SUNRISE GILTS & SECURITIES PRIVATE LIMITED

IT ACCESS CONTROL 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 **IT Access Control 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	ApprovalDate	Version No
PRATIK KUMAR MORE	IT Access Control Policy	13/06/2019	1.0
PRATIK KUMAR MORE	IT Access Control Policy	28/05/2025	1.1

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

IT Access Management Policy

Purpose

The purpose of this policy is to establish the framework and the rules for controlling logical access of SUNRISE GILTS & SECURITIES PRIVATE LIMITED users to the information processing systems of SUNRISE GILTS & SECURITIES PRIVATE LIMITED.

Scope

This policy applies to all staff and non-employees and other individuals, entities or organizations responsible for administering and maintaining SUNRISE GILTS & SECURITIES PRIVATE LIMITED's IT infrastructure.

Policy Statement of Logical Access

The Company shall control access to its information to help ensure its confidentiality and integrity.

Access Control

- Access shall be provided to meet following two principles of Role Based Access Control:
    - Need-to-know: granted access to the information you need to perform your tasks (different tasks/roles mean different need-to-know and hence different access profile)
    - Need-to-use: granted access to the information processing facilities
- There must be a formal user access provisioning and de-provisioning procedure for granting access to information, information processing systems and IT services.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

- All users shall have controlled access (read, write, modify, execute, full control) to information processing systems, in accordance with the user's functional role and information security requirements.
- For Contract Employees, Interns and Consultants, the validation of the ID must be only for the period of contract and must be automatically de-activated thereafter. There must also be a periodic review of the same.
- A record of disabled accounts must be maintained by the Designated Officer & Technology Committee.
- All information processing systems shall be configured to enable audit logs.

User ID

- Unique user IDs shall be assigned to each user for the purpose of their job roles and responsibilities.
- SUNRISE GILTS & SECURITIES PRIVATE LIMITED's IT administrator is responsible for creation of all SUNRISE GILTS & SECURITIES PRIVATE LIMITED's User IDs.
- All User IDs shall follow a standard naming convention defined as a part of this policy:
  - For SUNRISE GILTS & SECURITIES PRIVATE LIMITED employees (permanent and contractual basis) the naming convention is <First Name>Dot<<Last Name>
  - If the User ID already exists, <First Name>DOT<Last Name><Numeric Value> shall be considered.
- User-IDs and related passwords shall not be shared with any other individual.
- User-IDs must be disabled and deactivated when the user leaves SUNRISE GILTS & SECURITIES PRIVATE LIMITED.
- Anonymous user-ids (such as "Guest") must not be allowed.
- Common user-IDs must not be issued to multiple users. In situations where a common ID is required, written permission shall be taken from Senior Management and Designated Officer.
- Default user-IDs and passwords shipped with information processing systems and software applications must be disabled.
- User-ID that is inactive for a maximum period of 60 days shall be disabled after seeking the approval from the user's reporting manager and/or Designated Officer.

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMEDABAD

Privilege Management

- All privileges to the users shall be assigned through a formal access provisioning procedure
- Designated Officer shall ensure that no privileges are assigned before access request is approved by his/her reporting manager.
- Privileges that are temporarily granted shall be authorized and tracked. Such privileges shall be revoked as soon as they are deemed not required.
- Designated Officer shall maintain detailed records for all allocated privileges.

Review of Access Rights

- Designated Officer in coordination with Technology Committee shall review all user access rights at least every 12 months.
- Designated Officer shall review access logs, security logs, etc., on a periodic basis (once in 6 months is recommended). Findings of such reviews shall be reported to senior management for their review and possible action.
- Privileged accounts shall be reviewed by the Designated Officer at least every 6 months, and changes to such accounts shall be logged for periodic review.

Network Access Control

- Access to networks and network services shall be specifically requested by the user's reporting manager and reviewed by Designated Officer.
- Remote user access to SUNRISE GILTS & SECURITIES PRIVATE LIMITEDnetwork shall be subjected to appropriate user authentication and cryptographic controls, for example, use of VPN (virtual private network) connectivity and two factor authentication / security tokens.

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMADABAD

- Wireless networks and publicly accessible systems shall be segregated from the rest of the internal network.
- Wireless networks shall be secured by binding each IT asset's physical address (MAC address binding) on wireless access point.
- Groups of information processing systems, services and users shall be segregated on networks based on their sensitivity and classification of information stored or processed, exposure to public networks/users and corresponding risk levels.
- Access between the segregated network segments shall be appropriately controlled.
- Use of Network services shall be continuously monitored.
- SUNRISE GILTS & SECURITIES PRIVATE LIMITED shall formulate an internet access policy on content filtering proxy device to monitor and regulate the use of internet and internet-based services such as social media sites, cloud-based internet storage sites, etc. within their critical IT infrastructure.

Secure log-on

Secure log-on shall be implemented for systems and applications, as follows:

- Information processing systems shall suspend the user account and prevent user access to the system when an incorrect user password has been entered for specific number of times
- All actions performed by an individual on system programs shall be logged.
- All systems shall be locked, or sessions terminated after a defined time of inactivity.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

measures for application authentication security

- Any Application used by SUNRISE GILTS & SECURITIES PRIVATE LIMITED containing sensitive, private, or critical data such as IBTs, SWSTs, Back office etc. referred to as "Application" over the Internet shall be password protected.
    - Strong password policy must be followed as per company's policy.
- Passwords, security PINs etc. shall never be stored in plain text and shall be one-way hashed using strong cryptographic hash functions before being stored in database.
- For added security, a multi-factor e.g. two-factor authentication scheme shall be used. In case of IBTs and SWSTs, two-factor authentication is mandatory.
    - In case of Applications installed on mobile devices (such as smart phones and tablets), a cryptographically secure biometric two-factor authentication mechanism shall be used.
- Post multiple failed login attempts into Applications, the Customer's account should be locked out.
- SUNRISE GILTS & SECURITIES PRIVATE LIMITED hall focus on strong multi-factor authentication for security and educate Customers to choose strong passphrases.
    - Customers may be reminded within 60 days intervals to update their password.
- Login attempts to system much be logged for both successful and failed attempts.
- CAPTCHAs can be implemented for limiting the bruteforce attack and enumeration attacks against logins.

SUNRISE GILTS & SECURITIES PVT. LTD. ★ AHMEDABAD