**Logical Access Control Policy and Procedure**

Doc ID: POL/LACP

Document Classification: Internal

July 2022

**Document Control**

| Document Name | Organization of Information Security |
| --- | --- |
| Document ID | POL/LACP |
| 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 Introduction 4](#_heading=h.30j0zll)

[2.0 Purpose 5](#_heading=h.3znysh7)

[3.0 Scope 6](#_heading=h.3dy6vkm)

[4.0 Responsibility and Authority 7](#_heading=h.2s8eyo1)

[5.0 Policy and Procedure 8](#_heading=h.3rdcrjn)

[5.1 Access Control 8](#_heading=h.lnxbz9)

[5.2 Managing User Access 8](#_heading=h.35nkun2)

[5.2.1](#_heading=h.1ksv4uv) User Access to Information, Data and Application 8

[5.2.2](#_heading=h.44sinio) User Account Management 8

[5.2.3](#_heading=h.2jxsxqh) User ID Nomenclature 9

[5.2.4](#_heading=h.z337ya) Recording of User Ids 9

[5.2.5](#_heading=h.3j2qqm3) Privilege User ID Management 9

[5.2.5.1](#_heading=h.1y810tw) Privilege User ID maintenance procedure 9

[5.2.5.2](#_heading=h.4i7ojhp) Review of Privileges 10

[5.2.5.3](#_heading=h.2xcytpi) Privileged Password Management Procedures 10

[5.2.5.4](#_heading=h.1ci93xb) Emergency User ID Management Procedures 11

[5.2.5.5](#_heading=h.3whwml4) Review of User Access Rights 11

[5.2.6](#_heading=h.2bn6wsx) Access Logs 11

[5.2.7](#_heading=h.qsh70q) Managing User IDs 11

[5.2.8](#_heading=h.3as4poj) Password Management 12

[5.2.8.1](#_heading=h.49x2ik5) Password Allocation Process 13

[5.2.8.2](#_heading=h.2p2csry) One time use of initial password 13

[5.2.8.3](#_heading=h.147n2zr) Password reset process 13

[5.2.8.4](#_heading=h.3o7alnk) Password confidentiality 13

[5.2.8.5](#_heading=h.23ckvvd) User capability to select passwords 13

[5.2.8.6](#_heading=h.ihv636) Renaming Administrator / Guest Account 13

[5.2.8.7](#_heading=h.32hioqz) Screen Saver password 13

[5.2.9](#_heading=h.1hmsyys) Ensuring Logical Security on Laptops and Desktops 13

[5.3 Controlling Privileged User IDs 13](#_heading=h.2grqrue)

[5.4 Usage of Sensitive System Utilities 14](#_heading=h.3fwokq0)

[5.4.1](#_heading=h.2u6wntf) Restricting Use of Sensitive System Utilities 14

[5.5 Operating System, Applications and Databases 14](#_heading=h.19c6y18)

[5.6 Monitoring Access and Usage 14](#_heading=h.3tbugp1)

[5.7 Synchronization of System Clocks 14](#_heading=h.28h4qwu)

[5.8 Revocation of Users Access Rights 15](#_heading=h.nmf14n)

[6.0 Reference Documents 16](#_heading=h.1mrcu09)

# Introduction

Electronic Information Systems and, the Business information stored and communicated via these systems, are essential resources for accomplishing {Company} business activities.

{Company} grants its employees shared/exclusive access to these resources in support of accomplishing the Company's mission.

These resources and information are valuable and confidential assets to be used and managed responsibly to ensure their integrity, reliability, and availability for appropriate business activities.

# Purpose

The purpose of this policy is to:

* Safeguard the integrity of computers, networks, and data, either owned by, or under the custody of {Company}
* Define the authorization and access rights of persons who can access the above systems and data
* Ensure that use of electronic communications complies with the Company policies
* Protect the Company against damaging legal consequences, through abuse of access accorded to computing resources

# Scope

This policy applies to

* Business information stored in and communicated via {Company} Electronic Information Systems
* Hardware consisting of server computers, personal computers, laptops, detachable storage media, etc.
* Network components, namely, routers, switches, server Networking equipment and other components.
* Software servers namely, operating systems, e-mail servers, database servers, application servers, multi-user business applications, stand-alone single-user business applications, etc.
* Note: IT systems (hardware/software) owned or under the custody of {Company} include but are not limited to systems at {Company} office premises in India / abroad, data-centers and data-centers elsewhere, and also systems leased out to vendors.

# Responsibility and Authority

The Head – IT is responsible for implementing the policy.

Management Representative / Information Security Officer for auditing the policy.

# Policy and Procedure

Logical access to the organization network shall be granted and revoked promptly based on the role of the employee/consultant/vendor/apprentice/contractor employee and periodically reviewed. Local Administrator privileges and superuser privileges to critical applications shall be restricted only to a few employees with authorization from their Delivery / Department Heads.

## Access Control

This access control process is to be followed for the following areas, but not limited to

* Network (LAN) access
* Internet access
* Application access

All creation and deactivation of the user account shall be performed by the said policy. The policy applies to the management (creation, modification, and deactivation) of:

* Active Directory accounts (user accounts as well as special accounts)
* Any other accounts that provide access to IT-managed systems, data, or applications

## Managing User Access

### User Access to Information, Data, and Application

* User’s shall be granted access to information, data, and applications strictly on a "need to know" basis.
* Any change in access privileges shall be carried out only after approval by appropriate personnel, by using a formal documented process.
* Segregation of duties shall exist between information access requestors, information access approvers, and those implementing access changes. Each of these roles is limited to a pre-defined group and only those specifically given the responsibility shall be allowed to either request or approve access.

### User Account Management

* There is a formal user registration procedure for granting logical access and privileges to all multi-user information systems and services.
* New users and their access rights to Operating Systems, Applications, Databases, and Network Levels shall be implemented based on formal authorizations by the respective Delivery Heads / Department Heads based on the job requirements of the user.
* The IT Team shall be responsible for allocating and managing the user access rights on the folders.
* Only the IT Team shall have local administrator privileges to desktops and servers as per business needs. For other employees, the local administrator privileges should be provided as per the Change Control Procedure and on authorization from the Delivery / Department Head.
* The IT Team shall create additional access rights to the project or department data on the Operating Systems, Applications, Databases, and Network Levels for the new user / existing user, based on the approval from the reporting managers.
* The following guidelines must be followed:
  + All users must have a unique user ID and it must not be shared between multiple people unless approved and signed off by the Department / Delivery Head / Management Representative for some specific business purpose.
  + The names of default accounts (like administrator) must be renamed, wherever possible, or deleted wherever applicable.
  + The user account created for an application such as local FTP must have a start and end date. The respective stakeholder must inform IT about the requisite details.

### User ID Nomenclature

* The user ID for systems must follow a nomenclature defined and documented in the system documentation for that system.
* The same nomenclature must be followed for all users within that system.
* User IDs that are being used for special purposes, like contractors or temporary accounts must be distinguished by adding an appropriate prefix to segregate these accounts from standard user accounts.

### Recording of User IDs

* The system administrators of all systems (not part of the Corporate Network) must create, maintain, and manage this list, as applicable.

### Privilege User ID Management

### Privilege User ID maintenance procedure

The following procedures must be maintained for the operation and maintenance of privileged user IDs that have high levels of authorization in critical systems:

* User IDs with special system privileges must be controlled and restricted to a limited number of authorized personnel.
* Privileged user IDs must include IDs, that are used to administer modifications to the operating system, security functions, and audit logs.
* Administrators must log on as themselves, using a normal user ID when performing a regular work duty rather than logging in as the supervisor/administrator. Logging in as the supervisor/administrator must be limited to administrative activities only.
* The IT Team should identify all the privileges associated with all Operating Systems, Business Applications, Databases, and Network elements used in the organization.
* These privileges should then be mapped with the job functions of the personnel to develop and document privileges in the Role Wise Privilege Matrix. In most Applications, Operating Systems, and Databases, privileges required for performing a job function are put together to create an application role for effective and secure management of access privileges. Wherever applicable, application roles should be created for each of the corresponding job functions in the organization.
* At the end of this exercise all access privileges required for a specific role shall have been identified and documented.
* This exercise should be carried out whenever an Application or Operating System or a Database or Network equipment is to be used for the first time.
* Role Wise Privilege Matrix should be modified in the following scenarios by the respective stakeholders:
  + When an Application, Operating System, Database, or Network Equipment undergoes a major change or a new module or functionality is added
  + A new job function or role is created
  + Job Function or Role is changed
* Privileges shall be granted to users on two occasions. One is by default during the creation of a user account and the second is when a user requests for additional privileges due to changes in job function or changes in responsibilities.
* Quarterly review of the privileges (i.e. access rights assigned to the folders on the servers vis-à-vis Access Control List) for various departments/support functions is performed by Local IT. The Access Control List Master is maintained by the IT team for various departments/support functions and is reviewed by the respective Department Head / Delivery Head on a quarterly basis
* Timely revocation of user access rights shall be ensured. The IT Team shall be responsible for the timely revocation of logical access rights on the domain (enterprise ID) and the business unit/project data, respectively based on the intimation received to this effect from HR, over mail.

### Review of Privileges

* The IT Team shall review the access control list master on a quarterly basis and audit the list of users in the database (domain controller) along with their access privileges as per the audit schedule. They shall verify:
  + Whether the privileges granted to the user are as per what is approved and documented.
  + Whether the privileges once granted are removed on the expiry date.
  + Whether any additional privileges are obtained in an unauthorized manner.
* Privileges like Administrator rights, internet access, etc. will have to be revalidated by the reporting manager at the expiry date as mentioned in the Change Request Form, whichever is earlier.

### Privileged Password Management Procedures

* All critical system passwords must be written on paper, put in envelopes, and stored securely under lock and key (Privileged Password Log Template)
* Below listed tables explain what type of passwords are called critical passwords. These passwords should be carefully managed to ensure that these passwords are not forgotten or lost:

| **System** | **Types of Password** |
| --- | --- |
| Operating Systems | Administrator Password (s) |
| Information Systems / Business Applications | Super User Password (where available)  Administrator Password  System Password (for database connectivity) where available |
| Databases | Database Super User Password  Database Administrator Password  Database Security Officer Password |
| Networking Components | Access Password (s)  Administrator Password (s) |
| External Websites | Access Password (s) |

* The password envelope must be sealed, signed across all openings seams and taped with transparent sticky tape – to ensure that any attempt to open the envelope should be immediately apparent.
* These envelopes should be placed in the company safe and in the custody of the Head – of IT and/or Department / Delivery Head. These passwords shall be used in case of emergency only. The distribution list shall be maintained and signed off.
* The use of the password stored in the envelope must be logged, and the password must be changed immediately after use (within 12 hours). (Privileged Password Log Template).
* The following information must be documented on the face of the envelope:
  + User Name, Department / Project and Designation
  + Name / Identity of the Application, Operating System or Database for which the password has been lodged
* The custodian of the stored passwords should only release the password to the following persons under the following circumstances:

| **Password released to** | **Circumstance / Reason** | **Authorization requirement** |
| --- | --- | --- |
| Password Owner (as mentioned on the password envelope) | On request where:   * The password requires to be changed/replaced * The owner has forgotten the password | None |
| Systems Engineer | The owner of the password has become unavailable to the company (e.g. termination of service, resignation, death etc.) | Relevant Department / Delivery Head |

* Head – IT and/or Department / Delivery Head must monitor the password envelopes from time to time and ensure that:
  + All password envelopes are accounted for (in comparison to the password envelopes registered in the password log)
  + The password envelopes have not been tampered with
* If the Head – IT and/or Department / Delivery Head detects that password envelopes are missing or have been tampered with, then he should immediately instruct all relevant users to change their passwords with immediate effect and raise it as security incident.

### Emergency User ID Management Procedures

* Emergency IDs that have high-level access privileges must only be created and used in the event of extreme emergency.
* All emergency actions, that bypass normal access control procedures, must be logged and reported for immediate review by Department Head or Head – IT.
* Designated owners must be notified immediately of all emergency fixes and they must retrospectively review all emergency amendments to their production environment.

### Review of User Access Rights

* User access rights for all critical systems must be reviewed on a half-yearly basis.
* In case the authentication and authorization for an application are not being managed by a centralized active directory, then the application administrator managing the system shall prepare the list of application users and associated privileges. The list should be sent to the related Department Head for confirmation. The Department Head shall confirm the privileges and notify of any deviations. The application administrator shall rectify the deviations notified by the Department Heads.
* Authorizations for special privileged (Administrative) access rights must be reviewed at an interval of 6 months or earlier on a need basis. Head - IT shall review all the accounts with special privileges and notify any deviations to the IT Team for rectification.
* The user access rights must be reviewed when changes to the user’s normal duties are required, for example, as a result of resignation, termination, transfer, or promotion.

### Access Logs

* A reactive approach shall be adopted for log review where incidents shall be analyzed only when reported/requested and the report shall be submitted to the Head– of IT. In case of security breaches, the Incident shall be reported to the Management Representative as well.
* Logging of activity on organization equipment is limited and restricted, and this logging will only be used to troubleshoot technology and problems and to capture data to provide proof of illegal outside (external to the organization) activity. Capturing of data from internally identifiable computers will only be done after approval from the HR / Legal / Management Representative.

### Managing User IDs

* User IDs shall follow a standard naming convention for all computer systems to facilitate user identification. Naming conventions will cover all end users (employees/apprentices), contractors, consultants, and vendors. Generic IDs shall not be used.
* Access to information services shall be controlled by using unique user IDs, wherever possible, which will enable:
  + individual accountability
  + permit centralized identification of users
  + aid in timely control of potential threats
* The application/system administrators are responsible for identifying inactive accounts and disabling them. If a user account has been inactive for more than 30 days, the application/system administrator shall intimate the details to their respective Department Head / Delivery Head.
* "Guest" accounts and other default accounts shall be disabled on all servers.
* Each user is personally responsible for the usage of his or her user ID and password.

### Password Management

* An initial password shall be provided to the users securely during the user creation process and the system shall be configured to force the users to change the initial password immediately after the first login.
* Passwords shall be securely conveyed to users. Passwords shall never be disclosed via telephone or through third parties or unprotected (clear text) electronic mail.
* Password constraints and account policy shall be enforced for all user and administrative accounts on operating systems, applications, databases, and all other information protected by password controls.
* Users shall not choose passwords, which can be easily guessed such as the user’s name, car registration number, telephone number, birth date, etc.
* In case the user has forgotten the password, IT shall reset the user password based on user-request*.* The user must immediately change the reset password.
* Password shall be changed at least every 60 days or immediately if a user suspects that the password is leaked or compromised.
* All vendor-supplied default passwords (or other alternative access mechanisms) must be changed before any computer or communications system is used for any organization's business activity beyond initial evaluation in a test environment. These standards apply to passwords associated with end-user user IDs, as well as passwords associated with systems administrator and other privileged user IDs. In case of vendor-supplied password cannot be changed then exception approval from the Department / Delivery Head must be obtained. The same would be recorded in the Context and approval from MISF shall be obtained.
* Incorrect passwords will be automatically unlocked by the system after 30 minutes.
* Users can share the password with the team members, as needed, and with the understanding that they are accountable for their decisions and access to their accounts. This sharing can be done ONLY with pre-approval from the Department / Delivery Head and Management Representative
* Passwords should not be written down or left in a place where unauthorized persons might discover them.
* Passwords shall not be stored in unencrypted format in system resources.
* Appropriate procedures shall be put in place for storing and management of administrative passwords for critical information systems.
* Due to system limitations or business necessity if any of the password or logical access control policies cannot be followed, associated risks should be brought to the attention of the management, and exceptions shall be documented. Compensating controls shall be put in place to mitigate the associated risk
* Password Construction Requirements:
  + Changing Passwords: 60 days
  + Password History: Last 5 passwords
  + Failed Logon Attempts: 5 unsuccessful attempts
  + Password Unlock: After 30 minutes
  + Password Composition:
    - Length: 8 characters
    - Elements: Combination of 1 Upper Case, 1 Lower Case, 1 Number, 1 Special Character.

### Password Allocation Process

* The IT executive who has created the user ID shall set the initial password.
* To ensure that passwords are communicated only to relevant users, they must be communicated back to the originator of the request or the person to whom it is assigned.
* All initial passwords must be configured to “Force Modify” on the first usage.

### One-time use of initial password

* Wherever possible, the system will enforce a password change following the initial login.

### Password reset process

* Users/administrators over time may forget their passwords, in which case the same has to be reset. If the password reset is not done properly and securely, unauthorized users can ask for the password of authorized users to be reset and gain access to systems.
* If the account has been locked for some reason, to unlock the user account, the user must send a request to the IT team. Positive user identification is mandatory before any account is unlocked by the IT Team or by an automated system.
* The IT Team must confirm the request with the person who has requested the reset. After checking and confirming the details, the new password is allocated and confirmed back to the end user only. The user must immediately change the password.
* A log of password resets, for critical servers must be maintained for auditing purposes.

### Password confidentiality

User passwords are to remain confidential and not shared, pasted, or otherwise divulged in any manner. Users can, however, share the password with the team members, based on exceptional business needs and with the understanding that they are accountable for their decisions and the access to their accounts. This sharing can be done only with pre-approval from the Management Representative.

### User capability to select passwords

Users shall be provided with the capability to change their password on the login interface (after authentication).

### Renaming Administrator / Guest Account

All the administrator accounts and guest accounts shall be renamed.

### Screen Saver password

Password-protected screen saver shall be activated after 10 minutes of inactivity.

### Ensuring Logical Security on Laptops and Desktops

#### Securing Information on Laptops and Desktops

* The folders or disk drives in individual desktops or laptops shall not be shared unless appropriate access controls have been enabled on the folder or the disk drive. Sharing of any information classified as ‘restricted’ or ‘confidential’ is not permitted unless authorized by the concerned authority.
* If any removable devices need to be used then prior approval shall be taken from the Department Head / Delivery Head and Management Representative.

## Controlling Privileged User IDs

#### Use of privileged user IDs

* User IDs with high-level access privileges (administrators) shall only be used in the event of an emergency.
* System Administrator shall log on using their normal user ID when performing regular work duties rather than logging in as the administrator. Use of the Administrator profile shall be limited to administrative activities only.
* Passwords of such user IDs shall be stored in sealed envelopes in the company safe. This will ensure that an authorized employee has access to this password if the concerned person cannot be reached during an emergency.
* All emergency actions, that bypass normal access control procedures, shall be logged and reported for immediate review by delegated authority.

## Usage of Sensitive System Utilities

Sensitive system utilities are the utilities that give unrestricted access to critical system resources. The sensitive system utilities include but are not limited to Format, User addition/deletion/update, and Change in Network Settings.

### Restricting Use of Sensitive System Utilities

* Access to system utilities shall be restricted to authorized personnel by their business functions and business needs.
* All unnecessary sensitive utilities shall be removed/disabled from the system.
* The use of all system utilities shall be logged and reviewed by the IT Team in case of any incidents or breakdowns.
* It shall be ensured that normal users do not have access rights to use utilities. Any backend update to the data using SQL / similar utilities shall be done only after prior written approval.
* System utilities shall be separated from application software.

## Operating System, Applications, and Databases

* Head – IT shall ensure that all the installations of Operating Systems, Applications and Databases are configured as per MBSS defined:
  + All the policy requirements for Operating Systems, Applications and Databases as per the Access Control Policy
  + Restriction on use of various type of user accounts
  + Restriction on access advanced programs and utilities
  + Restriction on access to OS commands
* Head – IT is the owner of all security and system audit tools. The software shall be used only by the Head – of IT or a person designated by him. Access to this software shall be maintained as per the Account Management and Privilege Management procedure detailed in the document.

## Monitoring Access and Usage

* All user activities shall be logged by the Operating Systems, Applications, Databases, and network elements.
* Logging of activity on organization equipment is limited and restricted, and this logging will only be used to troubleshoot technology problems and to capture data to provide proof of illegal outside (external to the organization) activity. Capturing of data from internally identifiable computers will only be done after approval from the HR / Legal / Management Representative.

## Synchronization of System Clocks

* The correct setting of system clocks is important to ensure the accuracy of audit logs, which is required for investigations or as evidence in legal or disciplinary cases. Inaccurate, audit logs hinder such investigations and damage the credibility of such evidence. A system (for example, usage of NTP) shall be put in place to ensure that all the servers, network equipment, and desktops are synchronized at the same time. The system engineers and network engineers in charge of the network must ensure that users cannot change this setting.

## Revocation of User Access Rights

* Timely revocation of user access rights shall be ensured. The HR Team / IT Team shall be responsible for the timely revocation of logical access rights on the domain and the business unit/project data, respectively based on the intimation received to this effect from HR, over mail.

# Reference Documents

* ISMS Overview Policy
* Change Management Procedure
* ISO 27001:2013
* Statement of Applicability for ISO27001:2013
* Role Wise Privilege Matrix
* Privileged Password Log Template