Information Security Policy

Date: 01/01/2024

Document Status: Approved

Version: 1.0

Document Owner: IT Manager

Table of Contents

1. Introduction

Suraj Estate Developers Ltd intends to follow process-based approach to document, implement, improve and maintain information security across all group companies. SURAJ ESATE DEVELOPERS LTD looks at information security as a strategic issue and has therefore set up a Compliance Officer (CISO) role to be primarily responsible for implementing and monitoring the SURAJ ESATE DEVELOPERS LTD's information security policies & processes. This entails creation of a framework which will govern the entire information security aspect.

Information Security is the protection of Information and Information Assets, from a wide range of threats in order to safeguard business and profits. It is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Information Security Management System (ISMS) is an overall management system, based on a business risk approach, to establish implement, operate, monitor, review, maintain and improve information security. ISMS is a systematic approach to manage sensitive company information so that it remains secure. It encompasses People, Process and Technology.

It provides the following benefits to SURAJ ESATE DEVELOPERS LTD:

- Protects the SURAJ ESATE DEVELOPERS LTD's information assets
- Manages and minimizes risk exposure
- Enhances customer satisfaction that improves customer retention
- Builds a culture of security
- Keeps confidential information secure
- Allows secure exchange of information
- Ensures meeting legal obligations
- Provides consistency in the delivery of service or product

1.1. Scope of ISMS

Information Security Policy is applicable to:

- All employees, contractors, third-parties, outsourced partners and personnel associated with SURAJ ESATE DEVELOPERS LTD whether in India or out of India.
- All information Assets which include, but are not limited to: software assets, physical assets, paper assets, service assets, people assets and assets that are physically or electronically stored, processed and/or transmitted by any of the aforesaid types of assets.

1.2. Context of the organization

SURAJ ESATE DEVELOPERS LTD are a group of companies within SURAJ ESATE DEVELOPERS LTD has significant interests in real estate. The combined market cap of SURAJ ESATE DEVELOPERS LTD's publicly listed entity.

SURAJ ESATE DEVELOPERS LTD intends to manage its internal and external issues that may affect the information security objectives of the Company. These issues include but are not limited to the following:

- Compromise in confidentiality, integrity and availability of information
- Non-compliance to legal, regulatory and contractual obligations
- Risks involved in online business
- Third party risks with respect to information security (i.e. Outsourced vendors, contractors, IT and cloud services, suppliers, etc.)

SURAJ ESATE DEVELOPERS LTD identifies all the relevant interested parties i.e. Senior Management, employees, vendors, contractors, service providers, suppliers, customers, legal and regulatory authorities, etc. through risk

assessment exercise and also ensures that needs and expectations of these parties are also taken into consideration.

2. Policy

SURAJ ESATE DEVELOPERS LTD has documented an Information Security Policy (ISMS Policy, this document) that outlines all the information security objectives to be met by SURAJ ESATE DEVELOPERS LTD. The information security policy of SURAJ ESATE DEVELOPERS LTD addresses several domains including security at people, technology and process levels. Also, there are supporting process and procedure documents available for various aspects of information security.

The Information Security policy of SURAJ ESATE DEVELOPERS LTD shall be reviewed and updated at least annually or at major changes and communicated to all the users in the organization. In addition to the internal stakeholders, relevant sections of the ISMS Policy may be shared with external parties, on approval from CISO. The policy ensures that SURAJ ESATE DEVELOPERS LTD's information is protected and provides assurance to SURAJ ESATE DEVELOPERS LTD's customers and business partners.

The policy statement is as follows:

Information assets are important business assets to SURAJ ESATE DEVELOPERS LTD and needs to be appropriately protected in order to preserve trust and confidence of customers, Business partners and regulatory authorities in SURAJ ESATE DEVELOPERS LTD, ensure business continuity and maximize return on investments and business opportunities.

At SURAJ ESATE DEVELOPERS LTD, the management views information security as a critical business driver. Management understands the business risks associated with ineffective information security management. The management at SURAJ ESATE DEVELOPERS LTD is committed to the governance, implementation, systematic operation, maintenance and improvement of the Information Security Management System (ISMS). The management expressly supports the following activities associated with effective information security management:

- *Information Risk identification and their treatment to acceptable levels or risks*
- *Establishing information security policy and procedures.*
- *Compliance with statutory and regulatory requirements*
- *Establishing roles and responsibilities for critical activities associated with information security management.*
- *Providing sufficient resources to develop, implement, operate, and maintain the ISMS.*
- *Periodic review of Information Risk & ISMS and its management*
- *Conduct necessary programs for creating and increasing awareness about ISMS.*
- *Achieve global standards in Information Security Management.*

3. Objectives

The objectives of the SURAJ ESATE DEVELOPERS LTD Information Security policy are:

- To strengthen internal control and prevent threats to the SURAJ ESATE DEVELOPERS LTD's information, thereby ensuring the appropriate protection of information assets of SURAJ ESATE DEVELOPERS LTD through regular monitoring.

To ensure the confidentiality, integrity and availability of information assets of SURAJ ESATE DEVELOPERS LTD through maintenance of asset registers and risk assessment.

- To continually strengthen and improve the overall capabilities of the Information Security Management System of the SURAJ ESATE DEVELOPERS LTD. This shall be assessed based security metrics designed for the organization and risk treatment methodology.

SURAJ ESATE DEVELOPERS LTD tracks the performance of its Information Security objectives and effectiveness of Information Security management system through defined Key Performance Indicators (KPIs). Also it reviews, monitors and reports the same to senior management on periodic basis and takes appropriate corrective action.

4. Consequence Management and Non-Compliance

- All violations of security policies, standards and/or guidelines are subject to disciplinary action. The specific disciplinary action depends upon the nature of the violation, the impact of the violation on informational assets and related facilities, etc. Violations will be handled as per the existing HR processes and could range from verbal reprimand, to termination of employment/contract and/or legal action.
- If a department or function is unable to comply with any requirements detailed within this policy, an exception shall be obtained. Such exceptions shall be documented and approved Compliance officer indicating the rationale for the exception and the related risks.

5. Leadership and Commitment

5.1 Security Organizational Structure

SURAJ ESATE DEVELOPERS LTD's top management demonstrates leadership and commitment with respect to Information Security Management. by delegating responsibilities to the Information Security Council. The organizational structure for Information Security comprises of four groups namely

- Management Committee

- IT Team: - Development and ongoing maintenance of cyber security policies and procedures; Identify, access and monitor cyber security incidents; conduct cyber security related awareness campaigns across SURAJ ESATE DEVELOPERS LTD; Identification and mitigation of Cyber Security vulnerabilities. Responsible for implementation of SURAJ ESATE DEVELOPERS LTD's policies and procedures across the entire SURAJ ESATE DEVELOPERS LTD IT infrastructure.
- Audit Team: - Conduct internal audits and vendor/third-party assessments to ensure the control objectives, controls, processes and procedures of SURAJ ESATE DEVELOPERS LTD Information Security Management System are in conform to the standard, effectively implemented, working as expected, and properly maintained.

6. Risk Management

- Risk assessment exercise shall be conducted at least annually to identify and evaluate various information security risks faced by SURAJ ESATE DEVELOPERS LTD and to prioritize the required controls based on the business impact and the likelihood of risk occurring.
- IT team will be responsible for identifying risks, developing a plan, tracking and treating the risks for assets.
- Status of Identified risks and corresponding treatment plan shall be reviewed by the management committee on annually.

7. Training and Awareness

- Online training and awareness programs shall be conducted annually for all employees based on current Cyber Security Threat Landscape. Relevant records shall be maintained for reporting purpose.
- Mandatory online trainings shall be assigned to newly joined employees with respect to organizations polices, standards and guidelines. Trainings with respect to cyber security awareness shall also be mandated.
- Organization shall identify and assign role-based security trainings for roles that require specific knowledge and expertise as part of their day-to-day operations.

- Completion and attendance shall be mandated where required and possible consequences shall be defined for non-adherence by HR Teams.
- An overall assessment of the employee's understanding where required shall be conducted at the end of an awareness, education, and training course to test knowledge transfer.

8. Documentation

- SURAJ ESATE DEVELOPERS LTD shall document all the information required by the standards, and requirements of its Information Security Policies which are necessary for the effectiveness of the information security management system.
- All supporting policies and procedures shall be reviewed annually and revision history shall be maintained.
- All the documented information of SURAJ ESATE DEVELOPERS LTD in paper or electronic form shall be created and updated appropriately with identifications and descriptions such as title, date, author, version no., change details and review frequency.
- All the documented information shall be available when needed. The distribution, access, retrieval, use and storage of information documents shall be properly maintained and monitored.

9. Security Policy

- Any SURAJ ESATE DEVELOPERS LTD Staff, intern who intends to access SURAJ ESATE DEVELOPERS LTD's infrastructure shall be allowed only Mobile/Tablet Devices. Any service provider and third-party contractor, who intends to access IT's infrastructure shall be allowed only mobile/tablet device.
- Users shall erase all information and software related to any previous employment, before using their device under this policy for the first time.
- In case, the device user is transferred, or retired / contract expired, or device is lost, the user shall notify IT team for de-registration of device and wiping off entire SURAJ ESATE DEVELOPERS LTD data stored on the mobile device (smart phones, tablets, etc.)
- IT Team shall at a minimum ensure that adequate security measures are implemented to ensure compliance to SURAJ ESATE DEVELOPERS LTD ISMS Policy.
- Access to the SURAJ ESATE DEVELOPERS LTD's network and business applications shall be restricted to only approved devices that meet a predetermined minimum-security configuration.
- Users are advised to keep their personal data separate from business data on their personally owned device in separate directories to reduce the possibility of disclosure.
- Organization shall have the right to seize and forensically examine any personally owned device believed to contain, or to have contained, SURAJ ESATE DEVELOPERS LTD's data where necessary for investigatory or control purposes.
- SURAJ ESATE DEVELOPERS LTD IT team shall have the right to enforce technical security controls such as access control, malware protection software and encryption.
- Users of employee-owned devices shall be subject to a comprehensive and targeted security awareness campaign so that they clearly understand and can comply with the acceptable use

policy.

- Users (SURAJ ESATE DEVELOPERS LTD Staff, interns, service providers and third-party contractors etc.) at a minimum shall ensure that they:
    1. Operate the device in compliance with Information Security Policy.
    2. Users shall obtain written approval from their respective Supervisor/ Head of the department to access confidential or classified information using external devices.
    3. Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.
    4. Immediately contact SURAJ ESATE DEVELOPERS LTD IT Team and their immediate Supervisor/ Head of the department if the mobile device is lost, stolen, damaged, destroyed, compromised, or non-functional.
- Control wireless network and service connectivity: Wi-Fi connectivity shall be turned off when not in use, and users shall only connect their devices to trusted networks. Devices shall be set to prompt users before connecting to networks so that users aren't unknowingly connecting to unsafe networks.
- Never store confidential data on a device: Users shall avoid saving any sensitive data like password, personal, financial data on their devices. This precaution ensures that confidential data is safe even if a device gets compromised.
- Employees shall not install freely available mobile applications from unauthorized sites which may collect data on the device.
- Employee shall never access or use SURAJ ESATE DEVELOPERS LTD systems or company data through a device in a way that breaches any of other SURAJ ESATE DEVELOPERS LTD policies.
- On last working day of an employee, all company data (including work emails), and any software applications provided for business purpose, shall be removed from the device. If this cannot be achieved remotely, the device must be submitted to IT Department for wiping and software removal.

10. Acceptable Use Policy

Refer 'Information Systems Acceptable Use Policy'

11. Human Resource Security

11.1. During Recruitment

- HR Team shall be responsible for performing background verification checks prior to recruitment of employees or engagement of staff on contract basis.
- Information security responsibilities for all staff and third-party personnel shall be specified in terms and conditions of employment.
- All staff and third-party personnel shall sign the Code of Conduct at the time of joining.
- The contractual agreements with employees and contractors shall state their and SURAJ ESATE DEVELOPERS LTD's responsibilities for information security. Terms and conditions of employment shall:

1. state that information security responsibilities extend outside normal working hours and premises and continue after employment has ended.
2. explain the employee's legal responsibilities and rights
3. include a non-disclosure / confidentiality clause

11.2. During Employment

- All staff and third-party personnel shall agree to perform their security responsibilities and comply with the requirements specified in the security policies.
- All staff and third-party personnel shall be responsible for protection of any sensitive information and assets assigned to them.
- All staff and third-party personnel shall use information processing systems and data residing on systems for authorized business purposes only.
- All staff and third-party personnel shall report any suspected information security incident or weaknesses to his/her reporting manager and Cyber Security team.
- The Cyber Security team shall ensure relevant cyber security awareness education and training (upon hire as part of induction and subsequently periodic) for all staff of SURAJ ESATE DEVELOPERS LTD and where relevant, third-party personnel.
- The Cyber Security team shall monitor, review and measure the effectiveness of cyber security awareness through internal compliance and awareness tests.
- The Business IT Head shall report all information security breaches committed by any employee to the HR head for taking necessary disciplinary actions against them.

11.3. Termination and Change of employment

- Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.
- All physical and logical access privileges shall be revoked immediately when an authorized user no longer requires access to information or systems as part of their job, or when they leave SURAJ ESATE DEVELOPERS LTD. In case access needs to be retained, the same shall be approved by the HR team
- In the case of a contractor provided through an external party, the termination process is undertaken by the external party in accordance with the contract between the organization and the external party.
- Upon termination of employment/contract/agreement, internal staff and third-party personnel shall:
    1. Return Assets that belong to SURAJ ESATE DEVELOPERS LTD
    2. Confirm that they have destroyed all copies of information owned by SURAJ ESATE DEVELOPERS LTD.
- The activities performed by a staff / third party may be subject to additional monitoring at the time of termination or change of employment, on communication from respective Business representative (BU Head or BU SPOC). The department representative shall assume ownership and responsibility for monitoring related activities in co-ordination with IT.

12. Asset Management Policy

There shall be documented standards and procedures for managing the asset lifecycle.

12.1. Ownership of Information Assets

- All Information assets (hardware and software) shall be identified and have an asset owner.
- An asset custodian shall oversee and implement necessary safeguards to protect the assets per the classification level defined by the asset owner.
- Asset reconciliation and verification shall be performed on bi-annual basis.

12.2. Asset Register

- IT Team shall develop and maintain an asset register containing all assets within their business function.
- The asset register shall contain at a minimum, the asset type, asset location, owner, custodians and name of the function/processes that use those assets.
- The asset register shall also maintain the CIA rating for all assets and accordingly label them as per the Asset Classification Scheme. (Refer Asset Management procedure for asset classification categories).
- Asset rating shall be reviewed on periodically as part of annual Risk Assessment exercise.

12.3. Information Classification and Handling

- The Information Classification scheme shall be used to define an appropriate level of protection or special handling required for an information asset.
- The level of protection shall be commensurate with the classification level of the data.
- The classification of the information shall be consistent with the business value of the data.
- Information shall be classified using SURAJ ESATE DEVELOPERS LTD's Information Classification Scheme as tabulated below:

Information Classification Guidelines

Classification Category	Category Description
CONFIDENTIAL	This classification applies to the most critical business information assets, which are intended strictly for use within SURAJ ESATE DEVELOPERS LTD for limited authorized users. Its unauthorized disclosure could adversely impact its business, its shareholders, its business partners and/ or its customers, leading to legal and financial repercussions and adverse public opinion.
RESTRICTED	This classification applies to any sensitive business information assets, which are intended for use within SURAJ ESATE DEVELOPERS LTD for some of the authorized users. Its unauthorized disclosure could adversely impact its business, its shareholders, its business partners, its employees and/or its customers
INTERNAL	This classification applies to information assets that are specifically meant for all employees of SURAJ ESATE DEVELOPERS LTD. While its unauthorized disclosure is against the policy, it is not expected to seriously or adversely impact the business, employees, customers, stockholders and/ or business partners.

PUBLIC	This classification applies to information assets, which has been explicitly approved by the management for release to the public.

Electronic Information Handling Guidelines

Usage	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
Creation/ Obtainment of Information	Shall be labelled at the time of creation/obtainment	Shall be labelled at the time of creation/ obtainment	Shall be labelled at the time of creation/ obtainment	Shall be labelled at the time of creation/ obtainment
Storage on static media	Shall be protected by password	Shall be protected by password	No Special requirements	No Special requirements
Storage on removable media	Shall be protected by password	Shall be protected by password	No Special requirements	No Special requirements
Printing and duplication	Printing permitted with explicit business need and approval from Business owner and IT teams.	Printing permitted with explicit business need and approval from department head.	Printing permitted	No Special requirements
Read/Update/ Delete access to information	Shall be restricted to Information owners, relevant authority of groups	Shall be restricted to Information owners, relevant authority of groups	Access to delete/update information shall be restricted to authorized individuals, relevant authority or groups. Read access shall be provided to all users within the company	Access to delete/update information shall be restricted to authorized individuals. No special requirements for read access
Transmission to internal email ID	Encryption or password protection is required as mandated by the Information Owner	Encryption or password protection is required as mandated by the Information Owner	No special requirements	No special requirements
Transmission to external email ID	Shall not be emailed unless authorized by Information owner.	Shall not be emailed unless authorized by Information owner	Shall not be emailed unless authorized by Information owner	No special requirements

Usage	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
	Encryption or password protection is mandatory. While sending such data outside, reporting manager should be kept in Cc	Encryption or password protection is recommended		
Disposal of Information	Shall be degaussed and destroyed if media is not to be reused in future	Shall be deleted from the media	Shall be deleted from the media	No special requirements

Paper Information Handling Guidelines

Usage	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
Creation/ Obtainment of Information	Shall be labelled mandatorily at the time of creation/obtainment	Shall be labelled mandatorily at the time of creation/obtainment	No Special requirements	No Special requirements
Storage and Access	Shall be stored in appropriate location with restricted access Shall not be available to personnel without prior authorization from information owner	Shall be stored in appropriate location with restricted access Shall not be available to personnel without prior authorization from information owner	No Special requirements	Shall be available widely for public No Special requirements for storage
Duplication	Shall not be copied/scanned without permission from information owner Unattended coping/scanning should not be done	Unattended coping/scanning should not be done	Unattended coping/scanning should not be done	No Special requirements
Mailing	Mailing allowed as per permission of relevant authority or	Mailing allowed as per permission of relevant authority or	Mailing allowed as per permission of relevant	No special requirements

Usage	CONFIDENTIAL	RESTRICTED	INTERNAL	PUBLIC
	information owner only Classification marking shall be visible on the envelope.	information owner only Classification marking shall be visible on the envelope.	authority or information owner only Inter-office mailing of documents is permitted	
Disposal of Information	Shall be shredded	Shall be shredded	Shall be shredded	No special requirements

12.4. Asset Retention and Disposal

- Information owners shall define types of records and their retention requirements.
- Records which are no longer active shall be archived for a period of time as set forth in the SURAJ ESATE DEVELOPERS LTD Data Retention Schedule.
- Information shall be disposed when no longer needed subject to its retention schedule and approval by asset owner.
- Hardware assets and electronic records shall be disposed in a secure manner in accordance with the Asset Disposal guidelines.
- All assets destroyed in compliance with this policy shall require ‘e-waste certificate’ to be retained as per defined policy.
- Prior to disposal of system devices like Hard Drives, RAMs, etc., the same shall be sanitized by use of techniques like degaussing, low-level formatting, or physical destruction to ensure that data cannot be reconstructed.

12.5. Media Handling

- All media containing sensitive data shall be stored in a secure safe, which shall be fire resistant and free of toxic chemicals.
- Access to media library and media safe shall be restricted to authorized persons only.
- Prior to disposal of removable media, all data shall be securely deleted, or the media shall be destroyed.
- All incoming/outgoing media transfers shall be authorized and shall be checked against a gate pass.
- Removable media shall be scanned for malware/anti-virus prior to providing read/write access.

13. Access Control Policy

13.1. User Access Management

- A formal user registration and de-registration process shall be implemented to create user IDs and assign access privileges.
- A unique ID shall be assigned to each user of information system to hold them responsible for their actions. User Ids shall follow a standard naming convention for all computer systems to facilitate user identification. Naming conventions shall cover all end users, contractors, consultants and vendors.
- A single user shall not be assigned more than one user ID on the same information system.
- The administrator of Information systems shall not grant a user, access to any system without the authorization of the user's supervisor or manager.
- The supervisors 0r managers shall revoke access rights of users in a timely manner who have either changed their job function or have been terminated.
- Generic user IDs where necessarily required as an exception shall be assigned to a nominated user post approval from the respective Business Head or Business SPOC. The nominated user along with the Business head shall maintain the accountability, by whom, when and for what the generic ID is used.
- All vendor supplied default user IDs shall be disabled or removed where possible.
- SURAJ ESATE DEVELOPERS LTD systems to be scanned to identify orphan IDs, dormant IDs, unauthorized IDs, etc. on a periodically as part of quarterly ID validation process. Same need to be deleted if not required. Exception to be raised for IDs which need to be retained with proper business justification.
- Access to information and information technology resources shall be controlled, monitored, and authorized based upon user's job function, need-to-know and need-to-perform criteria.
- The access to specific functionalities in information systems and level of access required at the granular level of read, modify & update, deletion shall be identified and documented. These requirements shall be translated into system profiles for the different classes of business users.
- Access privileges shall be assigned to a unique user ID that is mapped to an employee/Contractor based on individual's subscribed role, business need and security requirements.
- Role based access shall be provided based on the systems profiles defined by the system and business owners.
- The use of Group and shared IDs shall be restricted and if it is absolutely required to use shared IDs, mechanisms shall be established to ensure traceability/audit trails of usage to individual users.
- Request for change in the access right shall be documented and approved by the user's Manager or the respective Business SPOC.
- Audit trails for all requests for additions, modifications or deletions of individual accounts and access rights shall be maintained.
- Access rights shall be defined based on the least privilege principle and be approved by user's Manager or the respective BU SPOC.
- The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.

- User access shall be reviewed and access shall be disabled if the account is found to be inactive for a period of Ninety (90) days or more. If the same cannot be disabled, exception shall be taken from the CISO or the Information Security Council and same shall be maintained.
- IT Operations shall enable user account lockout after five (5) unsuccessful attempts to logon to the system.
- Users shall be required to re-authenticate themselves after a specific period of inactivity.
- System lock duration shall be set to a maximum period of 5 minutes in case of system inactivity.
- Access review for critical applications shall be done on quarterly basis.

13.2. Network Access Control

- Appropriate interfaces shall be created to segregate SURAJ ESATE DEVELOPERS LTD network from the networks owned by other organization and public networks.
- Users shall only be provided with access to the services that they have been specifically authorized.
- Only authorized users shall be permitted to establish remote connections to the network using secure channels.
- An equipment identifier shall be used to authenticate all equipment connecting to the network.
- Users connecting to the network shall be authenticated and their access attempts shall be logged.
- The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.

- User sessions shall be disabled after 15 minutes of inactivity so as to limit the connection time to sensitive network.
- Vendor shall provide details of their employees who shall need access to SURAJ ESATE DEVELOPERS LTD network. Access shall be granted to only those vendor employees whose details have been provided to SURAJ ESATE DEVELOPERS LTD.

13.3. Application Access Control

- Logical access to the application software shall be restricted to authorized users.
- Access to application functionalities shall be restricted based on business requirements.
- User access (except administrators) to data repositories shall be approved and recorded.
- Application accounts created for inter-application access shall not be used by individual users.
- Application Owners shall be responsible for management of access rights to their respect applications.
- Application access for critical applications shall be reviewed on a quarterly basis.

13.4. Remote Access

- Remote access shall not be provided to employees/vendors/contractors by default. Remote access to network shall require an appropriate management approval and a valid business need.
- Remote access request for third party vendor/consultant shall be raised by the SURAJ ESATE DEVELOPERS LTD employee responsible for the vendor /consultant engagement along with proper business justification. The request needs to be approved by BU SPOC and Cyber Security Manager.
- Remote user sessions shall be terminated after a maximum period of 15 minutes of inactivity.
- Unauthorized inbound and outbound connections to and from SURAJ ESATE DEVELOPERS LTD network shall be prohibited.
- Remote access to the network shall utilize approved VPN (Virtual Private Network) infrastructure and multi-factor authentication.
- All remote access to an internal network, whether through VPN, or other mechanism, shall be logged.

13.5. Access to third Party Users

- The designated manager within SURAJ ESATE DEVELOPERS LTD shall authorize and supervise access requirements for non-employees.
- Basic information Security principles such as least privilege, Separation of duties and defense in depth shall be applied.

14. Data Backup, Retention and Disposal Policy

- Information owners shall determine the backup and recovery requirements based on the criticality of information systems to prevent operational disruptions or data loss.
- Backup media shall be stored in a secure location in a off-site facility such as an alternate or backup site.
- Data recovery processes shall be tested for effectiveness on annual basis.
- Data backup shall be encrypted.
- IT operations team shall identify and establish appropriate processes to meet the backup and recovery requirements determined by information owners.
- Data retention period shall be defined and records shall be retained for the defined period. This shall be reviewed at least once in a year and updated with changes if any. Retention periods for data shall be decided based on the following,
    1. SURAJ ESATE DEVELOPERS LTD's business requirements,
    2. Legal or regulatory compliances,
    3. Contractual obligations.
- Records shall be maintained in a safe and secure environment. Records shall be protected from unauthorized access.
- All waste copies of sensitive information that are generated while copying, printing, or faxing shall be shredded using paper shredders/incinerators or shall be placed in locked bins clearly marked as containing confidential data.
- Storage media like floppy disk, hard drives, CDs, tape or optical media, zip disks, etc. shall be erased using a degaussing device or "disk-wiping" software before being discarded.

- If the data cannot be erased, then Media shall be physically destroyed prior to disposal in such a manner that data should be beyond retrieval.
- Non-disclosure agreement shall be signed between the Organization and external contractor for outsourcing disposal. Certificates of secure disposal shall be obtained from external contractor.

15. Data Security Policy

- SURAJ ESATE DEVELOPERS LTD shall implement mechanisms to prevent the accidental disclosure of email and attachments to unauthorized individuals by enforcing encryption between email servers (e.g. using Transport Layer Security (TLS) or equivalent).
- Email servers shall protect messages by using digital signatures to identify if email messages have been modified in transit.
- Users shall be educated in how to protect the confidentiality and integrity of email messages (e.g. by the use of encryption, digital certificates and digital signatures).
- Data Security solution (e.g. DLP, IRM, etc.) should be used to identify specific types of sensitive information, monitor channels of data leakage (vectors) and take actions to prevent this data from leaking.
- Data Security solution should be configured to monitor and control the flow of sensitive data using technical Data Security solution policies, defining:
    1. what data can and cannot be sent, posted, uploaded, moved or copied and pasted.
    2. where data can be transmitted.
    3. who can send and receive data (e.g. via email).
    4. how data can be shared.
- Data Security solution should be configured to include a register of keywords, electronic document characteristics and the specific types of sensitive information (sometimes referred to as pre-registration) that need to be protected from unauthorized disclosure.
- Data Security solution should be configured to detect sensitive data by using
    1. described content matching, which checks data against regular expressions, defined strings, keywords, patterns or dictionaries (a list of specific terms, keywords or key phrases);
    2. fingerprinting (indexing), which takes a cryptographic hash of a sample file or file contents to create a 'fingerprint', checking content against this fingerprint for complete or partial matches (i.e. to detect either the complete text or excerpts that match the sample document)
    3. machine learning, which uses algorithms and statistical techniques to determine if content is similar to test data, used to train the machine learning algorithm, used by the Data Security solution
    4. optional character recognition (image recognition), which analyses image files (e.g. screenshots or scanned documents) and extracts text to find matches for sensitive content.

- Data Security solution should be configured to monitor data leakage channels where sensitive data is in motion (e.g. data traversing a network such as the internet or private network), in use (e.g. data processed on endpoint devices) or at rest (e.g. data stored in file systems, databases, the cloud or endpoint devices)
- Backups should be encrypted to protect sensitive information, when:
    1. transmitted via a network to external storage facilities, particularly when engaging with a third party to support backup capabilities
    2. stored on physical media, to prevent unauthorized access in the event backups are lost or stolen in transit to an alternative location, such as an off-site storage facility
- Data processed by cloud services should be protected, which includes encrypting sensitive data by using the CSP default encryption solution, configuring customer-managed key encryption or implementing customer-supplied key encryption.
- USB shall be blocked for all end-users. In case of any deviation, policy change shall be pre-approved by the respective Business heads.
- Sensitive information shall not be kept for longer than it is required to reduce the risk of undesirable disclosure.
- Information shall be deleted from systems, applications, and services in accordance with business requirements and taking into consideration relevant laws and regulations.
- When using service suppliers for information deletion, evidence of information deletion shall be obtained from them.

16. Anti-Virus Policy

- All servers, desktops and laptops shall have anti-virus agent installed. Infrastructure Team shall ensure that all new systems including desktops, laptops, and servers have anti-virus agent installed, pre-loaded and configured before provisioning.
- Anti-virus agent installation shall be password protected to ensure that end users cannot uninstall the agent. The anti-virus agent shall be configured in such a way that end users will not have privileges to change any settings or to disable the agent.
- Anti-virus agent shall be configured to scan the machine at least once every week. The scanning can be scheduled during non-peak usage hours.
- 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.
- Access to websites and other resources on the internet known to host malicious content shall be prevented using the web content filtering tool. Antivirus software shall be installed on the Internet Proxy and if feasible configured to scan downloads/uploads for malicious code.
- SURAJ ESATE DEVELOPERS LTD shall employ anti-malware signature auto update features. After applying an update, automated systems shall verify that each system has received its signature update. The SURAJ ESATE DEVELOPERS LTD shall monitor anti-virus console logs to correct any systems that failed to be updated.
- Infrastructure team shall submit monthly reports on the status of the Anti-Virus protection to the Cyber Security Team.
- For external users (including consultants, vendors, customers, and service providers) who bring laptops/desktops into the Organization's premises, SURAJ ESATE DEVELOPERS LTD shall ensure the devices are scanned for viruses or compensating controls are in place to prevent the spread of viruses before allowing these devices access to SURAJ ESATE DEVELOPERS LTD network.
- Provisions shall be made for real-time triggering and monitoring of alerts related to virus/malware detection and necessary actions shall be taken to remediate the same.

17. Email Security Policy

- SURAJ ESATE DEVELOPERS LTD shall implement technologies to protect e-mail by analyzing and filtering e-mail messages, and block suspicious messages such as spam and phishing emails.
- Access to e-mail messages shall be restricted to SURAJ ESATE DEVELOPERS LTD employees, consultants & contractors only.
- SURAJ ESATE DEVELOPERS LTD shall ensure that email systems are only accessed by individual users via their user IDs.
- All emails sent from organization addresses to recipients outside of the organization shall carry the following disclaimer in English: "DISCLAIMER: The information in this message is

confidential and may be legally privileged. It is intended solely for the addressee. Access to this message by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, or distribution of the message, or any action or omission taken by you in reliance on it, is prohibited and may be unlawful. please immediately contact the sender if you have received this message in error.

- SURAJ ESATE DEVELOPERS LTD shall prohibit the System Administrator to access the e-mail contents of any employee without prior permission.
- SURAJ ESATE DEVELOPERS LTD shall ensure that SURAJ ESATE DEVELOPERS LTD's email is only used for business purposes.
- Multi-Factor Authentication shall be required to access the email service remotely or through a Webmail page.
- SURAJ ESATE DEVELOPERS LTD emails that contain classified information shall be encrypted.
- SURAJ ESATE DEVELOPERS LTD shall archive the emails and perform backups periodically and according to business requirements.
- Limits shall be defined for email attachments to ensure appropriate capacity management for each user's mailbox.
- A warning notice shall be displayed for emails being sent to recipients outside the organization.
- Incoming and outgoing email attachment shall be filtered at the email gateway. SURAJ ESATE DEVELOPERS LTD email gateway shall be protected against Advanced Persistent Threats and Zero Day attacks shall be implemented.
- Anti-virus software shall be configured to scan attachments in all emails. If a virus is found in an incoming SMTP mail, then the appropriate actions shall be taken to delete or quarantine the attachment.
- Third party vendors shall not be allowed to send emails to external domains.
- The organization shall prohibit:
    1. Automatic email diversion to external email addresses.
    2. Unauthorized private encryption of email or attachments.
    3. The opening of attachments from unknown or untrusted sources.
- SURAJ ESATE DEVELOPERS LTD shall disable the Open Mail Relay service. Cloud Security Policy

- SURAJ ESATE DEVELOPERS LTD shall perform an assessment of the cloud service provider (CSP) prior to onboarding.
- The Procurement and Legal teams shall include the necessary legal, non-disclosure, business continuity and disaster recovery clauses in the CSP contract.
- The Data Owner/Custodian shall classify the data being hosted/stored at the CSP as per the 'SURAJ ESATE DEVELOPERS LTD Information Classification Scheme'.
- The organization shall ensure that the CSP's data privacy policy complies with the applicable laws.
- The IT team should implement the necessary cryptography controls for the data as per the data classification and on the network channel.
- Contracts with CSP shall include clauses for complete deletion of data/ information at the end of the Agreement.

- Contract shall also include clauses for the return of data to the organization and that there is no vendor-lock in period defined by the CSP.
- Wherever applicable, SURAJ ESATE DEVELOPERS LTD shall align its Cloud Security controls with industry good practices such as CIS benchmark.
- Roles and responsibilities for protecting the cloud environment should be agreed with the CSP, including shared responsibilities and the need for collaboration.

- SURAJ ESATE DEVELOPERS LTD shall ensure monitoring of security-related events and logs for cloud systems.
- The IT team shall implement the appropriate access permissions for the cloud environment as per the 'SURAJ ESATE DEVELOPERS LTD Access Management Policy'.
- Access to cloud-based services shall be provided using multi-factor authentication mechanism.
- Secure methods of connecting to cloud services shall be provided, which may include applying HTTPS (TLS) to all network traffic, configuring a virtual private network (VPN) for sensitive traffic and/or implementing a wide area network (WAN) solution for critical and/or highly sensitive information, segmenting networks by implementing virtual local area networks (VLANs), etc.
- The IT team should perform periodic backups of data hosted/stored on cloud environment as per 'SURAJ ESATE DEVELOPERS LTD Data backup & restoration policy'.
- SURAJ ESATE DEVELOPERS LTD shall conduct an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services and that the acquisition or outsourcing of dedicated information security services is approved by Cyber Security Team within the organization.
- The organization performs scans to identify vulnerabilities in the cloud environment as well as applications hosted in the cloud as per SURAJ ESATE DEVELOPERS LTD's Vulnerability Management Policy.
- Information security awareness, education and training programs about cloud services shall be provided to employees and the supervising managers, including those of business units.
- The organization shall perform penetration testing at a defined frequency on cloud information systems and application hosted.
- Information security events shall be reported through appropriate management channels as quickly as possible. The mechanisms for incident reporting shall be agreed with the CSP as part of the agreement.
- Organizations shall regularly monitor, review and audit supplier/ CSP service delivery & SLA to ensure CSP complies to SURAJ ESATE DEVELOPERS LTD's Information Security Policies.

18. Business Continuity & Disaster Recovery

- Business Functional Heads shall identify critical business applications & processes under their purview that are required for continued operations of SURAJ ESATE DEVELOPERS LTD, in the event of a disaster. The criticality of applications & processes shall be evaluated based on the impact to business and implications on services.

- Business process and technology redundancies shall be identified and deployed to avoid or reduce impact of disaster events. DR site shall be set up for critical business applications and processes to ensure continuity of business.
- Business Functional Heads shall identify and document the Recovery Time Objective [RTO] and Recovery Point Objective [RPO] for critical business applications and processes.
- Business Functional Heads along with IT department Heads shall evaluate and define DR plan.
- Business Functional Heads along with IT Team shall conduct DR drills/tests on biannual basis to verify the appropriateness of the DR plan.
- Application owner shall be responsible for reviewing and updating the DR plan based on the test results.
- DR plan documents shall be accessible and available to respective stake owners and teams in case the same needs to be referred in an event of an incident/disaster.
- Business Heads shall maintain all records with respect to DR drills for a minimum period of 2 years.
- Training & Awareness program shall be established for all SURAJ ESATE DEVELOPERS LTD functions and facilities. Relevant records shall be kept for a minimum period of 2 years for reporting purpose and to identify areas of improvement.
- Business Heads shall document & maintain all records in case of incidents/disasters where DR needs to be invoked. Same shall be retained for a minimum period of 2 years.
- Business Functional Heads shall work together with the IT Team to improve Recovery Time taken on the DR Setup for critical business applications. External storage media, mobile devices or any other external devices shall not be connected to OT technology components and OT networks.