SUNRISE GILTS & SECURITIES PRIVATE LIMITED

IT COMPUTER MALWARE 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 Computer Malware 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 Computer Malware Policy	13/06/2019	1.0
PRATIK KUMAR MORE	IT Computer Malware Policy	28/05/2025	1.1

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

1.0 IT COMPUTER MALWARE POLICY

1.1 PURPOSE

Malicious codes such as viruses, worms, Trojans, spy ware, root-kits etc. represent a significant threat to the performance and security of SUNRISE GILTS & SECURITIES PRIVATE LIMITED IT assets and services dependent on these assets.

1.2 SCOPE

All staff and non-employees (contractors, consultants, suppliers, vendors etc.) of SUNRISE GILTS & SECURITIES PRIVATE LIMITED and other individuals, entities or organizations that have access to and use SUNRISE GILTS & SECURITIES PRIVATE LIMITED IT systems and IT Services in order to perform their daily job-related responsibilities or meet their contractual obligations

1.3 POLICY STATEMENTS

All servers, desktops, laptops and hand-held devices of SUNRISE GILTS & SECURITIES PRIVATE LIMITED must be protected against malicious code using enterprise level Anti-virus solution. The Anti-virus solution suite must ensure early detection, efficient containment and eradication of malicious code. Anti-virus software must be used on all systems commonly affected by malicious code to protect systems from current and evolving malicious software threats.

1.3.1 SELECTION OF ANTI-VIRUS

- Technology Committee shall identify suitable and reliable anti-virus software available.
- Selected anti-virus software shall be capable to detect, remove and protect against all known types of malicious software (for example viruses, Trojans, worms, spy ware, ad-ware and root kits)
- The Anti-virus enterprise solution must support signature update rollback

1.3.2 INSTALLATION & CONFIGURATION

- All servers, desktops, laptops and hand-held devices shall have anti-virus agent installed and configured before they are connected to the network.
- Anti virus agent installation shall be password protected to ensure that end users cannot uninstall the agent or change any settings or to disable the agent.
- Anti-virus agent shall be configured for full system scan the machine once in a week. The time of scanning can be either when the system boots up or during non-peak usage hours depending on load on various departments in SUNRISE GILTS & SECURITIES PRIVATE LIMITED.
- Anti-virus agent shall be configured to do a real time scan of all the files when they are accessed, copied or moved. This will ensure that all viruses are detected before they get activated.
- Anti-virus agent shall be configured to scan all removable disks before use.
- Anti-virus agent shall be configured to quarantine virus infected files if they cannot be cleaned.
- Anti-virus administrator shall submit periodic reports (weekly & monthly) on the status of the Anti-virus protection to Designated Officer.
- The report shall include the following at a minimum:
  - Number of PC's / Servers / Laptops not updated with the latest signature patterns.
  - Top 10 viruses detected in the SUNRISE GILTS & SECURITIES PRIVATE LIMITED network.
  - Number of viruses/worms/malicious programs detected.
  - Number of viruses/worms/malicious programs cleaned/quarantined.
  - Action taken to resolve the virus infection
  - Number of systems without the software installed
  - Number of systems without the latest signature patterns

1.3.3 ANTI-VIRUS SIGNATURE UPDATE

- The design of the Anti-virus application architecture shall ensure that all systems across the SUNRISE GILTS & SECURITIES PRIVATE LIMITED are updated with latest signatures within 72 hours from the time of release
- All systems on the SUNRISE GILTS & SECURITIES PRIVATE LIMITED network shall be configured to receive the signature updates from offline updates.

1.3.4 EXTERNAL USERS

- External users (including consultants, vendors, customers and service providers) who bring laptops/desktops/servers into SUNRISE GILTS & SECURITIES PRIVATE LIMITED premises shall not be allowed to connect to the SUNRISE GILTS & SECURITIES PRIVATE LIMITED network without prior approval from the relevant Department Heads and Designated Officer.
- SUNRISE GILTS & SECURITIES PRIVATE LIMITED Department shall verify whether vendor owned device has anti-virus installed and updated with latest signature pattern and that there are no active viruses.
- It shall also be checked whether all the necessary security patches have been installed. The device shall be allowed to connect only if all the above conditions have been met.

1.3.5 INCIDENT REPORTING

- In case of virus outbreak, anti-virus administrator shall take immediate steps to limit the extent of damage for recovering the systems with the help from the anti-virus solution vendor.
- Following steps shall be taken to ensure fast recovery:
  - Contact anti virus vendor for assistance in formulating the action plan

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- Take necessary steps to limit the spread of virus including configuring access lists on firewalls
- Take adequate steps to monitor the network for any traces of virus. This could include deployment of temporary intrusion detection systems or using vulnerability scanning tools.