SUNRISE GILTS & SECURITIES PRIVATE LIMITED

BYOD POLICY

(EFFECTIVE DATE: 10/06/2025)

SUNRISE GILTS & SECURITIES PVT. 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 **BYOD 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	BYOD Policy	13/06/2019	1.0
PRATIK KUMAR MORE	BYODPolicy	28/05/2025	1.1

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

BYOD Policy

1.1 PURPOSE

Many employees and other contractors / vendors of the SUNRISE GILTS & SECURITIES PRIVATE LIMITEDuses personally owned computing devices to accomplish their work. This policy addresses the rights and obligations of both owners of a device used for official work and the SUNRISE GILTS & SECURITIES PRIVATE LIMITED's rights and obligations to protect and secure its data residing on these devices.

1.2 SCOPE

This policy applies to:

- All Staff (Permanent & on contractual basis) and non-employees (contractors, consultants, suppliers, vendors, etc.) of SUNRISE GILTS & SECURITIES PRIVATE LIMITED and other individuals, entities or organizations that uses or brings their own devices to accomplish official work

All mobile computing devices (Laptops, Smart phones, Tablets, PDAs etc.) that are used to access SUNRISE GILTS & SECURITIES PRIVATE LIMITED network environment

1.3 POLICY STATEMENTS

Company employees and contractors may use their personal electronic devices (e.g., smart phones, tablets) for conducting company business, provided that they understand and agree with the "Bring Your Own Device" (BYOD) policy, have been granted express permission, and act in accordance with the policy.

1.3.1 BACKGROUND

SUNRISE GILTS & SECURITIES PRIVATE LIMITED management fully understands that Bring Your Own Device (BYOD) program is associated with a few information securities risks such as:

- Loss, disclosure or corruption of corporate data on Personally Owned Devices (PODs)
- Incidents involving threats to, or compromise of, the SUNRISE GILTS & SECURITIES PRIVATE LIMITED network infrastructure and other information assets (e.g. malware infection or hacking)

- Non-compliance with applicable laws, regulations and obligations (e.g. privacy or piracy)

1.3.2 GENERAL STATEMENTS

- Due to SUNRISE GILTS & SECURITIES PRIVATE LIMITED management's concerns about information security risks associated with BYOD, individuals who wish to opt-in to BYOD must be first authorized by Technology Officer and must explicitly accept the requirements laid out in this policy beforehand.
- SUNRISE GILTS & SECURITIES PRIVATE LIMITED Management reserves the right not to authorize individuals, or to withdraw the authorization, if they deem BYOD program is not appropriate for them and in the best interests of the organization.
- The SUNRISE GILTS & SECURITIES PRIVATE LIMITED shall continue to provide its choice of fully owned and managed mobile computing devices (Laptops or smart phones) as necessary for work purposes, so there is no compulsion for anyone to opt-in to BYOD if they choose not to participate in the scheme.
- The SUNRISE GILTS & SECURITIES PRIVATE LIMITED and the owners and users of Personally Owned Devices (POD) share responsibility for information security.
- Personally, Owned Devices must not be used to create, modify, store or communicate corporate data without prior approval.
- Personally, Owned Devices (POD) must use appropriate forms of device authentication approved by Technology Officer, such as digital certificates created for each specific device. Digital certificates must not be copied to or transferred between PODs.
- BYOD users must use appropriate forms of user authentication approved by Technology Officer, such as userIDs, passwords and authentication devices.
- The following classes or types of corporate data are not suitable for BYOD and are not permitted on PODs:
    - Anything classified as Confidential or above (Restricted)

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

  - Other currently unclassified but highly valuable or sensitive corporate information which is likely to be classified as Confidential or above
  - Large quantities of corporate data on single device (i.e. greater than 1 GB in aggregate on any one POD or storage device).

- The SUNRISE GILTS & SECURITIES PRIVATE LIMITED has the right to control its information. This includes the right to backup, retrieve, modify, determine access and/or delete corporate data without reference to the owner or user of the POD.
- The SUNRISE GILTS & SECURITIES PRIVATE LIMITED has the right to seize and forensically examine any POD believed to contain, or to have contained, corporate data where necessary for investigatory or control purposes.
- Suitable antivirus software approved by Technology Officer must be properly installed and running on all PODs.
- POD users must ensure that valuable corporate data created or modified on PODs are backed up regularly, preferably by connecting to the corporate network and synchronizing the data between POD and a network drive, otherwise on removable media stored securely.
- Any POD used to access, store or process sensitive information must encrypt data transferred over the network (e.g. using SSL or a VPN) and while stored on the POD or on separate storage media, whatever storage technology is used (e.g. hard disk, solid-state disk, CD/DVD, USB/flash memory stick, floppy disk etc.).
- Owners should report theft or lose of POD or mobile devices to Technology Officer or IT Service Desk

1.3.3 RESPONSIBILITIES

- While SUNRISE GILTS & SECURITIES PRIVATE LIMITED users (employees / non-employees) have a reasonable expectation of privacy over their personal information on their own equipment, the organization's right to control its data and manage PODs may occasionally result in support personnel unintentionally gaining access to their personal

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD

information. To reduce the possibility of such disclosure, POD users are advised to keep their personal data separate from business data on the POD in separate directories, clearly named (e.g. “Private” or “BYOD”).

- It is responsible for issuing digital certificates to authenticate authorized PODs, and for monitoring network security for unauthorized access, inappropriate network traffic etc.
- Technology Officer is responsible for managing the security of corporate data and configuring security on authorized PODs.
- IT Help/Service Desk is responsible for providing limited support for BYOD on PODs on a ‘best endeavors’ basis for work-related issues only. Information security incidents affecting PODs used for BYOD should be reported promptly to IT Help/Service Desk in the normal way.

SUNRISE GILTS & SECURITIES PVT. LTD.
AHMEDABAD