Sunrise
Gilts & Securities (P) Limited

SUNRISE GILTS & SECURITIES PRIVATE LIMITED

INFORMATION SYSTEMS & CYBER SECURITY 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 **Information Systems & Cyber Security 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	Information Systems & Cyber Security Policy	13/06/2019	1.0
PRATIK KUMAR MORE	Information Systems & Cyber Security Policy	28/05/2025	1.1

Sunrise
Gilts & Securities (P) Limited

TABLE OF CONTENT

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

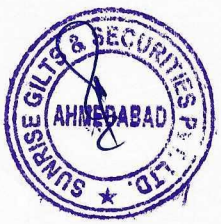
1.0 INTRODUCTION

Information and the supporting processes, systems and networks are important business assets.Increasingly, organizations and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, fire or flood. Sources of damage such as computer viruses, computer hacking, and denial of service attacks have become more common, more ambitious and increasingly sophisticated. Dependence on information systems and services means organizations are more vulnerable to security threats.

Information Security Management needs, as a minimum, participation by all employees in the organization.

1.1 OBJECTIVE & NEED

- The objective for developing and implementing Information Systems & Cyber Security Policies is to provide SUNRISE GILTS & SECURITIES PRIVATE LIMITED direction and support for information security in accordance with business requirements and relevant laws and regulations.
- Need for having Information Security Policies is listed below.
  - Regulatory and legal requirements – One of the most compelling reasons for developing formal policy is because it is mandated
  - Consistency – Similar problems are treated in a similar and consistent fashion
  - Fairness – Policies ensure that all users are treated fairly with respect to the level of access they may have
  - Understanding – Policies ensure that all involved parties understand clearly what is expected



2.0 INFORMATION SYSTEMS & CYBER SECURITY POLICY

2.1 PURPOSE

The purpose of Information Systems & Cyber Security Policy is to provide guiding principles and support to safeguard the information security in the organization. SUNRISE GILTS & SECURITIES PRIVATE LIMITED aims to ensure the appropriate confidentiality, integrity and availability of its data. The security policies contained in this document have been established to cover data and information assets at rest in the IT infrastructure or in transit over the communication networks owned and operated by SUNRISE GILTS & SECURITIES PRIVATE LIMITED.

2.2 SCOPE

This policy applies to:

- All staff (permanent & on contractual basis) and non-employees / stakeholders (interns, contractors, consultants, suppliers, vendors etc.) of SUNRISE GILTS & SECURITIES PRIVATE LIMITEDand other individuals, entities or organizations that have access to and use SUNRISE GILTS & SECURITIES PRIVATE LIMITED' information systems environment.
- SUNRISE GILTS & SECURITIES PRIVATE LIMITED staff, who are responsible for administering and maintaining SUNRISE GILTS & SECURITIES PRIVATE LIMITED' IT infrastructure.

2.3 INFORMATION SECURITY RESPONSIBILITIES

IT Committee shall be created. Chaired by a senior member of the Information Security or Information Technology management team, and will comprise the following members:

- Chair
  - Head of IT Security, or,
  - Head of Information Technology

- Members
  - Head of IT Applications
  - IT team member(s)
  - IS team member(s)
  - HR head or designated team member
  - Finance Head or designated team member

This Technology Committee should on a yearly basis review the implementation of the Information Systems and Cyber Security policy approved by the Board.

The technology committee of SUNRISE GILTS & SECURITIES PRIVATE LIMITED Equities should periodically review instances of cyber-attacks, if any, domestically and globally, and take steps to strengthen Cyber Security and cyber resilience framework.

2.4 INFORMATION SECURITY AUDIT

SUNRISE GILTS & SECURITIES PRIVATE LIMITED Equities shall arrange to have their systems audited on an annual basis by a CERT-IN empanelled auditor or an independent CISA/CISM qualified auditor to check compliance with all areas of information security and shall submit the report to Stock Exchanges / Depositories along with the comments of the Board of SUNRISE GILTS & SECURITIES PRIVATE LIMITED Equities within three months of the end of the financial year.

2.5 INFORMATION SECURITY POLICIES LIST

Following policies shall be developed as part of SUNRISE GILTS & SECURITIES PRIVATE LIMITED Information Systems Security guidance documentation. These policies, procedures, guidelines will be approved by SUNRISE GILTS & SECURITIES PRIVATE LIMITED senior management or Board as appropriate.

POLICY NO.	POLICY NAME
1	Information Systems & Cyber Security Policy
2	Acceptable Use Policy
3	Patch Management Policy
4	Teleworking Policy
5	Data Backup & Recovery Policy
6	Technical Vulnerability Management Policy
7	Cryptography and Encryption Policy
8	Application Development and Security Policy
9	User Awareness & Training Policy
OTHER POLICIES	
10	IT Asset Management Policy
11	IT Vendor Selection Policy
12	IT Threat-Risk Assessment
13	IT Access Control Policy
14	IT Incident Handling Policy
15	IT Business Continuity Plan
16	IT Computer Malware Policy
17	IT Security Audits Planner
18	BYOD Policy
19	E-Mail Policy
20	IT Outsourcing Policy
21	IT Records & Documents Management Policy
22	Physical Security Policy
23	HR Security Policy
24	Change Management Policy
25	Hardening Procedure

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

3.0 ACCEPTABLE USE POLICY

3.1 PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at SUNRISE GILTS & SECURITIES PRIVATE LIMITED.

3.2 SCOPE

This policy applies to the use of information, electronic and computing devices, and network resources to conduct SUNRISE GILTS & SECURITIES PRIVATE LIMITEDbusiness or interact with internal networks and business systems, whether owned or leased by SUNRISE GILTS & SECURITIES PRIVATE LIMITED, employee, or a third party. All employees, contractors, consultants, temporary, interns and other workers at SUNRISE GILTS & SECURITIES PRIVATE LIMITED and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources.

3.3 POLICY STATEMENT

General Use and Ownership, proprietary information stored on electronic and computing devices whether owned or leased by SUNRISE GILTS & SECURITIES PRIVATE LIMITED, the employee or a third party, remains the sole property of SUNRISE GILTS & SECURITIES PRIVATE LIMITED.

- Employees have a responsibility to promptly report the theft, loss or unauthorized disclosure of SUNRISE GILTS & SECURITIES PRIVATE LIMITEDproprietary information.
- Employees may access, use or share SUNRISE GILTS & SECURITIES PRIVATE LIMITEDproprietary information only to the extent it is authorized and necessary to fulfil their assigned job duties.
- Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- SUNRISE GILTS & SECURITIES PRIVATE LIMITEDreserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

3.3.1 SECURITY AND PROPRIETARY INFORMATION

- All mobile and computing devices that connect to the internal network must comply with the User Access Policy.
- System level and user level passwords must comply with the Password Policy Guidelines.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 10 minutes or less.
- Employees must lock the screen or log off when the device is unattended.
- Postings by employees from SUNRISE GILTS & SECURITIES PRIVATE LIMITEDemail address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of unless posting is during business duties.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

3.3.2 UNACCEPTABLE USE

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during their legitimate job responsibilities.

Under no circumstances an employee of SUNRISE GILTS & SECURITIES PRIVATE LIMITED is authorized to engage in any activity that is illegal under local, state, government or international law while utilizing SUNRISE GILTS & SECURITIES PRIVATE LIMITEDowned resources.

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software
- Accessing data, a server or an account for any purpose other than conducting SUNRISE GILTS & SECURITIES PRIVATE LIMITEDbusiness, even if you have authorized access.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others.
- Using SUNRISE GILTS & SECURITIES PRIVATE LIMITEDcomputing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any SUNRISE GILTS & SECURITIES PRIVATE LIMITED account.
- Effecting security breaches or disruptions of network communication.
    - Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access.
    - Disruption includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Executing any form of network monitoring which will intercept data not intended for the employee's host.
- Introducing honeypots, honeynets, or similar technology on the SUNRISE GILTS & SECURITIES PRIVATE LIMITED network.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session
- Providing information about, or lists of, SUNRISE GILTS & SECURITIES PRIVATE LIMITED employees and customers to parties outside SUNRISE GILTS & SECURITIES PRIVATE LIMITED

3.3.3 EMAIL AND COMMUNICATION ACTIVITIES

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

When using company resources to access and use the Internet, users must realize theyrepresent the company. The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

3.3.4 ALLOWED INTERNET USAGE

Internet usage is granted for the sole purpose of supporting business activities necessary to carry out job functions.Acceptable use of the Internet for performing job functions might include:

- Communication between employees and non-employees for business purposes
- IT technical support downloading software upgrades and patches
- Review of possible vendor websites for product information
- Use of social network websites for business purpose
- Reference regulatory or technical information
- Research

3.3.5 RESTRICTIONS ON INTERNET USAGE

The company prohibits acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

The company also prohibits the conduct of a business enterprise, political activity, engaging in fraudulent activities.

Other activities that are strictly prohibited include, but are not limited to:

- Using gambling related websites
- Unauthorized downloading of any shareware/freeware programs or files for use
- Any illegal use or unauthorized access or network scanning – both internal and external
- Any ordering (shopping) of items or services on the Internet
- Downloading through torrents or bulk file sharing websites
- Browsing pornographic and any inappropriate sites
- Downloading pirated software and graphics
- Forwarding of chain letters
- Participation in any on-line contest or surveys or promotion
- Acceptance of promotional gifts
- Deliberate pointing or hyper-linking of company Web sites to other Internet/www sites whose content may be inconsistent with or in violation of the aims or policies of the company.
- Any conduct that would constitute or encourage a criminal offense, lead to civil liability, or otherwise violate any regulations, local, state, national or international law
- Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization.
- Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.
- Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

3.3.6 CLEAN DESK POLICY

- Computer workstations must be locked when workspace is unoccupied.
- Computer workstations must be shut down at the end of the workday.

- Any Restricted or Sensitive information must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
- File cabinets containing Restricted or Sensitive information must be kept closed and locked when not in use or when not attended.
- Keys used for access to Restricted or Sensitive information must not be left at an unattended desk.
- Laptops must be either locked with a locking cable or locked away in a drawer.
- Passwords may not be left on sticky notes posted on or under a computer, nor may they be left written down in an accessible location.
- Printouts containing Restricted or Sensitive information should be immediately removed from the printer.
- Whiteboards containing Restricted and/or Sensitive information should be erased.
- Treat mass storage devices such as CDROM, DVD or USB drives as sensitive and secure them in a locked drawer
- All printers and fax machines should be cleared of papers as soon as they are printed; this helps ensure that sensitive documents are not left in printer trays for the wrong person to pick up.

3.3.7 SOFTWARE INSTALLATION POLICY

- Employees shouldnotinstallsoftwareonSUNRISE GILTS & SECURITIES PRIVATE LIMITEDcomputingdevices without prior approvals.
- Softwaremustbeselectedfromanapprovedsoftwarelist, maintainedbythe system admin ofSUNRISE GILTS & SECURITIES PRIVATE LIMITED
- For installation of software not present in approved list, employee should submit formal request to his/her manager, along with business justification for software usage.

4.0 PATCH MANAGEMENT POLICY

4.1 POLICY STATEMENT

4.1.1 IDENTIFICATION AND VALIDATION OF PATCHES

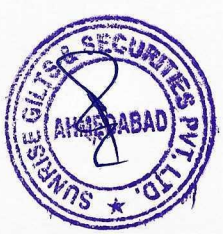
- System administrator and Application administrator of SUNRISE GILTS & SECURITIES PRIVATE LIMITED IT department are responsible for identification and validation of all patch related issues concerning their domain of work.
- Head of Information Technology, Head of IT Security, Head of IT Applications are responsible for approving all security related patches.
- To ensure that all patches are tracked, the administrator shall:
  - Subscribe to the trusted advisories, vendor's security patch mailing list or have agreements with vendors for receiving new security patches
  - Maintain an updated list of OS, application and database related patches released
  - Head of Information Technology or Head of IT Security shall validate whether the released patch is applicable to the environment
  - If the patch is affecting a service and is not implemented, system administrators shall track and keep a record of the discarded patches for future audit purposes

4.1.2 PATCH SCHEDULING & PRIORITIZATION

- Patches shall be tested and applied on priority basis based on their identified criticality.
- Criticality of Patches are as follows:
  - Critical: A vulnerability whose exploitation could severely impact the IT systems that provide services to critical business functions of SUNRISE GILTS & SECURITIES PRIVATE LIMITED.
  - High: A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of SUNRISE GILTS & SECURITIES PRIVATE LIMITED information.
  - Medium: A vulnerability whose exploitation would affect SUNRISE GILTS & SECURITIES PRIVATE LIMITED IT systems but on a controllable level.
  - Low: A vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

4.1.3 PATCH INSTALLATION

- All patches deployed in SUNRISE GILTS & SECURITIES PRIVATE LIMITED IT infrastructure (pre-production and production environment) must be performed as per change management process.



- Respective System administrators and vendors shall check whether the patch installation affects the operating system or application's functionality in a test environment, wherever applicable.
- If the tested patch is successful, it can be applied on the production environment, only after an approval from IT Management as per the change management process.

4.1.4 PATCH TRACKING

Respective IT Administrators shall maintain a patch tracking sheet which shall detail the list of patches that have been installed and the ones that are scheduled. Unapproved patches shall also be listed in Patch Tracking Chart with business justification.

5.0 DATA BACKUP & RECOVERY POLICY

5.1 POLICY STATEMENT

Management and system admin shall ensure that adequate data backup mechanism is in place to ensure that the data is not lost and can be recovered or restored in the event of an equipment failure, intentional destruction of data, or disaster.

5.1.1 BACKUP PROCESS

- Responsibility for data backup operations shall be assigned by System Admin.
- There shall be a documented backup and recovery procedure to back up the following:
  - Customer information
  - Source codes and executable of Application software
  - Data files of all application software
  - End-user document files like Photoshop, CAD or Microsoft Office documents etc.
  - Electronic mail
  - System software (operating system, RDBMS etc.)
  - Parameter and configuration files of networks and network devices, if applicable
  - System documentation likes user manuals, technical manuals etc.
- Backup scheduling shall be done to ensure that all critical data is backed up without affecting system operations. Preferably Backup shall be scheduled during non-peak hours

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- In case of the data exceeding the daily back up limits, appropriate type of backups like full, incremental or differential shall be scheduled and taken.
- Type and frequency of backup and type of backup media to be used shall be decided by the data owner in consultation with system admin taking into consideration the following parameters.
  - Volume of data
  - Criticality of data
  - Recovery time constraints
- Data shall be retained for the period necessary to satisfy both business and legislative requirements. Data owners shall assign the retention period for essential business data and establish any requirement for archive copies to be permanently retained.
- All backup media shall be properly labelled for identification and information classification. From the labelling it shall be possible to identify the following:
  - Server Hostname/IP address
  - Application Name
  - Date of Backup
  - Type of Backup
  - Media Expiry date
  - Location Name
  - Classification level
- A backup register shall be maintained by system administrator to track the backup and recovery operations
- The recovery register shall have following details:
  - Application name
  - Backup administrator name and User ID
  - Date of testing
  - Status
  - Comments

5.1.2 SECURITY OF BACKUP MEDIA

- Data on backup media shall be secured against unauthorized access.
- Backup media shall be secured against environmental and physical threats.

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- Backup media shall be stored in a fire resistant safe.
- Access to the fire resistant safe containing the backup media shall be restricted.
- Environmental conditions like dust, humidity, fire etc. shall be considered while selecting media storage room.
- Backup media shall not be exposed to direct sunlight or other heat radiating sources.
- Backup media shall be securely disposed.
- Backup media shall be disposed under the following conditions:
  - Media life has expired
  - Media is damaged, and data is not accessible

5.1.3 RECOVERY TESTING

- Recovery testing shall be done periodically to ensure the integrity of data being backed up and good health of backup tapes or media.
- Frequency of recovery testing shall be determined by management & system administrator.
- Frequency of recovery testing can be determined based on the following:
  - Criticality of the application
  - Existing Redundancy in place

6.0 TECHNICAL VULNERABILITY MANAGEMENT POLICY

6.1 POLICY STATEMENT

Management and system admin shall ensure that the assets are regularly verified for the vulnerabilities from the Information Security team. Adequate actions would be taken to mitigate the identified vulnerabilities.

6.1.1 CONTROL OF TECHNICAL VULNERABILITIES

Application and operating system vendors operate notification schemes which publish detailed information about any known vulnerabilities including regular updates and, normally, criticality ratings. The following points should be considered by SUNRISE GILTS & SECURITIES PRIVATE LIMITEDfor inclusion within the vulnerability management process:

- Roles and responsibilities for the process should be defined, including; monitoring, risk assessment, patching, asset tracking and coordination,

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- Sources of notifications should be identified for all SUNRISE GILTS & SECURITIES PRIVATE LIMITED' critical assets,
- Risk assessment of each relevant patch should have carried out to compare the risk of installing it against the risk of not doing so,
- Patches should be tested to ensure they are effective and do not adversely affect other system components,
- If a vulnerability is discovered and no patch is available other mitigating controls should be considered, including:
  - disabling services or capabilities related to the vulnerability,
  - adapting or adding compensating controls elsewhere i.e. disabling a port at a firewall or blocking a protocol,
  - increasing monitoring to detect and react to any attempted exploit,
  - raising awareness of the vulnerability to any potentially impacted users,
- Any high risk or particularly sensitive systems should be prioritized within the process.
- In case of vulnerabilities discovered in off-the-shelf products (used for core business) or applications provided by exchange empanelled vendors, SUNRISE GILTS & SECURITIES PRIVATE LIMITED Equities shall report them to the exchanges and Regulatory bodies like SEBI in a timely manner

7.0 CRYPTOGRAPHIC AND ENCRYPTION POLICY

7.1 POLICY STATEMENT

- Encryption shall be used wherever it is required to protect confidentiality, integrity and authenticity of the information, data and message.
- The encryption techniques shall identify agreed and applied before implementing them in the organization.
- The algorithms used shall be suitable for the business processes they are supporting.
- The key length shall be at least 128 bits. The length shall be appropriate for the security requirements of information that will be protected, and the solutions implemented shall be consistent throughout the organization.

7.1.1 RESPONSIBILITY

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- The responsibility for deciding cryptographic keys and the management of keys lies with the respective Application owners.
- The responsibility for implementing the required encryption or cryptographic techniques lies with the Application, Network and Database Managers
- The responsibility for securing the individual keys lies with the relevant managers. However, they shall hand them over before going on leave or leaving the organization

7.1.2 USE OF CERTIFICATES

- Digital certificates shall be used in transactions where there is need for authentication, non-repudiation and encryption.
- Certificates can be issued by SUNRISE GILTS & SECURITIES PRIVATE LIMITED' internal Certificate Authority or by an external party.

7.1.3 KEY MANAGEMENT GUIDELINES

- The key management system shall provide protection of the cryptographic keys according to their use, the management methods that support the handling and use of keys as required by the business processes for which these controls will be used.
- The requirements for key management shall be different depending on which cryptographic technique, secret or public key technique will be used and what type of key, public, private is considered.
- The protection of secret and private cryptographic keys is different from the protection necessary for the public keys. When defining a key management system, these protection requirements shall be analysed and appropriate protection shall be in place before the keys are generated and used.

7.1.4 CERTIFYING AUTHORITY KEY MANAGEMENT

- If SUNRISE GILTS & SECURITIES PRIVATE LIMITEDsets up an internal CA, the system shall be installed in secure location and the private keys shall be protected from unauthorized access.
- There shall be a secure backup of CA private keys.

7.1.5 KEY USAGE PERIODS

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- All certificates shall have pre-defined validity periods.
- Certificate renewal shall be processed as per new certificate generation guidelines.

7.1.6 KEY COMPROMISE

- If the CA private key has been compromised all subscriber certificates shall be revoked.
- If a subscriber private key is compromised CA shall immediately revoke the certificate.

8.0 APPLICATION DEVELOPMENT AND SECURITY POLICY

8.1 POLICY STATEMENTS – SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

Security shall be considered and included in all phases of the SDLC process namely Initiation / Requirement, Acquisition / Development, Testing, Implementation, Operations/Maintenance and Disposal. Depending upon the size and complexity of the project, phases may be combined or may overlap.

To ensure the segregation of roles involved in application development, testing and production, there may be three separate environments.

8.1.1 INITIATION / REQUIREMENT PHASE

- The business (the requesting department) is expected to provide the approved Business Requirements. All requirements need to be measurable and testable and relate to the business need.
- A risk analysis shall be performed to determine the threats associated and the corresponding security and quality controls required for the requested system or system application under development.
- It shall be ensured that there is a balance between user requirements and Security & Quality controls.
- Specifications for the new system shall be documented to provide the development group with specific requirements. This enables SUNRISE GILTS & SECURITIES PRIVATE LIMITED in identifying, reviewing and testing the security functionalities of the system or software.

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

8.1.2 ACQUISITION/ DEVELOPMENT PHASE

- The following points shall be considered at a minimum while preparing the detailed requirements for thesystem application:
    - Impact on existing systems
    - Security vulnerabilities involved when connecting with other systems and applications
    - Operating environment security
    - Cost of providing security to the system over its life cycle (includes hardware, software, personnel and training)
- While purchasing a system or software, the security requirements shall be specified in the Request for Proposal and the selection criteria shall be based on secure functionality.
- There shall be a separation between the operational, test and development facilities.
- Application controls shall be designed into all application systems to prevent loss, modification or misuse of user data. These controls shall include:
    - Validation of input data
    - Control of internal processing
    - Message Integrity
    - Validation of output data
- Where software development is outsourced, the following points shall be considered:
    - Licensing arrangements, code ownership and intellectual property rights
    - Certification of the quality and accuracy of the work carried out
    - Escrow arrangements in the event of failure of the third party
    - Rights of access for audit of the quality and accuracy of work done
    - Contractual requirements for quality of code
    - Testing before installation to detect backdoors or Trojan code
    - Meeting compliance regulations

8.1.3 TRAININGSAND MANUALS

- Manual: The updated system manual should be available for both users and technical team to use and/or support the system effectively.

- Training: The business/functional trainings to be provided for business users, UAT In-charge, Application Support and Technical training to be provided for other peers-in-Development, Application Support, and Technical Support/Operation, etc., for managing and supporting the system

8.1.4 TESTING PHASE

- All modifications, enhancements and installation of new systems shall be subject to testing for sanity, capacity, peak load, etc.
- The appropriate users shall do design testing and unit testing on the new systems prior to installation into the production environment.
    - Test Cases & Unit Test: The developers should prepare the test cases and do the adequate unit tests of their work before placing the work to the team leader
    - System Integration Test: The team leader should review/update test cases and test to ensure various components of the system are integrated and functioning as per the functional requirements.
- User Acceptance Testing
    - During User Acceptance Test, actual business user shall test the system to ensure that the business requirements,are satisfied by the developed or modified system
    - The implementation of operating systems, patches/upgrades, or standards systems in which there were no-customizations, however, must undergo compatibility check or certification to ensure that the production environment shall not be disturbed.

8.1.5 IMPLEMENTATION PHASE

Before the implementation of any new system, a security procedure document shall be prepared for the new system. It should contain hardware specification, prerequisites, implementation steps for client, server (UNIX, Windows, etc.), database, proposed system architecture showing interaction with other subsystems and data flow, application server, etc.

- For software packages, system default settings shall be reviewed prior to installation to determine potential security holes.

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- The system or system modifications shall be installed and made operational in a production environment using approved 'Implementation Specification'. The phase is initiated after the system has been successfully tested and accepted by the user and concerned parties during User Acceptance Phase.
- Different implementation approach such as Pilot, Soft Live, Parallel Run or Complete Live shall be selected depending on the project nature and complexity. The approach shall be approved by Section Head – Business Applications, Head of Information Security.
- The project manager shall arrange the handing over the system to 'Application Support' and hands over the details required for application support team required to carry out the support.

8.1.6 OPERATIONS/MAINTENANCE PHASE

- SUNRISE GILTS & SECURITIES PRIVATE LIMITEDIT Department shall maintain the system and perform identified IT Operations activities.
- The system shall be monitored by the users for continued performance in accordance with user requirements. The users shall record issue/problems and system modifications to the IT Department.
- All requisite procedures for operational tasks shall be documented. Access to this documentation shall be restricted.
- All changes to the system shall be carried out in line with the Change Management Procedure.
- Libraries containing application source code, production executable, and systems audit tools shall be secured from unauthorized access.
- The development staff shall not have access to operational systems. For occasional and essential support purposes, the development staff may be granted special access for a limited period.
- An audit log shall be maintained of all updates to operational systems and system applications.

8.2 POLICY STATEMENTS – APPLICATION SECURITY

Applications deployed in SUNRISE GILTS & SECURITIES PRIVATE LIMITEDIT Department shall have controls for secure input, processing, storage, and output of data. Applications must

be tested for security and performance before deployment and shall be managed for high availability.

8.2.1 APPLICATION ACCESS

- Application shall have authentication and authorization controls.
    - Application shall authenticate all users before allowing access
    - Application shall have the provision for allocating access rights based on the principle of least privilege
    - Role based access controls shall be defined. The access level shall be documented by the Senior Business Analyst in coordination with Head of Business Applications
    - The application shall restrict menu options based on a need to know and need to do basis
    - Access shall be granted only after adequate authorization by the application owner
- All applications enabling business transactions shall facilitate maker and checker role.
- No individual irrespective of his/her grade, title or function shall be allowed to complete a transaction involving sensitive, valuable, or critical information from initiation to the final authorization.
- Applications shall not allow end-users to invoke operating system level commands through the application interface.
- Application shall use secure channel for transmission of sensitive user credentials and financial information.
- SSL shall be configured to ensure that all sensitive information is encrypted and sent from client to server.
- For web-based applications, application shall redirect the login credentials to another page for authentication purposes.

8.2.2 DATA SECURITY

- Sensitive data including application user login credentials shall be stored in secure manner.
- User login passwords shall be stored in an encrypted format. The user passwords shall be stored in such a way that it is not retrievable even by system administrators / application developer.
- Application shall have facility to check the integrity of the data.

- Application owner shall define the retention period for all data handled by the application.
    - This shall be done after considering relevant statutory and regulatory requirements
    - Retention period is required for determining the backup media rotation cycle and for deciding on erasing old data for creating free disk space

8.2.3 INPUT CONTROLS

- All user inputs shall be checked by the application to ensure it is both appropriate and expected:
    - Application shall have additional controls to identify duplicate transaction records
    - The application shall have adequate controls to ensure that, data has been accurately input e.g. range checks, validity checks, missing or incomplete data

8.2.4 PROCESSING CONTROLS

- The application shall ensure processes cannot be initiated out of sequence.
- Application shall ensure that all tasks associated with a process are completed and cannot be manipulated or bypassed.
- The application shall have built-in checks to ensure that if there are any pre-requisites for executing a process, these are met before initiating the same.

8.2.5 PERFORMANCE TESTING

- Head of Applications shall ensure that application is tested for peak load conditions before deployment.
- For all multi-user applications, the load testing needs to be done in environments which simulate real life conditions.

8.2.6 SECURITY TESTING

- Head of Application along with Head of Information Security shall ensure that application code review and security testing is carried out at least annually.
- Web user access restricted to the front-end web servers only. Also, it shall be reviewed for:
    - Protection against common vulnerabilities (such as Parameter Manipulation, SQL Injection, Command Injection, Cross Site Scripting, Directory Traversal, Buffer

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

Overflow, Cookie Snooping, Authentication Hijacking, Log Tampering, Attack Obfuscation, Error message Interception, Denial of Service, etc.)

- Web applications shall be secured against the key vulnerabilities that have been identified in latest OWASP (Open Web Application Security Project) standards.
- Internet facing application shall be subjected to external penetration testing / vulnerability assessment by a qualified Cert-In empanelled auditor
- The application system shall have Multi-tier Architecture

- SUNRISE GILTS & SECURITIES PRIVATE LIMITED Equities shall ensure that off the shelf products being used for core business functionality (such as Back office applications) should bear Indian Common criteria certification of Evaluation Assurance Level 4.
  - The Common criteria certification in India is being provided by (STQC) Standardisation Testing and Quality Certification (Ministry of Electronics and Information Technology).

8.2.7 RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES

- Vendor/OEM supplied software packages shall be used without modification as far as possible.
- Vendor shall not have any access to production environment.
- If it is necessary to make changes in the software package, the required changes shall be made with the consent of the vendor.

8.2.8 PROTECTION OF TEST DATA

- Test data shall be selected carefully, protected and controlled.
- The use of operational data containing personally identifiable information or any other confidential information for testing purposes shall be avoided.
- The following guidelines shall be applied to protect operational data, when used for testing purposes:
  - The access control procedures, which apply to operational application systems, should also apply to test application systems
  - There should be separate authorization each time operational information is copied to a test environment
  - Operational information should be erased from a test environment immediately after the testing is complete

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- The copying and use of operational information should be logged to provide an audit trail
- All the test data should be cleaned from the database and applicable folders, and configuration files.

8.2.9 AUDIT LOGS & MONITORING

- The application shall have the facility to log all transactions and security related events. including the following:
  - User account management
  - User privilege changes
  - User login/logout time
  - Changes in application configuration
  - Authentication failures
- Auditing mechanism deployed shall have tamper proof, continuous logging systems. The logs shall be available in "Read Only" mode only to authorized user.

8.2.10 ERROR HANDLING

- The error messages generated by the application shall not disclose any information related to installed packages, OS, Databases and / or security setup.
- The error shall not reveal information to the end user of what the correct input might be.
- Custom error messages shall be used by modifying the default error messages.

8.2.11 FIREWALL

- All critical multi-user applications shall be placed behind a firewall to adequately segregate access from internal and external users.
- IT Managers shall review any request for Firewall rule base change pertaining to the applications (IP addresses, ports and users) and Head of Information Security shall approve the request.
- Access to the system audit tool, which is used to test the applications, shall be restricted.

8.2.12 VENDOR DECLARATIONS

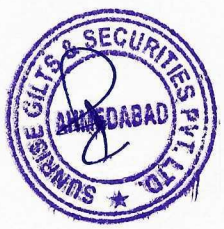
- The vendor shall agree on (by declarations/acceptance or contract)

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

- Not to violate any Intellectual Property Rights, licensing rights, etc. while producing the system and subsequently providing it to SUNRISE GILTS & SECURITIES PRIVATE LIMITED IT Department.
- Must agree to provide fix for all the concerns raised and elimination of existing vulnerabilities before launching on the internet.
- Not to deploy techniques to covertly gather information about individuals at the time of access authentication.
- Installation according to best practices such as remove unnecessary services, files or programs, disable anonymous user account, according to business needs of SUNRISE GILTS & SECURITIES PRIVATE LIMITED Technologies.
- Protection against source code vulnerabilities for the system such as hard coded passwords, time/events triggers, loops, trap doors, etc.

8.2.13 DOCUMENTATION

- Application owner shall ensure that detailed documentation is available for the following activities:
  - Application installation
  - Configuration Settings
  - Privilege levels and associated roles
  - User procedures
  - Backup and recovery procedure
  - Data retention period
- All settings mentioned in the secure configuration document shall be incorporated in the application documentation.
- Adequate backups of all documentation shall be maintained.
- Every new system/application shall have the step by step user manual for better understanding and navigation of the system



9.0 USER AWARENESS AND TRAINING POLICY

9.1 POLICY STATEMENTS

9.1.1 GENERAL STATEMENTS

- HR department in coordination with Head of Information Technology shall ensure that information security awareness programs are conducted as a part of employee induction training apart from general orientation for every new staff joining SUNRISE GILTS & SECURITIES PRIVATE LIMITED.
- HR department shall ensure that relevant awareness, training and education programs are conducted on a continuous basis to raise and maintain the employee awareness with regards to information security.
- The information security awareness, training & education programs are:
  - Useful to counter threats through a basic knowledge of IT security principles
  - Useful to make staff capable of performing their IT security-related tasks effectively and efficiently
- The information security awareness, training & education programs shall aim at achieving the following:
  - Improve awareness across staff on the need for information security
  - Develop skills to perform jobs in a secured manner
  - Build in-depth knowledge to maintain and improve IT security of SUNRISE GILTS & SECURITIES PRIVATE LIMITED
  - Enable SUNRISE GILTS & SECURITIES PRIVATE LIMITEDstaff and third-party users to adhere to Acceptable Usage Policy
  - Educate SUNRISE GILTS & SECURITIES PRIVATE LIMITEDstaff and third-party users about the disciplinary action if user actions found not complying with the SUNRISE GILTS & SECURITIES PRIVATE LIMITEDIT Security Policies.
- This training shall include subject areas like organizational security requirements, organizational security policies and procedures, security threats and concerns, legal responsibilities and business controls, as well as correct use of information processing facilities.

- Head of Information Technology shall periodically review the security awareness program to verify that it provides awareness to all personnel about the importance of data security.
- HR department in coordination with Head of Information shall ensure:
  - Relevant awareness materials are developed in compliance with the information security policies, procedures and standards of SUNRISE GILTS & SECURITIES PRIVATE LIMITED.
  - Evaluate existing levels of employee knowledge with regards to information security issues and identify areas of improvement based on business needs.
  - Obtain employee training feedback so that the awareness, training, and education program can be further enhanced.

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

10.0 TELEWORKING POLICY

10.1 POLICY STATEMENT

All access to the network from mobile computing devices shall be authorized and provided in a secure manner only. Policy also ensures that minimum necessary access rights are provided based on business requirements.

10.1.1 GENERAL STATEMENTS

When using mobile devices, special care shall be taken to ensure that business information is not compromised.

Following parameters shall be considered:

- Registration of mobile devices
- Requirements for physical protection
- Restriction of software/app installation
- Requirements for mobile device software versions and for applying patches
- Restriction of connection to information services
- Access controls
- Cryptographic techniques
- Malware protection
- Remote disabling, erasure or lockout
- Backups
- Acceptable usage of web services and web apps
- Theft of asset

10.1.2 REMOTE ACCESS

- On approval from Management and Security team, authorized staff and non-employees shall be allowed to remotely access SUNRISE GILTS & SECURITIES PRIVATE LIMITEDnetwork with minimum necessary access rights while delivering their official duties.
- All remote connections initiated to/from remote / branch networks made to the SUNRISE GILTS & SECURITIES PRIVATE LIMITED'network shall be done through the approved

SUNRISE GILTS & SECURITIES PVT. LTD. AHMEDABAD

secure methods such as IPSec, virtual private network and should not be initiated from open or non-trusted public Wi-Fi networks.

- Strong authentication mechanism, such as two factor authentications, shall be used while remotely accessing information.
- Sharing of login credentials for Remote Access shall be strictly prohibited among SUNRISE GILTS & SECURITIES PRIVATE LIMITED staff and non-employees.
- All user activities through remote access shall be monitored for any malicious activities.
- All hosts connecting to SUNRISE GILTS & SECURITIES PRIVATE LIMITED network remotely shall have the anti-virus with latest AV updates, host-based firewall, latest OS and application patches installed.