Sbi Financials
Information Security Policy

Last revision date-2/10/2025

Purpose

Information and systems are used by the company to Deliver value to our customers and business partners. As Such the information has value and must be protected in accordance with its sensitivity.

This policy outlines the expectations and behaviours of the organization to protect those systems, applications and information confidentiality, Integrity and availability.

This policies approach is to comprehensively provide the full scope of policy for delivering sound information security to the organization.

Scope

This policy applies to all staff at Sbi Financials and its subsidiaries, to include any third part staff contracted or providing services on behalf of Sbi Financials. This policy applies to all systems, applications and data within the Sbi Financials business and Information technology (IT) systems to include Software as a Service (Saas) (Cloud Systems).

Policy

The following statements provide the information security policy

For the organization. Any exclusions to the policy statements below must be explicitly documented.

Information Security

The organization shall ensure information security is part of overall risk management strategy.

Role and Responsibilities

To ensure the effective implementation of information security policies, responsibilities are shared by all the members of the organization. The following roles are established to maintain compliance and manage organization security posture.

1 Executive management is responsible for:

Executive management (i.e. CEO, CTO, CFO) responsible for overall decision in organization.

- Evaluating and accepting risk on behalf of the entity.
- Defining information security responsibilities and goals and integrating them into organization 's strategic processes.
- Ensuring the consistent implementation and compliance of information security policies and standards.
- Supporting security program through clear direction and commitment of appropriate resources (e.g., funding, staffing, tools).

2 Chief Information Security Officer (CISO) is responsible for:

Chief Information Security Officer is responsible for supervision of organization security posture.

- Develop, implement and oversee the information security policies and rules in an organization.
- Lead information security risk management strategy.
- Escalating security concerns to executive management that are not being adequately addressed.
- Promote General Information Security Awareness among the workforce of the organization.

- Manage the security incident process.

3 IT management is responsible for:

IT management (i.e. System admins, SRE) are responsible for overall management of IT infrastructure in an organization.

- Identify, Implement and manage the technical security controls like firewalls in IT infrastructure.
- Ensure that security controls are consistent with the information security policies.
- Implementing business continuity and disaster recovery plans.
- Providing training to appropriate technical staff on secure operations.
- Conducts regular reviews of user access logs and security configurations.

4 The workforce is responsible for:

Every individual covered by the policy has a personal responsibility to uphold security.

- Complying to all the statements and expectations outlined in the information security policy.
- Protecting company's information and resources from unauthorized use or disclosure.
- Report any suspected information security incidents or weakness to the security team.
- Understanding the information security controls necessary to protect confidentiality, integrity and availability of information entrusted.

Separation of duties

- Duties and permissions should be divided among multiple individuals to ensure that checks and balances are in place.
- No single individual should have control over all phases of a critical transaction, process, or task.

- If separation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision.

Information Classification and Handling

- All information, which is created, acquired or used in support of business activities, must be only be used for its intended purpose.

- All information must be classified into one of the following categories:
    - Public -Information intended for public release. Its disclosure will not harm the SBI Financials.eg-published reports, public website contents.

    - Internal -information intended for business use only. Its unauthorized disclosure causes Minor organisational disruption.eg -Internal policies, process documents and Internal mail.

    - Confidential –sensitive information or customer information whose unauthorized disclosure may result in major operation disruption, financial loss and legal impact. Eg-Customer data, financial statements and employee records.

    - Restricted -highly or critical sensitive information whose unauthorized disclosure Could cause severe financial, operational or legal damage. Eg-Encryption keys, Authentication credentials, incident investigation data and merger documents.

- Each classification has an approved set of baseline controls designed to protect this classification and these controls must be followed.

- All information must have an information owner which is responsible for managing and classification of information.

- Confidential data and restricted data must be encrypted at rest and in transit using AES-256.

- Internal data should be stored securely with multi factor authentication.

- A written or electronic inventory of all information assets must be maintained.

Access Control

The following policies are associated with the control of access to systems and data

User Access

- Any access granted to Sbi Financials systems, applications, and, and data shall require appropriate approval.
- All user shall be granted based on the principle of least privilege, providing only minimum level of access necessary for an individual to perform their job duties
- All access to systems, applications, and data shall be documented and reviewed for validity on Management approved frequency
- Account access to systems, applications, and data shall be removed when no longer appropriate on demand, or as discovered during review.
- User account types shall be appropriate for the user access required, (i.e. general user, privileged user, non-staff (3rd party), guest and emergency users).
- Adding, modifying, reviewing, deleting user accounts (which user accounts: end user, privilege user, 3rd party, guest, emergency)
- Shared user accounts shall be explicitly approved for use by management on case-by-case basis.

Authentication

- All access to organizational systems, applications, and data that is accessible via the Internet shall require multi-factor authentication.
- All mobile devices (i.e. tablets, mobile phones) shall have an authentication mechanism to unlock and access the device.
- All credentials must meet a minimum complexity requirement (i.e. minimum length, character types).
- Credentials shall be changed immediately if a compromise is suspected.
- Default vendor password must be changed before system is put in production.

Remote Access

- Remote access shall be allowed using management approved remote access solutions.
- Third party remote access shall be reviewed and approved.
- Third party remote access shall be requiring a member of Sbi Financials to explicitly authorize or approve the access on demand.
- No unattended access shall be granted to any company resources (systems, data, applications).

IT Asset Management

- All IT hardware and software (i.e. laptop, server, CRM software) asset must be assigned to a designated department or individual.
- All departments are required to maintain an inventory of hardware and software assets, including all system components (e.g., machine name, network address, software version, designated department or induvial name).
- Regular scanning must be implemented to identify any unauthorized hardware or software and must be immediately notified to system admin.

Vulnerability management

- All systems must be scanned for vulnerabilities before being deployed in production and Periodically thereafter.
- All systems are subjected to yearly penetration testing.
- Penetration tests are required Quarterly for all critical environments/systems.
- Penetration testing of Outsourced systems and third-party systems must be coordinated. Penetration testing and mitigation must be included in third party agreements.

- Any vulnerability assessment/Penetration testing must be conducted by authorized penetration testers. The CISO must be notified before conducting vulnerability assessment.

- The output of the scans/penetration tests must be reviewed system owner within 5 business days of receiving the report. Copies of the penetration tests must be shared with Cybersecurity analyst for evaluation of risks.

- Penetration testers must perform penetration testing/vulnerability scanning must have a formal process defined, tested and must be followed all times

- Discovered vulnerabilities must be remediated based on their severity rating:
    - Critical: remediated within 5 business days.
    - High: remediated within 15 business days.
    - Medium: remediated within 30 business days.

- Any discovered vulnerability, a plan of action and milestones must be created and updated accordingly to document the planned remedial actions to mitigate vulnerabilities.

Systems Security

Systems are not limited to servers, networks, databases, communications and software applications.

- IT management department must be responsible for maintenance and administration of any system deployed in organization.

- All system must be developed, maintained and decommissioned in accordance with a secure system development lifecycle (SSDLC).

- Each system must have set of controls based on classification of information stored or processed in the system.

- Environments and test plans should be established to validate the system works as intended prior to deploying in production.

- Separation of environments (e.g., development, test, production and QA) must be there either logically or physically including separate environmental identifications.

- A formal change procedure must be defined for all systems. Any change that effects different environments must be included.

- Privilege access to production system must be restricted.

- Migration processes must be documented and implemented for transfer of software from development to production environment.

- All the network traffic must be filtered through firewalls.

- Network architecture must include segmentation between non-production and production environments.

- All systems must be hardened and configured in accordance to organizations secure configuration standards before being deployed into production.

- All systems must be configured to generate security audit logs and must be regularly monitored for any suspicious activities.

- All software development must follow secure coding practises to prevent common vulnerabilities.

- All software applications must be thoroughly tested and must pass through proper approval process before being deployed to production environments.

Cyber Incident Management

- Organization shall maintain a documented and regularly updated Incident response plan aligned with industry best practises and standards. This plan ensures timely and effective response, mitigation, and recovery from cybersecurity incidents.

- Any observed or suspected information security incidents or weakness must be reported to SOC (Security operation centre) Team and CISO as quick as possible.

- Any Employee feels that if a security concern is not adequately addressed, they may contact to CISO directly.

- The SOC (Security Operation Centre) must be notified of any cyber incident which may have a significant or severe impact on operations or security. SOC must to follow proper incident response procedures for containment, investigation and remediation.

- Organisation shall maintain detailed records of all cybersecurity incidents, including their nature, impact, response actions, and lessons learned to support continuous improvement and regulatory requirements.

- Incident response plan must address all phases of the incident lifecycles: Preparation, Identification, Containment, Eradication, Recovery and Lessons Learned.

- A formal Cybersecurity Incident Response Team must be established, with clearly defined roles and responsibilities of members in dealing with incidents.

- The incident response plan must be tested annually through exercises. Members of response team must receive training on their incident response duties.

Personnel Security

- A new recruit must receive general security awareness training, to include recognizing and reporting insider threats within 30 days of hire. All security training must be reinforced at least annually.

- Workforce must abide by Acceptable use of information technology Resources Policy, and an audit process must be there to ensure that workforce abide by the policy as per the requirements.

- All job positions must be evaluated to determine whether the require access to sensitive information or assets.

- For the jobs requiring access to sensitive information or assets. The organisation must conduct workforce suitability checks. Depending on risk levels, suitability checks consist of background verification like criminal history records or other reports maintained by government or private sources that maintain public and non-public records.

- A process must be defined to review suitability checks yearly and upon change in job positions or duties.

- Organization must ensure that all the issued assets must be returned prior to an employee separation and all accounts and access should be revoked immediately upon separation from the organization.

Physical and Environmental Security

- Server rooms, data centres and restricted zones must have a defined security parameter And access must be controlled through electronic access controls (i.e. keycards, turnstiles).

- All visitor visiting Server rooms, data centres and restricted zone must be checked, Logged and must be escorted by authorized personnel at all the times within these zones.

- Server rooms and data centres must be equipped with adequate fire protection (e.g., fire detection and suppression system).

- All environmental and security systems including HVAC, fire suppression, access controls And CCTV must be regularly inspected, tested, and maintained to ensure functionality.

- Server rooms and data centres must be quipped with proper HVAC (Heating, Ventilation and Air conditioning) systems to maintain an ambient environment that adheres to equipment manufacturer specifications.

- Access to server rooms and restricted areas must be reviewed quarterly, and access for terminated or transferred employee must be revoked immediately.

- Server rooms, data centres and restricted zones must be under continuous(24x7) CCTV surveillance, and footage should be retained and periodically reviewed as per organizational or regulatory requirements.

Related Procedures

- Access control approval
- Remote Access
- Authentication
- Roles and Responsibilities
- Information classification and handling
- Separation of duties
- Cyber Incident Management
- Personnel Security
- System Security
- Physical and Environment Security
- Vulnerability Management
- IT Asset Management

Non-Compliance

- Any individuals that this policy applies to are required to follow the policy. Non-compliance with the policy will result in appropriate management-guided sanctions.
- Sanctions may include disciplinary actions, up to and including termination of employment and legal action where applicable.

Management Commitment / Authority

This policy is supported and approved by CISO. This is the published

Information security policy effective publish date.

Clark, CEO

John smith, CISO

Review Schedule

This policy shall be reviewed at least annually, or upon significant changes to the business or threat landscape, to ensure its continued relevance and effectiveness.

Definitions

- Systems, applications, data are the software, hardware third-party and cloud assets that organization uses to perform business.
- Mobile device-Devices that are "travel" and are typically on an individual's persons and travel outside the office environment. This includes mobile phones, tablets.
- Software as a service (SaaS) are software which are deployed on Internet.
- Information means any kind of data relevant for the business.
- SSDLC (Secure System Development Lifecycle) is the process of integrating security activities into every phase of the software development lifecycle.
- SOC (Security Operation Centre) is team and facility responsible for monitoring, analysing and responding to cybersecurity threats and incidents ongoing basis.
- CIRT (Cybersecurity Incident Response Teams) a designated group of individuals responsible for responding and managing security incidents.
- Least privilege is the principle of providing users with least access.
- MFA(Multi-Factor Authentication) A security method that requires user to provide two or more verification factors to gain access to a resources.