# SUNRISE GILTS & SECURITIES PRIVATE LIMITED

# IT ASSET MANAGEMENT POLICY

### (EFFECTIVE DATE: 10/06/2025)

| 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**     IT Asset Management Policy

## Version History

| Version No. | Version Date | Author | Summary of Changes |
|---|---|---|---|
| 1.0 | 13/06/2019 | PRATIK KUMAR MORE | NA |
| 1.1 | 10/06/2025 | PRATIK KUMAR MORE | Review and Approval of BOD |

## Approvals

| Name | Title | Approval Date | Version No |
|---|---|---|---|
| PRATIK KUMAR MORE | IT Asset Management Policy | 13/06/2019 | 1.0 |
| PRATIK KUMAR MORE | IT Asset Management Policy | 28/05/2025 | 1.1 |
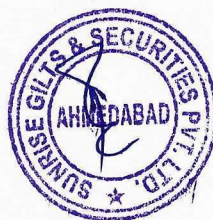
# 1.0 IT ASSET MANAGEMENT POLICY

## 1.1 PURPOSE

Purpose for defining this policy includes:

- Identify, categorize and classify Assets
- To educate users about the importance of protecting assets
- To identify procedures that shall be in place to protect the confidentiality, integrity and availability of the organization Information

## 1.2 SCOPE

This policy applies to:

All staff and non-employees, stakeholders of SUNRISE GILTS & SECURITIES PRIVATE LIMITED and other individuals, entities or organizations that have access to and uses SUNRISE GILTS & SECURITIES PRIVATE LIMITED's information processing systems to perform their daily job-related responsibilities.

## 1.3 POLICY STATEMENTS

SUNRISE GILTS & SECURITIES PRIVATE LIMITED has the responsibility in protecting the information assets from unauthorized access, generation, modification, disclosure, transmission or destruction. In order to ensure the security, reliability, integrity, and availability of information, appropriate asset handling scheme for labels shall be adopted by SUNRISE GILTS & SECURITIES PRIVATE LIMITED.

- Any asset acquisition or disposition should be performed only based on approvals from Technology Committee and Designated Officer
- All the assets shall be identified, and an inventory of these assets should be drawn up and maintained by Technology Committee.
- The inventory of assets shall minimum have the following details:

  - Asset Id – Unique id for tracking the asset
  - Asset Name and Description
  - Asset Location
  - Nominated Owner & Custodian of the asset

o Asset Value (High, Medium and Low)

## 1.3.1 IT ASSETS OWNERSHIP

The asset owner shall:

- Ensure that assets are appropriately classified (High, Medium or Low on basis of Confidentiality, Integrity and Availability) and protected.
- Define and periodically review access restrictions and classifications to important assets, considering, applicable access control policies.
- The asset owner shall be responsible for approving access and the level of access permitted for information assets under his/her ownership.

## 1.3.2 IT ASSETS GROUPING

Assets for SUNRISE GILTS & SECURITIES PRIVATE LIMITED shall be grouped under the following asset types:

- IT Infrastructure Assets - Network devices, security devices, servers, server racks, backup media, printers, biometric devices, desktops, laptops etc.
- Software Assets - Business applications, operating systems, database, executable files, etc.
- Electronic Information Assets – Internet links, MPLS links, E-mails, Contracts, Agreements, etc. in electronic format.
- Information classification must be reviewed at least once a year and signed off by the respective department heads.

## 1.3.3 IT INFORMATION ASSETS CLASSIFICATION

All the information assets shall be categorized under one of the following four classification levels

:

| Classification Level | Description |
|---|---|
| Restricted | Data / Information that is very critical or sensitive in nature and needs to be available only to the identified members of top management. If this data is lost or disclosed to unauthorized persons could lead to significant adverse impact, financial loss, penalties.<br><br>Examples include statutorily protected and sensitive information and information such as customer forms, strategic plans/ financial information, Merger and Acquisition information and investigation reports and findings. |
| Confidential | Data / Information which is of importance to department or teams within SUNRISE GILTS & SECURITIES PRIVATE LIMITED and cannot be shared with non-members of the department or team. The unauthorized modification or destruction of this information can affect the confidentiality, integrity or adversely impact SUNRISE GILTS & SECURITIES PRIVATE LIMITED or hamper the operations |
| Internal | Data / Information which must be confined only to SUNRISE GILTS & SECURITIES PRIVATE LIMITED staff and not to be disclosed to outside parties / public, including clients. It includes, but is not limited to, routine correspondence, employee newsletters, internal phone directories, inter-office memoranda, non-person identifiable information, organization policies and procedures. |
| Public | Data / Information that is available to the general public and is intended for distribution outside SUNRISE GILTS & SECURITIES PRIVATE LIMITED. Public Information includes, but is not limited to, various services, marketing brochures and promotional literature, advertising media and SUNRISE GILTS & SECURITIES PRIVATE LIMITED 's web site. |

## 1.3.4   IT ASSETS LABELLING

- All assets of SUNRISE GILTS & SECURITIES PRIVATE LIMITED shall be prominently labelled to ensure that they are given the necessary protection in use, storage and transport.

- All information, data, documents shall be clearly labelled so that all the users are aware of the ownership and classification of the information.

## 1.3.5   IT ASSET INSPECTION, ACCEPTANCE, DISTRIBUTION & INSTALLATIONS

- Physical assets shall be received by Shipping/Receiving and forwarded to Tech Support.

5
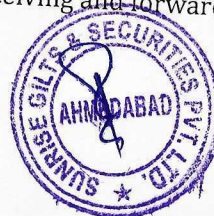
- Tech Support shall inspect and test assets for performance and capability prior to acceptance.
- When a nonconforming asset is identified, Tech Support shall report the nonconformity to the Purchasing Officer.
- The Purchasing Officer shall contact the vendor for replacement of the nonconforming asset and dispose of the nonconforming asset in accordance with any purchase/lease agreement in place.
- Only Tech Support shall distribute and install Information Technology assets.
- On installing hardware, Tech Support shall give each item a unique asset identifier. And shall update IT Asset Inventory and IT Network Architecture Diagram after installing assets.

## 1.3.6   IT ASSET RECORDS RETENTION & STATUS VERIFICATION

- Records are information created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligation/standard requirement or in the transaction of business.
- Retention period for all records shall be clearly identified by the owners and documented.
- The Designated Officer shall conduct a periodic assessment of Information Technology assets to verify their status (i.e., in use/not in use) and shall take corrective action.

## 1.3.7   MEDIA HANDLING

- Media should be disposed of securely when no longer required.
- Media containing information should be protected against unauthorized access, misuse or corruption during transportation.
- Upon disposal of said assets, Asset Management shall update IT Asset Inventory and IT Network Architecture Diagram.