Insert the organization logo by clicking on the image icon

Access Control and Physical Security Policy Template

Date:

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Title:** | Access Control and Physical Security Policy Template | | |
| **Document ID:** |  | Version: | 0.1 |
| **Status:** | Draft |  | |
| **Publish Date:** |  | | |

**Document Review**

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Reviewer(s) | Remarks |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[1 Objective 4](#_Toc97463074)

[2 Scope 4](#_Toc97463075)

[3 Access Control 4](#_Toc97463076)

[3.1 User Access 4](#_Toc97463077)

[3.2 Equipments 4](#_Toc97463080)

[3.3 Systems and Apps 4](#_Toc97463081)

[3.4 Systems Login 5](#_Toc97463082)

[3.5 Network Access 5](#_Toc97463083)

[3.6 Remote Access 5](#_Toc97463084)

[3.7 Mobile Devices 6](#_Toc97463085)

[3.8 Wireless Access 6](#_Toc97463086)

[3.9 Shared Folder 6](#_Toc97463087)

[4 Physical Security 6](#_Toc97463088)

[4.1 Data Centre / Server Room 6](#_Toc97463089)

[4.2 Premises 7](#_Toc97463090)

[4.3 Environmental 7](#_Toc97463091)

[4.4 Cooling System 8](#_Toc97463092)

[4.5 Power Supply 8](#_Toc97463093)

[4.6 Equipments 9](#_Toc97463094)

[5 Exceptions 9](#_Toc97463095)

[6 Policy Enforcement 9](#_Toc97463096)

# Objective

This policy aims to define the controls and standards to maintain the access control and physical security of the <entity name> to ensure all the assets are secured and the information remains accurate, confidential and available when required.

# Scope

This policy applies to all <entity name> employees, contracted personnel, trainees, third party's representatives who have been provided with an access to all <entity name> buildings, facilities and assets.

# Access Control

## User Access

3. Designated security team (DST) should implement the necessary controls and measures to protect the information assets and buildings containing it from any unauthorized access in line with <entity name> business requirements and based on formal risk assessment.
4. Users accessing the information systems at <entity name> must not use or access an account assigned to another individuals.
5. During the creation and activation of user accounts for contractors, consultants, temporary workers, or vendor personnel Information Technology (IT) team should ensure that the individual is exist and actively performing service for <entity name>.
6. A formal record of all registered users shall be maintained by DST. This record shall be checked periodically for unused, redundant, or expired user accesses or accounts, or incorrect privileges.
7. Disabling user accounts should be for those who are retired, terminated or inactive for a period of time as per the rules of DST.
8. Reviewing access rights should be whenever an <entity name> employee changes his duties and positions.
9. Access request for contractors, consultants, or vendor personnel to <entity name> information systems shall be stated only in the contractual agreement.

## Equipments

1. DST shall implement suitable controls over the <non-organization/non-entity> equipment’s when they are connected or attempting to access to <entity name> network.

## Systems and Apps

1. Strict controls shall be implemented over the use of utility programs that may give the user the ability to override existing system and application controls.
2. Granting access to specific IT resources or services shall be approved by the management of the requester considering the job roles and duties performed by the employee.
3. All users granted access to the computing resources should be through a unique identification code (user-ID).
4. Any access to <entity name> application systems shall be granted by DST after appropriate authorization from the management.
5. DST is responsible for protecting the application systems and related resources.

## Systems Login

1. DST should ensure that only minimal system information should be disclosed during the logon process and the system or application details should not be displayed till the successful completion of the log-on process.
2. The logon process should validate user credentials only after all the data relating to the log on process is entered / input.
3. Any error messages during the log-on process should not be suggestive of the type or kind of error during the log on process.
4. The user-id should be locked after number of unsuccessful log-on attempts as per the procedure followed by IT team.
5. The log on process, unsuccessful attempts, shall be logged and alerted to DST.
6. User IDs and passwords for administrator shall not be provided to users.

## Network Access

1. DST is responsible for securing <entity name> network by dividing it into logical segments based on the access requirements, management of risk and segregation of duties.
2. DST should separate the internal network from the external with different security controls on each network.
3. The connectivity between internal and external networks shall be controlled by DST.
4. DST is responsible for providing network services needed to support business objectives by explicitly enabling needed services and disabling unneeded services.
5. Information system network access must be restricted to the authorized users and systems, using the principle of least privilege.

## Remote Access

1. Remote users shall connect to <entity name> network only through approved and designated remote access services by DST. Secure gateways and Diagnostic ports shall be kept inactive until needed and kept active only for the minimum time required.
2. Remote access services must ensure of encrypting the traffic by implementing Virtual Private Network (VPN).
3. Authorized remote access users accessing <entity name> internal information or services must be secured by implementing Multi-Factor Authentication (MFA) as an additional layer of security.
4. Remote access must be monitored from unauthorised access attempt.

## Mobile Devices

1. Establishing for a mobile devices control by the DST and must be shard to all <entity name> employees.
2. Mobile devices access to <entity name> internal information or services must be granted by DST after appropriate authorization from the management.
3. Employ for a Mobile Device Management (MDM) to enforce the <entity name> controls on the mobile devices authorized to access internal information or services by implementing full or partially device encryption, containerization of used application, monitoring and remotely device wiping when lost or theft.

## Wireless Access

1. Wireless access to the <entity name> should be in accordance with Wireless Access Policy.

## Shared Folder

1. Access to shared folders shall be granted by DST and authorized by the requester management.
2. Shared folders shall be used for work purpose only. Sharing any non-work related materials (such as photos, videos, audio files, etc.) is strictly prohibited.

# Physical Security

## Data Centre / Server Room

1. Access to <entity name> secure information processing facilities such as data centre / server room or areas where sensitive information is kept must be restricted and clearly demonstrated to prevent any unauthorized physical access.
2. A manned reception shall be in place to restrict entry into <entity name> premises to authorized personnel.
3. Suitable personnel will be identified to accompany housekeeping personnel during the routine cleaning of the secure areas.
4. No photographic, video, audio or other recording equipment should be allowed into secure areas without authorization.
5. <entity name> employees and visitors shall obtain permission before entering the data Centre / server room.
6. The server room should not be used for storage of any combustible material or hazardous materials.
7. Restrict all edibles or beverages inside the server room.
8. For employee / visitor access control system to data centre / Server room & hub rooms, following details should be captured:
   * + - Name
       - CPR
       - Date
       - Entering time
       - Exit time
9. Visitors shall be escorted by authorized <entity name> employee while entering data centre / server room and any other restricted areas.
10. Access to secure areas outside normal working hours shall be specifically authorized and logged.
11. Access to secure areas shall be revoked immediately upon termination or resignation of employees or completion of a consultation or vendor agreement.
12. Access rights to secure areas shall be reviewed and updated regularly.

## Premises

1. Wherever possible multiple entry points to the building should be closed and all personnel shall be directed to enter the building through a common entrance.
2. Unsupervised working in secure areas by third party personnel and vendors shall be avoided both for safety reasons and to prevent opportunities for malicious activities.
3. Visitors shall be escorted by authorized <entity name> employee while entering data centre / server room, or any other restricted areas.

## Environmental

1. <entity name> premises shall contain suitable environmental controls to reduce the risk from damage by fire, flood or other site disaster. Requirements for power, heating and cooling shall be appropriately addressed.
2. All secure areas at <entity name> will be provided with effective fire detection systems, fire alarm system and firefighting equipment as adequate for the size of the room and it will be protected from theft, flood, excessive heat and other environmental hazards. Security personnel on duty will always attend to the alarm system to respond to any incident.
3. The integrity of power, temperature and humidity control equipment shall be monitored regularly.
4. All data centres / server room equipment shall be provided a UPS based power supply, which will be backed up by generator sets.
5. Adequate detection controls and safety devices e.g. fire alarm, smoke detector, Fire suppression systems etc. should be placed in all offices, switch rooms and data centre.

## Cooling System

1. The air conditioners shall be checked for effective functioning on a periodic basis.
2. Maintenance contracts shall be maintained for speedy recovery from failure of Air conditioner
3. The air conditioning system should be effective and the temperature in the data centre / server room should be monitored regularly.
4. The temperature in the data center / server room and other critical areas shall be monitored and available on a 24-hour basis.

## Power Supply

1. Power going to computer systems should be through uninterruptible power system (UPS). It should be ensured that the UPS is always in working condition.
2. Circuit breakers of appropriate capacity should be installed to protect the hardware against increase in power voltage.
3. Generators should be provided for the generation of power in case of failure of the general power lines.
4. Self-activating emergency lamps should be placed in the server room and any other location, as required for handling abrupt power failures.
5. UPS and generators should be maintained as per vendor specifications and Annual preventive Maintenance shall be conducted as per vendor contract.
6. Data cables, power and telecommunication lines shall be protected by conduits from any damage, interference and interception.
7. Power and telecommunication cables should be segregated to prevent.
8. The UPS where possible should be installed in a separate room and not in the same room as the servers.
9. The UPS room should not be very near the server room to prevent spread of any fire resulting from a short circuit in UPS room to the server room or vice versa.
10. The UPS room / cabin should have an independent access and not through the server room to obviate the need for the UPS maintenance personnel to pass through the server room.
11. The UPS and batteries should be provided with the recommended ambience with special attention to temperature control, humidity, dust free environment etc.
12. It must be ensured that the UPS is not switched off and that the power cord is properly secured to the equipment. It must also be made sure that the battery cords are properly connected.
13. It must be ensured that no unauthorized person tampers with or changes the switch-settings on the UPS.
14. Batteries of the UPS take 8 to 12 hours for getting fully charged if the local power supply is erratic or if there is no power supply for at least 8 hours in a day, suitable arrangement for provision of a generator should be made.
15. Hardware Maintenance refers to all activities involved in the upkeep, repair and review of hardware resources after the installation in order to ensure proper functioning, correction of faults, improvement in the performance and adaptation of the hardware in the IT environment.

## Equipments

1. Equipment should be maintained in accordance with the supplier’s recommended service intervals and specifications.
2. Only authorized maintenance personnel should carry out repairs and service equipment.
3. Activities of on-site maintenance should be supervised to ensure that he doesn’t have unauthorized access to <entity name> data.
4. All equipment / media taken off-premises shall be authorized.
5. An approved list of authorized signatories shall be prepared and maintained.

# Exceptions

1. All exceptions to this policy shall be explicitly reviewed by the DST and approved by management. The exceptions to this policy if any shall be approved and valid for a specific time period and shall be reassessed and re-approved if necessary.

# Policy Enforcement

1. Policy document sponsor and owner: <Head of Cyber Security Department>.
2. Policy implementation and enforcement: <Department Concerned with Information Technology>.
3. Any violation of this policy may subject the offender to disciplinary action as per the procedures followed in <entity name>.

-End of the Document-