Sbi Financials Information Technology Policy

Entity: Sbi Financials	**IT Policy No: 4855**
Policy Name: Information Security Policy	**Updated:** 2/10/2025
Issued By: Clark, CEO	**Owner:** John Smith, CISO

1.0 Purpose and Benefits

1. 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.
2. This policy outlines the expectations and behaviors of the organization to protect those systems, applications, and information confidentiality, integrity, and availability.
3. This policy's approach is to comprehensively provide the full scope of policy for delivering sound information security to the organization.

2.0 Authority

1. This policy is supported and approved by the CISO, John Smith, and Executive Management represented by CEO Clark.

3.0 Scope

1. This policy applies to all staff at Sbi Financials and its subsidiaries, to include any third-party staff contracted or providing services on behalf of Sbi Financials.
2. 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).

4.0 Definitions of Key Terms

Term	**Definition**
Systems, applications, data	The software, hardware, third-party, and cloud assets that the organization uses to perform business.

Mobile Device	Devices that "travel" and are typically on an individual's person and travel outside the office environment. This includes mobile phones and tablets.
SaaS	Software as a Service; software which is deployed on the Internet.
Information	Any kind of data relevant for the business.
SSDLC	Secure System Development Lifecycle; the process of integrating security activities into every phase of the software development lifecycle.
SOC	Security Operation Centre; team and facility responsible for monitoring, analyzing, and responding to cybersecurity threats and incidents on an ongoing basis.
CIRT	Cybersecurity Incident Response Teams; a designated group of individuals responsible for responding to and managing security incidents.
Least Privilege	The principle of providing users with the least access necessary.
MFA	Multi-Factor Authentication; a security method that requires the user to provide two or more verification factors to gain access to a resource.

5.0 Information Statement

Organizational Security

1. The organization shall ensure information security is part of the overall risk management strategy.
2. The following statements provide the information security policy for the organization.
3. Any exclusions to the policy statements below must be explicitly documented.

Functional Responsibilities (RACI Matrix)

To ensure the effective implementation of information security policies, responsibilities are shared by all members of the organization. The following RACI matrix establishes the roles responsible for maintaining compliance and managing the organization's security posture.

Key: R = Responsible, **A** = Accountable, **C** = Consulted, **I** = Informed

Activity / Responsibility	Executive Mgmt	CISO	IT Mgmt	Workforce
Risk Management Strategy	A	R	C	I
Defining Security Goals & Responsibilities	A	R	C	I
Policy Implementation & Compliance	A	R	R	R
Resource Allocation (Funding, Staffing)	A	C	I	I
Developing Security Policies & Standards	I	A/R	C	I
Incident Management Process	I	A/R	C	I (Report)
Security Awareness Training	I	A/R	I	R (Attend)
Technical	I	C	A/R	I

Controls Implementation (Firewalls, etc.)				
BC/DR Planning & Implementation	I	C	A/R	I
System Configuration & Log Review	I	C	A/R	I
Reporting Incidents	I	I	I	R
Protecting Company Resources	I	I	I	R

Separation of Duties

1. Duties and permissions should be divided among multiple individuals to ensure that checks and balances are in place.
2. No single individual should have control over all phases of a critical transaction, process, or task.
3. 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

1. All information created, acquired, or used in support of business activities must be used only for its intended purpose.
2. All information must be classified into one of the following categories:

Classification	Description
Public	Information intended for public release. Its disclosure will not harm Sbi Financials (e.g., published reports, public website contents).

Internal	Information intended for business use only. Its unauthorized disclosure causes minor organizational disruption (e.g., internal policies, process documents, and internal mail). Internal data should be stored securely with multi-factor authentication.
Confidential	Sensitive information or customer information whose unauthorized disclosure may result in major operational disruption, financial loss, and legal impact (e.g., Customer data, financial statements, and employee records).
Restricted	Highly or critically sensitive information whose unauthorized disclosure could cause severe financial, operational, or legal damage (e.g., Encryption keys, Authentication credentials, incident investigation data, and merger documents).

3. Each classification has an approved set of baseline controls designed to protect this classification, and these controls must be followed.
4. All information must have an information owner who is responsible for managing and classification of information.
5. Confidential data and restricted data must be encrypted at rest and in transit using AES-256.
6. A written or electronic inventory of all information assets must be maintained.

IT Asset Management

1. All IT hardware and software assets, such as laptops, servers, and CRM software, must be assigned to a designated department or individual.
2. All departments are required to maintain an inventory of hardware and software assets, including all system components like machine name, network address, software version, and designated department or individual name.
3. Regular scanning must be implemented to identify any unauthorized hardware or software and must be immediately notified to the system admin.

Personnel Security

1. 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.

2. The workforce must abide by the Acceptable Use of Information Technology Resources Policy, and an audit process must be in place to ensure that the workforce abides by the policy as per the requirements.
3. All job positions must be evaluated to determine whether they require access to sensitive information or assets.
4. For jobs requiring access to sensitive information or assets, the organization 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.
5. A process must be defined to review suitability checks yearly and upon change in job positions or duties.
6. The organization must ensure that all issued assets are returned prior to an employee separation and all accounts and access should be revoked immediately upon separation from the organization.

Account Management and Access Control

User Access

1. Any access granted to Sbi Financials systems, applications, and data shall require appropriate approval.
2. All user access shall be granted based on the principle of least privilege, providing only the minimum level of access necessary for an individual to perform their job duties.
3. All access to systems, applications, and data shall be documented and reviewed for validity on a Management-approved frequency.
4. Account access to systems, applications, and data shall be removed when no longer appropriate on demand, or as discovered during review.
5. User account types shall be appropriate for the user access required, including general user, privileged user, non-staff or third party, guest, and emergency users.
6. Shared user accounts shall be explicitly approved for use by management on a case-by-case basis.

Authentication

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

Remote Access

1. Remote access shall be allowed using management-approved remote access solutions.
2. Third-party remote access shall be reviewed and approved.

3. Third-party remote access shall require a member of Sbi Financials to explicitly authorize or approve the access on demand.
4. No unattended access shall be granted to any company resources including systems, data, and applications.

Systems Security

1. Systems are not limited to servers, networks, databases, communications, and software applications.
2. The IT management department must be responsible for maintenance and administration of any system deployed in the organization.
3. All systems must be developed, maintained, and decommissioned in accordance with a Secure System Development Lifecycle (SSDLC).
4. Each system must have a set of controls based on the classification of information stored or processed in the system.
5. Environments and test plans should be established to validate the system works as intended prior to deploying in production.
6. Separation of environments for development, test, production, and QA must be maintained either logically or physically, including separate environmental identifications.
7. A formal change procedure must be defined for all systems, and any change that affects different environments must be included.
8. Privilege access to production systems must be restricted.
9. Migration processes must be documented and implemented for the transfer of software from development to production environment.
10. All network traffic must be filtered through firewalls.
11. Network architecture must include segmentation between non-production and production environments.
12. All systems must be hardened and configured in accordance with the organization's secure configuration standards before being deployed into production.
13. All systems must be configured to generate security audit logs and must be regularly monitored for any suspicious activities.
14. All software development must follow secure coding practices to prevent common vulnerabilities.
15. All software applications must be thoroughly tested and must pass through the proper approval process before being deployed to production environments.

Vulnerability Management

1. All systems must be scanned for vulnerabilities before being deployed in production and periodically thereafter.
2. All systems are subjected to yearly penetration testing.
3. Penetration tests are required Quarterly for all critical environments/systems.
4. Penetration testing of Outsourced systems and third-party systems must be coordinated. Penetration testing and mitigation must be included in third-party agreements.
5. Any vulnerability assessment or Penetration testing must be conducted by authorized

penetration testers. The CISO must be notified before conducting a vulnerability assessment.

6. The output of the scans/penetration tests must be reviewed by the system owner within 5 business days of receiving the report. Copies of the penetration tests must be shared with the Cybersecurity analyst for evaluation of risks.
7. Penetration testers must perform penetration testing/vulnerability scanning and must have a formal process defined, tested, and followed at all times.
8. 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.
9. For any discovered vulnerability, a plan of action and milestones must be created and updated accordingly to document the planned remedial actions to mitigate vulnerabilities.

Cyber Incident Management

1. The organization shall maintain a documented and regularly updated Incident Response Plan aligned with industry best practices and standards.
2. Any observed or suspected information security incidents or weaknesses must be reported to the SOC (Security Operation Centre) Team and CISO as quickly as possible.
3. If any employee feels that a security concern is not adequately addressed, they may contact the CISO directly.
4. The SOC must be notified of any cyber incident which may have a significant or severe impact on operations or security. SOC must follow proper incident response procedures for containment, investigation, and remediation.
5. The organization shall maintain detailed records of all cybersecurity incidents, including their nature, impact, response actions, and lessons learned.
6. The incident response plan must address all phases of the incident lifecycles: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
7. A formal Cybersecurity Incident Response Team (CIRT) must be established, with clearly defined roles and responsibilities of members in dealing with incidents.
8. The incident response plan must be tested annually through exercises. Members of the response team must receive training on their incident response duties.

Physical and Environmental Security

1. Server rooms, data centers, and restricted zones must have a defined security perimeter and access must be controlled through electronic access controls such as keycards or turnstiles.
2. All visitors to server rooms, data centers, and restricted zones must be checked, logged, and must be escorted by authorized personnel at all times within these zones.
3. Server rooms and data centers must be equipped with adequate fire protection, specifically fire detection and suppression systems.
4. All environmental and security systems including HVAC, fire suppression, access controls,

and CCTV must be regularly inspected, tested, and maintained to ensure functionality.
5. Server rooms and data centers must be equipped with proper HVAC systems to maintain an ambient environment that adheres to equipment manufacturer specifications.
6. Access to server rooms and restricted areas must be reviewed quarterly, and access for terminated or transferred employees must be revoked immediately.
7. Server rooms, data centers, and restricted zones must be under continuous (24x7) CCTV surveillance, and footage should be retained and periodically reviewed as per organizational or regulatory requirements.

6.0 Compliance

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

7.0 Contact Information

For questions regarding this policy, please contact:

1. John Smith, CISO
2. Sbi Financials Security Team

8.0 Revision History

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.

Date	Description of Change	Reviewer
2/10/2025	Last revision date	Amritesh Shrivastava

9.0 Related Documents / Procedures

1. Access control approval
2. Remote Access
3. Authentication
4. Roles and Responsibilities
5. Information classification and handling
6. Separation of duties
7. Cyber Incident Management

8. Personnel Security
9. System Security
10. Physical and Environment Security
11. Vulnerability Management
12. IT Asset Management