Sunrise
Gilts & Securities (P) Limited

SUNRISE GILTS & SECURITIES PVT. LTD.

# PRIVILEGED IDENTITY MANAGEMENT (PIM) POLICY

(EFFECTIVE DATE: 10/06/2025)

SUNRISE GILTS & SECURITIES P. LTD. ★ AHMEDABAD

| | |
|---|---|
| **Author:** | PRATIK KUMAR MORE |
| **Owner:** | PRATIK KUMAR MORE |
| **Approved by:** | BOARD OF DIRECTORS |
| **Organization:** | SUNRISE GILTS & SECURITIES PRIVATE LIMITED |
| **Version No:** | 1.1 |
| **Approval Date:** | 28/05/2025 |
| **Effective Date:** | 10/06/2025 |

**Document Control**

**Document Title** **PRIVILEGED IDENTITY MANAGEMENT (PIM) POLICY**

**Version History**

| Version No. | Version Date | Author | Summary of Changes |
|---|---|---|---|
| 1.1 | 10/06/2025 | PRATIK KUMAR MORE | Review and Approval of BOD |

**Approvals:**

| Name | Title | Approval Date | Version No |
|---|---|---|---|
| PRATIK KUMAR MORE | PRIVILEGED IDENTITY MANAGEMENT (PIM) POLICY | 28/05/2025 | 1.1 |

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMEDABAD

# PRIVILEGED IDENTITY MANAGEMENT (PIM) POLICY

## 1. Purpose:

The purpose of this policy is to define controls for managing privileged user accounts in order to reduce the risk of unauthorized access, misuse of systems, and compromise of sensitive data.

Privileged accounts have elevated rights and therefore pose higher security risk if misused.

## 2. Scope:

This policy applies to:

- All IT systems, servers, applications and databases.
- All Directors, employees, IT administrators, consultants and vendors.
- All privileged or administrative accounts.

This policy is applicable to **Proprietary Trading systems and infrastructure only**.

## 3. Definition of Privileged Accounts:

Privileged accounts include:

- System administrators
- Database administrators
- Network administrators
- Root / superuser accounts
- Application admin accounts
- Any account with elevated system or application access rights

## 4. Policy Statement:

The Company shall ensure that:

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

- Privileged access is granted strictly on a **need-to-use basis**.
- Number of privileged accounts is kept to **minimum**.
- Privileged access is approved by authorized management.
- Privileged access is periodically reviewed and monitored.

## 5. Authorization & Approval:

- All privileged access must be approved by the **Director / IT Head**.
- No user shall have privileged access without documented authorization.
- Access rights shall be properly recorded and maintained.

## 6. Segregation of Duties:

To avoid conflict of interest and misuse:

- System administrators shall not perform trading operations.
- Trading users shall not have system administrator rights.
- Compliance and audit roles shall be segregated from IT administration.

## 7. Access Controls:

The Company shall implement:

- Unique user IDs (shared IDs shall be avoided wherever possible).
- Strong password controls.
- Two-factor authentication wherever technically feasible.
- Periodic password changes.

## 8. Monitoring & Logging:

The Company shall:

- Maintain logs of privileged user activities.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

- Monitor login, access and configuration changes.
- Investigate any suspicious or unauthorized activity.
- Retain logs for minimum **1 year**.

## 8A. Password & Access Control Standards:

The Company shall enforce the following minimum password and access control standards for all systems, applications and privileged accounts:

| Control | Standard |
|---|---|
| Password Expiration | Every 90 days |
| Minimum Password Length | 8 characters |
| Password Complexity | Enabled (combination of upper case, lower case, number and special character) |
| Password History | Last 4 passwords cannot be reused |
| Account Lockout | After 5 unsuccessful consecutive login attempts |
| Lockout Duration | 30 minutes |
| Renewed Login | After 30 minutes of inactivity or as enforced by system administrator |
| Screensaver | Activated after 10 minutes of inactivity and password protected |

These controls shall be configured at system level wherever technically feasible and shall be reviewed periodically by the IT Administrator.

## 9. Review & Revocation of Access:

- Privileged access shall be reviewed at least **quarterly**.
- Access shall be revoked immediately in case of:
  - Resignation
  - Role change
  - Termination
  - Completion of assignment

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

## 10. Emergency Access:

- Emergency privileged access shall be granted only with:
  - Management approval
  - Proper documentation
- Emergency access shall be:
  - Time-bound
  - Logged
  - Reviewed after use

## 11. Third Party Access:

- Third party vendors shall be granted access only:
  - For specific purpose
  - For limited duration
  - Under confidentiality agreement
- Their access shall be revoked after completion of work.

## 12. Training & Awareness:

All privileged users shall:

- Be trained on information security responsibilities.
- Be made aware of risks and consequences of misuse.

## 13. Violation & Disciplinary Action:

Any misuse of privileged access may result in:

- Disciplinary action
- Suspension or termination
- Legal or regulatory action, if required

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

## 14. Policy Review:

This policy shall be reviewed annually or upon regulatory or system changes.

## 15. Approval:

This policy is approved by the Directors of Sunrise Gilts & Securities Pvt. Ltd.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD