physical access violations.
* Review of violation logs for the pre-identified restricted areas must be done on monthly basis.

### Banners for Secured Areas

* Banners need to be posted at the main door, reception, all sensitive areas and the server room area, so that {Company} employees and visitors are aware of the security measures. The banners must prominently display: “Unauthorized entry is prohibited” or “Entry Restricted”.

### Management of Access Cards

* Admin team shall manage the access cards and maintain an inventory of the issued as well as unissued cards at {Company}.
* Reconciliation of the access cards (issued as well as unissued) must be done on monthly basis.

### Securing Information Storage Media

* All information storage media (e.g. hard disks, floppy disks, pen drives, magnetic tapes and CD-ROMs) containing sensitive or confidential data shall be physically secured, when not in use.
* Information storage media shall not be taken outside the office premises unless specifically authorized.
* Physical access to magnetic tape, disk and documentation libraries shall be restricted to authorized personnel only.
* Back-up media shall be stored in fire resistant safes or cabinets.
* Visitors and third parties shall not be allowed to bring along any other external storage devices, unless authorized by the selected Approvers. In case, any of the external devices need to be connected to {Company} network, then additional approval from the Department / SBU Head and Management Representative is required.
* Media containing sensitive corporate information shall be monitored with audit trails.

### Securing Offsite Facilities [Disaster Recovery Site]

* Fall back equipment and back-up media must be stored at a safe distance (at an offsite location) to avoid damage from disaster at the main site.
* The physical and environmental safeguards available at the off-site location must provide the same level of security, at a minimum, as at the primary site.
* Following are the characteristics required to ensure safety against environmental conditions. The corresponding mitigations requirements shall be setup at all {Company} office premises and Data-centers:

| ***S#*** | ***Condition*** | ***Mitigation*** |
| --- | --- | --- |
| 1 | Power Failures, Disruptions, Fluctuations, etc. | * Servers shall not be directly connected to power mains. Instead they shall be connected through online-UPS with back-up power to ensure safety against power fluctuations. * Workstations in {Company} office premises shall be provided with power lines backed up by UPS and back-up power. Users’ desktops, laptops and other computing equipment shall be connected to these lines. |
| 2 | Fire protection | * Back-up tapes shall be kept in safe and secure storage areas * Reliable Fire Extinguishing Infrastructure shall be setup * Smoke detectors shall be installed in the server room. * Inflammable and hazardous material must not be allowed to be taken into the server room and data centers * The server room shall not have any loose or open electrical cabling * All electrical cabling work shall be done by Licensed Class 1 Electrical contractors |

### Security Office Keys

* Admin team shall maintain a register of all keys (including duplicate keys) of the entry / exit / fire exit doors and all cabins including meeting rooms and labs and authorized key holders. The register shall be reviewed and updated on a monthly basis and / or on changes of door locks.

### Security Inspections

* Periodic physical security inspections shall be done at all sites and locations.
* List of registers shall be kept at the security guards’ desk.
* The Head – Admin on monthly basis shall inspect all the registers available with the security guards / receptionist.
* A strategy shall be planned and implemented to fill any identified gaps.

### CCTV Process

* The CCTV camera shall mandatorily cover Reception main entrance, restricted areas, project labs (if any as per project requirement) 24x7.
* The CCTV coverage shall be stored on the main DVR device for minimum of 30 days.
* A Remote monitoring facility shall be available for the Admin department to check the CCTV coverage and Admin department shall do random monitoring of approximately 15 minutes of clip on weekdays. No separate logs shall be maintained for this random monitoring.
* IT and Admin department together shall ensure that there is periodic clock synchronization of the DVR device with the other servers in the organization.

## Environmental Security

### Ensuring Suitable Environmental Conditions

* Temperature and humidity levels shall be monitored and maintained, especially in Server / UPS Room as per the recommendations mentioned in the Physical and Environmental Security Procedure and / or as per the recommendations of IT equipment manufacturers.
* Smoking shall be strictly prohibited inside the office area.
* Eating and drinking inside server and UPS rooms shall be strictly prohibited.

### Securing Premises from Fire

* All computer systems shall be housed in an environment equipped with fire extinguishers.
* The fire extinguishers (of appropriate class) shall be placed at all strategic and prominent locations within the office so that they are easily accessible in all areas.
* Smoke detectors shall be located within the office premises including Server Room.
* Fire safety equipment shall be checked regularly in accordance with manufacturer's instructions. A maintenance sheet / note shall be attached with the equipment.
* All fire exits shall be marked clearly and shall be easily accessible from work sections.
* Hazardous and combustible materials shall be stored at a safe distance from the server rooms and other computer rooms. Computer supplies such as stationery shall not be stored in server rooms.
* Comprehensive fire and emergency instructions shall be displayed at prominent locations.
* All new information processing sites shall be evaluated and appropriate fire safety controls shall be implemented before moving in at that site.
* Functioning and operations of the fire safety devices / equipment’s installed by {Company} shall be explained to the security guards periodically during internal training programs. Some of the {Company} employees (Fire Marshals) shall also be made part of such internal training programs.
* Evacuation drills shall be conducted at least once in six months to ensure the effectiveness of the training and instructions to be followed in case of emergency. Count of people present in the office at the time of the drill should be taken by Head - Admin i.e. Employees, Vendor Employees / Third Party Contractors, Security and External Visitors. It will be the responsibility of the individual Fire Marshalls to check and ensure that their respective assigned areas are evacuated.

### Securing Premises from Floods and Water Damage

* Computer and communication rooms shall not be located in areas like basements, as far as possible, which are susceptible to water seepage and flooding.
* Computer and communication rooms shall be located on raised or elevated floors.
* Adequate drainage provision must be provided to prevent water damage or flooding.
* Water sprinklers must not be installed in server rooms / storage rooms etc.
* Electrical equipment, damaged due to water, must be checked and dried before being returned to service.

### Risk of Fire

### Server Room

Smoke detection and fire alarms shall be installed inside the server room.

### Fire Alarms

The whole premises shall be fitted with automatic smoke detectors, sprinkler system and fire alarms. There shall also be manual call points located at strategic places in the building, which can be activated, by any employee who notices fire, which the smoke detectors / heat detectors have failed to detect.

### Water Damage Risk

### Protection from Floods

The premises shall have adequate flood and rainwater drains. The premises shall be maintained to ensure that water leakage / seepage, if any, is detected and corrective action is initiated.

### Location of Server Room

The server rooms shall be located in such areas within the delivery centers where there is no risk of damage by water seepage. Further all the racks of the server room shall be away from windows to ensure that it is isolated from any external atmospheric influence.

### Miscellaneous

### Flooring

The flooring of the server room shall be at raised from the ground and shall be tiled with anti-static material.

### Switches

Switches and sockets shall all be grounded (provided with earthing) and provided with circuit-breakers to avoid any untoward occurrences due to faulty wiring or short circuits. To reduce the risk of accidental tripping all wall mounted switches and circuit breakers should be at such a height that they do not come in the way of free movement of people.

### Emergency Lamps

UPS backed up and self-activating emergency lamps shall be placed in the Operations area and any other critical location, to allow lights in the event of abrupt power failures.

### Fire prevention steps

* Adequate fire protection methods must be implemented which includes provision of fire extinguishers of required kinds, fire alarms, sensors and displays for protection from fire.
* Clear instruction on usage must be made available near the extinguisher, which would provide prompt information on usage of the extinguishers.
* Fire emergency and evacuation procedures must be posted in common areas or on notice boards.
* Emergency phone numbers such as fire brigade, key security personnel, doctors, and hospitals must be posted in prominent places and also the same must be available with the security guards.
* All offices should have distinct space and pathways, marked as emergency exits as per the recommendations of statutory or external fire safety agencies. The routes for exit shall be clearly displayed at such entrances.
* Access to emergency exit doors should not be restricted in any way i.e. boxes; furniture, etc. should never be stored in corridors or near emergency exit doors.
* Combustible materials and any other materials that may provide fuel to a fire should be kept to an absolute minimum. Wood pallets, cardboard boxes, paper, oily rags, paint and cleaning fluids are materials that may provide fuel to a fire. Flammable liquids should be stored in approved containers and the containers should be under lock and key in metal cabinets.
* All employees and temporary staff should be trained in the fire safety precautions and must be imparted basic knowledge of escape and safety during fire accidents.
* Mock-drills should be conducted once in six months. Count of people present in the office at the time of the drill will be taken by Admin Manager i.e. Employees, Vendor Employees / Third Party Contractors, Security and External Visitors. It will be the responsibility of the individual Fire Marshalls to check and ensure that their respective assigned areas are evacuated.

### Maintenance and monitoring

* Fire-fighting equipment should be checked regularly and the test results should be documented.
* Environmental conditions must be monitored for extreme temperatures, dust, water leakage/seepage, moisture content etc. that could adversely affect the operation of information processing facilities.

Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup must be installed for the server rooms and all information processing facilities.

## Power Supplies

### Power Supply Controls

* Uninterrupted Power Supply (UPS) shall be installed to ensure continuous running of all critical computing and supporting equipment at all locations. UPS must have the capability to continue the power supply to allow for an orderly shutdown of the system.
* UPS equipment shall be maintained in accordance with the manufacturer’s recommendations to ensure that it is in working condition.
* Backup generators may be installed for continuous running of information processing systems in case of prolonged power failures. The generators shall be maintained by the property manager. All buildings shall have proper earthing to prevent electric surges.
* Voltage regulators shall be installed, wherever necessary, to guard against fluctuations in power. Circuit breakers of appropriate capacity shall be installed to protect the hardware against power fluctuations or short circuits.

### Power off Switches

* Emergency power off switches shall be installed at strategic locations in order to facilitate rapid power-off in case of an emergency such as a fire.
* The power-off switches shall be clearly labelled, easily accessible but shielded to prevent accidental activation.

### Power Supply

* Power supply is critical for uninterrupted functioning of the company. The following power supply arrangements shall be made

### Local Power Supply

Primary and regular power supply shall be obtained from the local power providers. This shall terminate at a local transformer to regulate the power that is available to the Operations area, which must not exceed the 220-250V range. Further, within the server room the voltages maintained shall be regulated to suit the servers as per the vendor recommendations. Circuit breakers of appropriate capacity shall be installed to protect the hardware against faults like over current, under voltage, earth fault, earth leakage, short circuit etc. The power cables shall be routed securely to prevent damage or interception. Power and data cable shall be routed separately.

### Dedicated UPS for the Server Room

A dedicated UPS (Uninterruptible Power Supply) shall be maintained for devices inside the server room. The UPS shall reside in a protected dust free environment. There shall be adequate space around the UPS for maintenance purposes. The UPS shall be of adequate capacity (rating) so that, in case of outage of regular power, it can deliver the required power for at least 20 minutes to allow systematic shutdown of servers where backup power (generator) is not available. The point-in-time threshold level for the UPS shall be 80% to 85%.

### Generator

A diesel generator shall provide backup to the delivery center and all the critical information systems inside the facilities. The generator is automated to start up as soon as the electricity supply from the local power supplies gets cut off. The generators shall be maintained by the property manager.

### Grounding (Earthing)

The premises shall have provision of adequate grounding. The Admin department shall ensure maintenance of the earth pit, as necessary, through the property owner so that the grounding resistance is always within normal range.

## Cabling Security

Power and telecommunication cables that connect various information processing facilities are exposed to many environmental hazards like sand storms, floods, fire, lightning, cutting due to careless digging or damage by rats and rodents. Cables carrying data or supporting information services shall be protected from interception or damage to reduce the risk of power or communication failure, if feasible.

### Cabling Standards

* Power and telecommunication lines used for information processing facilities shall be laid underground, where possible, or subject to adequate alternative protection.
* Network cabling must be protected from unauthorized interception or damage due to environmental hazards e.g. by using conduit or by avoiding routes through public areas.
* Power cables must be separated from communication cables to prevent interference, as far as possible.
* Cables carrying data or supporting information services shall be protected from interception or damage.
* The network hubs and switches located throughout the premises shall be placed in locked cabinets, as far as possible and shall be protected from fire, heat, dust and water.

### Testing and Maintenance

### Preventive Maintenance and Protection

Preventive Maintenance (PM) tasks / activities and frequencies for all the equipment’s shall be determined by the Admin team based on the following information:

* + - Original Equipment Manufacturers (OEM) operating and maintenance manuals and recommendations to prevent equipment’s from environmental hazards such as water leakage, moisture, dust, electromagnetic interference and chemical protection;
    - PM performed on existing similar equipment; and
    - Input from technicians

Preventive maintenance schedule for a year (52 weeks) shall be created by the Admin team for all the equipment’s consisting of weekly, monthly, quarterly, half yearly and annual maintenance activities as required based on the above information.

Preventive maintenance activities shall be carried out by the Admin team for all the equipment as per the PM schedule, which are not covered under Annual Maintenance Contracts (AMC).

For all the equipment, which is covered under AMC, PM activities shall be carried out by the respective service providers as per the schedule specified in the AMC.

Each scheduled PM activity will be recorded by the Admin team in the respective PM work order form after completion, which shall be reviewed by the Head – Admin. All the PM work orders shall be stored by the Admin team.

Adequate power supply shall be ensured to the equipment’s and also equipment’s shall be protected from power surges in case of fluctuations in power supply as per the OEM’s operation and maintenance manuals.

### Crisis / Emergency Maintenance

If any equipment breaks down, then necessary maintenance shall be carried out by the Admin team on priority basis. If required, Admin team shall take support from the original equipment manufacturer.

All efforts shall be made to reduce the total downtime and to bring back the equipment to normal operating conditions.

Equipment breakdowns and the maintenance carried out to bring back the equipment to normal operating conditions shall be documented by the Admin team. Necessary root-cause analysis reports (where ever required) along with the correction / corrective actions shall be documented and maintained by the Admin team.

### Heat and Air Pollution

All work areas within the premises shall have air conditioning facilities to prevent dust, heat and air pollution affecting IT equipment.

### Temperature

Temperature within the server room shall be controlled and retained between 18 (low) to 24 (high) degrees centigrade.

### Humidity

The humidity level in the server room shall be retained between 35% (low) and 80% (high).

### Dust

The server room shall be protected from particulate dust content. Cleaning of the server room shall be performed when required in the presence of authorized members of the IT / Project team.

## Clear Desk Policy

* Sensitive (Restricted / Confidential / Internal) information and storage media must be locked (in a fire resistant safe or cabinet), when not required or when office is vacated. The documents must not be kept unattended when not around.
* Photocopiers and other reproduction technology (e.g. scanners, digital cameras) are protected from unauthorized use.
* Documents containing sensitive or classified information should be removed from printers immediately.

## Equipment Security

### Physical Security of Laptops and Desktops

* A complete and up-to-date inventory of all laptops / desktops issued by the organization shall be prepared and kept updated at all times with the IT Team. Each laptop / desktop shall be marked with the asset code for easy identification.
* Laptops / Workstations must be traceable to individual users.
* Laptops and desktops shall be physically secured at all times to prevent unauthorized access or theft. Each individual shall be accountable for the physical security of his / her laptop / workstation / handheld devices.
* All Employees to whom laptops / handheld devices are issued are responsible for the security of the data contained within the laptops / handheld devices.
  + Laptops
    - It is the responsibility of laptop owners to ensure their physical safety in public places (like airports, hotels, conferences, trains, buses etc.). Laptops should not be left unattended.
    - All laptops should have a unique serial number. A list of all the laptop along with their serial number’s issues to {Company}. employees should be maintained by the IT team.
    - The owner of the laptop should be clearly identified.
    - For more details refer to the Laptop Code of Conduct Policy
  + Desktops
  + All desktops should have a unique serial number. A list of all the desktops along with their serial number’s issues to {Company}. employees should be maintained by the IT team.
  + The owner of the device should be clearly identified.

### Equipment Maintenance

* All equipment must be maintained, in accordance with manufacturer's specifications. Any frequent / repetitive breakdown of equipment may be analysed for corrective actions.
* Only authorized maintenance personnel must be allowed to service or perform repairs on equipment. A log must be maintained of all repairs or service work.
* If equipment needs to be sent offsite for repairs, the confidentiality and integrity of the information, stored in the equipment, shall be ensured. The entire data available on the equipment shall be backed up on a backup device and securely wiped from the equipment.
* A checklist must be maintained to ensure that regular maintenance is carried out for all equipment as per supplier’s recommendations. It is the responsibility of the respective equipment in-charge to ensure maintenance is carried out as per schedule.

### Security of Equipment off Premises

* If any IT equipment is required to be taken off-premises, the employee is required to obtain approval from Department Head and Manager – IT on the gate-pass.
* Administration Personnel should prepare a returnable/non-returnable gate-pass.
* The equipment movement must be recorded in an asset movement register.
* Security personnel at the door must retain a copy of the gate-pass.
* Outward entry of the equipment must be logged. It is the responsibility of the person taking equipment off-premises to ensure that it is returned in the same condition, in case of a returnable IT equipment.
* The concerned department must ensure that if the equipment is being taken off-premises for any repairs the entire data stored on the IT equipment must be appropriately backed up and deleted from the IT equipment before it leaves {Company} premises.

### Disposal of equipment

* User should mail the details for the equipment to be disposed to Admin and IT Team.
* User must take an approval for the equipment disposal from the Department Head.
* The employee must also forward the mail to Management Representative to verify any security concerns.
* If needed a backup of the user’s data should be taken by the IT Team before wiping the data.
* For the hard disks failure, the defined process in the Information Classification Procedure must be followed.
* The Asset register must be updated appropriately to reflect the absence of the disposed asset.
* The disposal must be based on the guidelines prescribed in the ‘Information Classification Policy’.

# Reference Documents

* ISMS Overview Policy
* ISO 27001:2013
* Statement of Applicability for ISO27001:2013
* Roles and Responsibilities
* Information Classification Policy
* List of Authorized Personnel for Server Room Template
* Disposal of Equipment Template
* Secure Room Log Register Template
* Laptop Code of Conduct Policy
* Preventive Maintenance Schedule
* Returnable / Non-Returnable Gate Pass
* Asset Monitoring Register