Information Security Policy

Commissioned by	:	Information Risk Management Department
Approved by	:	Board of Directors
Effective date	:	29- April-2024

Introduction

The Information Security Policy provides an integrated set of protection measures that must be uniformly applied across Jana Small Finance Bank (JSFB) to ensure a secured operating environment for its business operations.

Customer Information, organisational information, supporting IT systems, processes and people that are generating, storing and retrieving information are important assets of JSFB. The availability, integrity and confidentiality of information are essential in building and maintaining our competitive edge, cash flow, profitability, legal compliance and respected company image.

This Information Security Policy addresses the information security requirements of:

i. **Confidentiality:** Protecting sensitive information from disclosure to unauthorised individuals or systems;

ii. **Integrity:** Safeguarding the accuracy, completeness, and timeliness of information;

iii. **Availability:** Ensuring that information and vital services are accessible to authorised users when required

Other principles and security requirements such as Authenticity, Non-repudiation, Identification, Authorisation, Accountability and audit ability is also addressed in this policy.

Scope

i. This policy applies to all employees, contractors, partners, Interns/Trainees working in JSFB. Third party service providers providing hosting services or wherein data is held outside JSFB premises, shall also comply with this policy.

ii. Scope of this Information security Policy is the Information stored, communicated and processed within JSFB and JSFB's data across outsourced locations.

Objectives

The objective of the Information Security Policy is to provide JSFB, an approach to managing information risks and directives for the protection of information assets to all units, and those contracted to provide services

Ownership

The Board of Directors of JSFB is the owner of this policy and ultimately responsible for information security

Responsibility

To avoid conflict of interest formulation of policy and implementation / compliance to the policy to remain segregated. Therefore the Information Risk Management Department (IRMD) will be the owner of the Information Security (IS) Policy and Implementation responsibility to rest with IT Security Department under IT department.

The Chief Information Security Officer (CISO) is responsible for articulating the IS Policy that Bank uses to protect the information assets apart from coordinating the security related Issues within the organisation as well as relevant external agencies.

The CISO shall not be a member of IT department and shall be a member of Risk department.

All the employees and external parties as defined in policy are responsible to ensure the confidentiality, integrity and availability of Bank's information assets.

Information Risk Management Department (IRMD)

IRMD to give recommendations regarding the Information Security risk and responsible for maintenance / review of the IS Policy and also for formulating/review of all sub policies derived from IS Policy.

Policy Exceptions

Detailed in Exception handling procedure.

Periodic Review

The policy shall be reviewed every year or at the time of any major change in existing IT environment affecting policy and procedures, by CISO and placed to Board for approval.

This policy will remain in force until next review / revision.

Policy Compliance Check

Compliance review of IS policy should be carried out by Internal/External auditor on a periodic basis. Inspection & Audit Division is responsible for monitoring compliance of IS Policy. The compliance report should be placed by IAD to the Audit Committee of Board.

Information Security Governance

Information security governance consists of leadership, organisational structures and processes that protect information and mitigation of growing information security threats

Critical outcomes of information security governance include:

1. Alignment of information security with business strategy to support organisational objectives
2. Management and mitigation of risks and reduction of potential impacts on information resources to an acceptable level
3. Management of performance of information security by measuring, monitoring and reporting information security governance metrics to ensure that organisational objectives are achieved
4. Optimisation of information security investments in support of organisational Objectives

It is important to consider the organisational necessity and benefits of information security governance. They include increased predictability and the reduction of uncertainty in business operations, a level of assurance that critical decisions are not based on faulty information, enabling efficient and effective risk management, protection from the increasing potential for legal liability, process improvement, reduced losses from security-related events and prevention of catastrophic consequences and improved reputation in the market and among customers.

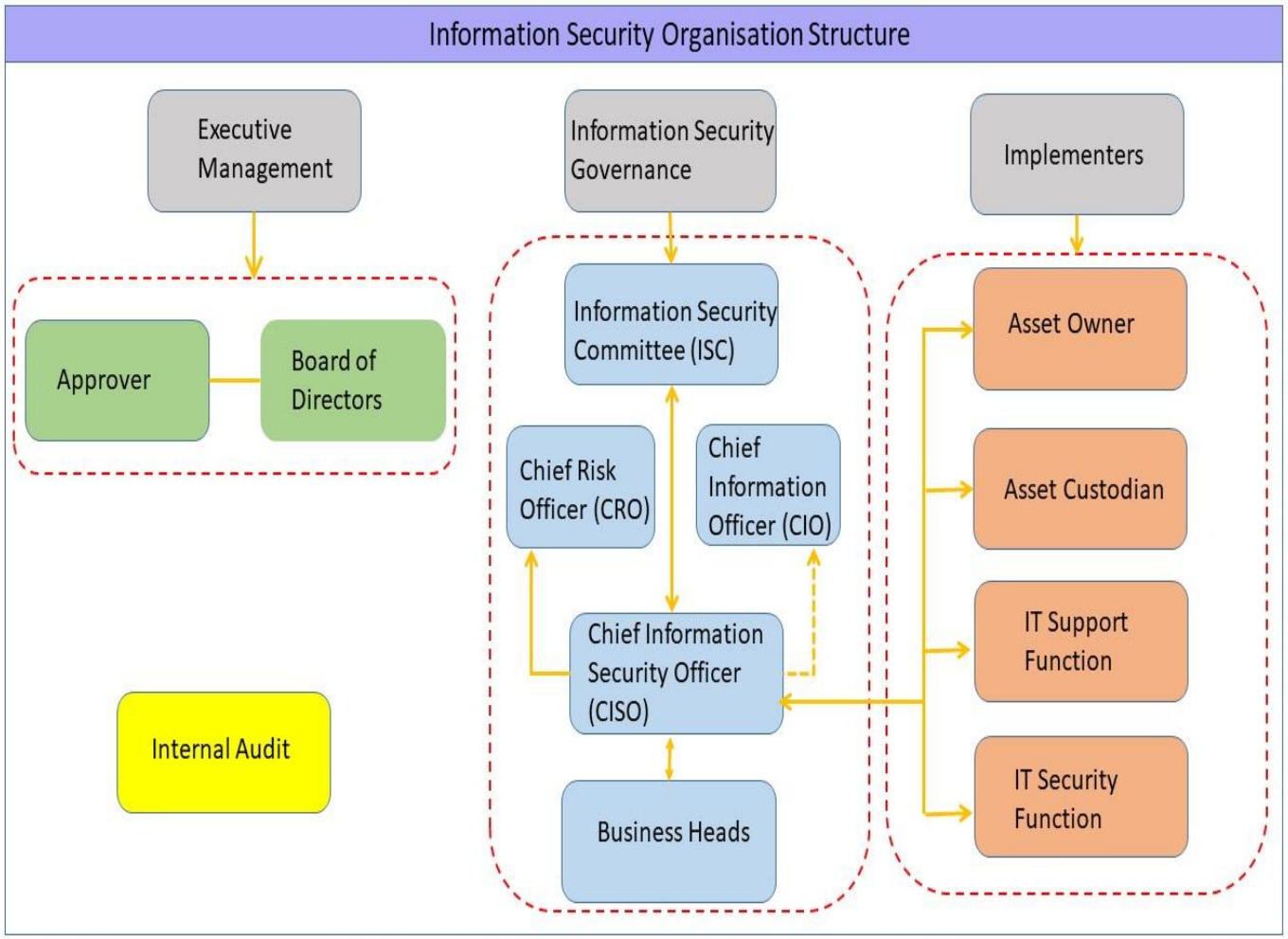
Management Responsibility

1. Approve policies related to information security function
2. Ownership for implementation of board approved information security policy
3. Ownership for establishing necessary organisational processes for information security
4. Ownership for providing necessary resources for successful information security
5. Ownership for establishing a structure for implementation of an information security program (framework)

Organisation Structure

Information security organisation shall comprise of the following

1. Board of Directors
2. Information Security Committee (ISC)
3. Business/Department Heads
4. Information Asset Owner
5. Chief Information Security Officer (CISO)
6. Chief Risk Officer (CRO)
7. Chief Information Officer (CIO)
8. Asset Custodian
9. IT Security operations
10. IT Operation
11. Internal Audit



The information Security Organisation is divided into 3 sections

i. **Executive Management**

Implementing effective security governance and defining the strategic security objectives of an organisation can be complex task. As with any other major initiative, it must have leadership and ongoing support from executive management to succeed.

ii. **Governance**

Governance is the set of responsibilities and practices exercise by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise resources are used responsibly

iii. **Implementer**

Ensuring that initiatives and existing operations adhere to policies is an area that the implementer is expected to manage.

Roles and Responsibilities

The roles and responsibilities of the Information Security Organisation members are as follows

1. Board of Directors

Approving the Information Security Policy

2. Information Security Committee (ISC)

The CRO shall be the chairperson of the ISC. The ISC shall have representation from the following Departments

- CIO
- CCO
- CISO

Members from Internal Audit, HR, Legal, Finance and other departments should be called for the ISC meeting on need basis

The ISC roles and responsibilities shall be as follows

- Developing and facilitating the implementation of information security policies, and procedures to ensure that all identified risks are managed within a bank's risk appetite.
- Approving and monitoring major information security projects and the status of information security plans and budgets, establishing priorities, approving procedures.
- Supporting the development and implementation of a bank-wide information security management program
- Reviewing the position of security incidents and various information security assessments and monitoring activities across the bank
- Reviewing the status of security awareness programs
- Assessing new developments or issues relating to information security
- Requirement for generating effective metrics for measuring performance of security control
- Reporting to the Board of Directors on information security activities
- Conducting regular ISC meetings (at least quarterly) and maintenance of MOM

3. Information Security Officer (CISO)

- Establishing, implementing, monitoring, reviewing, maintaining and improving Information Security Management System (ISMS)
- Reviewing the security policies/procedures and suggesting improvements
- Coordinating the ISC meetings
- Providing consultative inputs to the ISC on security requirements
- Coordinating information Security initiatives in the organisation
- Driving and monitoring the ISC directives in the organisation
- Updating ISC about IS initiatives, issues and incidents
- Facilitating and Conducting risk assessments of Information Assets used and recommend mitigation controls
- Promote security awareness amongst employees, customers and partners.

4. Business Heads

- Heads of Business Units are ultimately responsible for managing information risk in their respective business as part of their wider risk management responsibilities
- Nominate Asset owner
- Providing resources and support to the Asset Owners for information security implementation in the business unit

5. Information Asset Owner

Information asset owners shall be allocated to each information asset and shall ensure that security processes associated with these assets are established. For data and IT systems, they are called as application owners. The asset owner or the application owner is usually the business owner. Each application should have an application owner (asset owner) who will typically be part of the concerned business function that uses the application.

Responsibilities would include, but not be limited to:

- Assigning initial information classification and periodically reviewing the classification to ensure it still meets business needs under guidance of Information Risk Management department (IRMD);
- Ensuring security controls are in place, as recommended by IRMD;
- Reviewing and ensuring currency of the access rights associated with information assets they own;
- Determining access criteria and back-up requirements for the information assets / applications they own.

An information asset owner may delegate authority for the operation and protection of assets under their responsibility to an asset custodian. However, it will remain the responsibility of the asset owner to accept risk and to take appropriate steps to ensure that delegated authority is being responsibly applied

6. Asset Custodian

- An asset custodian shall be a member of the information technology team
- A custodian shall typically, but not necessarily be confined to, assist the owner in the identification of control mechanisms, ensuring their development/purchase, implementation, maintenance and effective operation, reporting issues that affect the information asset in the operational environment to the owner
- Together with the business owner, a custodian shall develop and maintain an information asset inventory including Confidentiality, Integrity and Availability ratings in such a way that the relationship between business process and IT component is documented and known by both parties
- A business owner shall not relinquish accountability for risk management of the owned asset by delegation of responsibility

7. IT Security Function

The IT Security is responsible for the execution of Information Risk policies, framework, guidelines and control processes

The responsibilities of IT Security includes, but not limited to:

- Enable Information Security controls
- Define IT security procedures and guidelines in line with the IS Policies
- Provide Security Architecture
- Implement and monitor operational effectiveness of mandatory IT controls
- Analysis of Security incidences, both internal and external and arriving at Lessons learned

8. Technology Infrastructure Service Providers

- Infrastructure services shall be provided by strategic outsourced partners with Service Level agreements. The service providers are custodians of IT assets on behalf of JSFB and are responsible for the implementation and operation of the infrastructure as appropriate to meet the Confidentiality, Integrity and Availability ratings specified by JSFB.
- Develop Standard Operating Procedures (SOP's), Security Guidelines for the assets managed.
- Manage IT assets as per JSFB approved policies and procedures.

9. Application Developers

Application systems (including both business applications and generic supporting software, e.g. middle-ware, databases) may be developed and maintained by an internal IT function or by a third party. These parties are responsible for ensuring that systems are developed and maintained, incorporating user requirements and information security requirements that are in adherence to JSFB Policies for Information Risk. They are also responsible, in conjunction with the provider of the underlying technology infrastructure, for ensuring that information risk is adequately managed in development and test environments and report to JSFB IT Security.

10. User Manager

The user manager is the immediate manager or supervisor of an employee. He has the ultimate responsibility for all user IDs and information assets owned by bank employees. In the case of non-employee individuals such as contractors, consultants, etc., this manager is responsible for the

activity and for the bank assets used by these individuals. He/she is usually the manager responsible for hiring the outside contractor.

11. End Users

- End Users are responsible for the following with regard to information security:
- Responsible and accountable for activities associated with an assigned account, as well as assigned equipment and removable media;
- Protect secrecy of passwords and Business Information.
- Report known or suspected security incidents

12. Audit Team

Conduct information Security audits to check compliance against Policies and procedures.

Policies, Procedures and Guidelines

At JSFB considering the security requirements, Information Security policies have been framed based on a series of security principles. All the Information Security policies and their need have been addressed below:

1. Asset Management Policy

Information assets shall be accounted for and have a nominated asset owner. Owners shall be identified and catalogued for all information assets and the responsibility for maintenance of appropriated controls shall be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains accountable for the proper protection of the assets

2. Information Risk management Procedure

Detailed risk assessments for Information risks (e.g. application risk assessment, Infra risk assessment) shall be undertaken in order to identify pertinent threats, the extent of vulnerability to those threats, the likelihood and the potential impact should a threat mature as a result of the vulnerability. This assessment shall determine acceptable, transferable and avoidable risk and the risk that shall be reduced by risk treatments (control mechanisms).

3. Data Classification Policy

To ensure that Confidentiality, integrity and availability of information is maintained, a data classification scheme has been designed. The level of security to be provided to the information will depend directly on the classification of the data

4. Acceptable IT Usage Policy

This Policy has been prepared and implemented to ensure that all the users and staff at JSFB are aware of their responsibilities towards the IT Resources of JSFB. This Policy details the end users aware of their responsibilities and the acceptable use of the IT Resources of JSFB.

5. Access Control Policy

Data must have sufficient granularity to allow the appropriate authorised access. There is a delicate balance between protecting the data and permitting access to those who need to use the data for authorised purposes. This balance should be recognised. The Access Control Policy addresses this need.

6. E-mail Security Policy

JSFB shall implement effective systems and procedures to ensure that e- mails are used as an efficient mode of business communication and implement control procedures so that the e-mail facility is not misused by the users. It also needs to be ensured that e-mail service and operations remain secure, efficient while communicating within intranet as well as through the internet. The E-mail Security Policy of JSFB addresses this.

7. Internet & Intranet Security Policy

JSFB should utilise Internet as an important resource for information and knowledge to carry on the business more efficiently. Users must also understand that any connection to the Internet offers an

opportunity for unauthorised users to view or access corporate information. Towards this direction, JSFB has developed systems & procedures to ensure that Internet is used only for business purposes in a secure manner, (without endangering the security of the JSFB's network) with a uniform code of conduct.

8. Password Security Policy

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change All Application software in JSFB will have to comply with minimum password standards as specified in this document.

9. Information Security (IS) Incident Management Policy

Incident management is required and needs to be established to ensure a quick, effective, and orderly response to security incidents. Such a policy would vary in scope depending on the sensitivity and size of the information systems being managed. A companywide incident management policy has been established for all systems.

10. Change Management Policy

Changes to information technology facilities and systems should be controlled in order to ensure that changes made to a production component are applied in a secure and consistent manner

11. Application Security Policy

It may be required to develop and maintain software, applications and add- on modules from time to time. Proper procedures, access controls and security requirements need to be addressed in the entire process. The application security policy has been framed to address these needs.

12. Operating System Security Policy

JSFB shall protect its operating system resources by providing security at a level that is appropriate for the nature of the data being processed. The operating system security policy has been framed for achieving this. JSFB shall protect all business data, related application systems and operating systems software from unauthorised or illegal access. Access to the operating system must be restricted to those people who need the access to perform their duties.

13. Network Security Policy

Appropriate controls should be established to ensure security of data in private and public networks, and the protection of connected services from unauthorised access. JSFB's Network infrastructure needs to be protected from unauthorised access. A range of security controls is required in computer networks to protect these environments. Considering the above, the network security policy has been framed for JSFB.

14. Anti-Virus Policy

Virus, Trojans, Worms, etc., are malicious programs called malware and can corrupt or destroy data or may spread confidential information to unauthorised recipients, resulting in loss of Confidentiality, Integrity, availability of the information. Malware detection and prevention measures as appropriate need to be implemented. The basis of protection against Malware should be founded on good security awareness and appropriate system access controls. The Anti-Virus policy has been framed on the above grounds.

15. Backup & Recovery Policy

In order to safeguard information and computing resources from various business and environmental threats, systems and procedures have been developed for backup of all business data, related application systems and operating systems software on a scheduled basis and in a standardised manner across JSFB. The backup and recovery procedures must be automated wherever possible using the system features and be monitored regularly. The backup & recovery policy that has been framed for JSFB considers these points.

16. Log and Audit Trail Policy

The log and audit trail policy addresses the framework for logging & auditing operating system events, application events, database events in the local area network and the network events.

17. Mobile Computing Policy

The mobile computing policy applies to all JSFB employees and staff provided with a company laptop or portable electronic device. It is the employees' responsibility for the proper care and use of the laptop computer / PED (Portable Electronic Device), data and accompanying software while using the same.

18. Version Control Policy

The version control policy of JSFB addresses implementing, managing and controlling the changes in versions of application systems, and customised add-on modules, network and operating system software, interfaces and utilities. This Policy is aimed at ensuring uniformity in versions running across JSFB and would involve maintaining up to date documentation for the entire version change process.

19. Data Archival Policy

Proper data management will facilitate and improve the retrieval, evaluation, use and storage of critical and related information. The purpose of the data archival policy for JSFB is to address the proper archival all its project related data as per the client requirement to support its high quality research service and also to ensure availability, integrity and confidentiality of the data.

20. Encryption Policy

In the current environment of increasingly open and interconnected systems and networks, network and data information security are essential. This policy describes cryptography as a tool for satisfying a wide spectrum of the Information Security Management System (ISMS) needs and requirements.

21. Wireless Security Policy

Wireless Local Area Networks (LANs) form part of the JSFB's corporate network infrastructure. In order to protect the business needs of JSFB, the wireless network must meet the same level of security employed by the rest of the infrastructure.

This policy is to ensure that the deployment of wireless networking is controlled and managed in a centralised way to provide functionality and optimum levels of service whilst maintaining network security.

22. Data Migration Policy

Sometimes, a need may arise to migrate data from one system / database to another. This typically occurs during replacement of existing application / database. This policy outlines the care to be taken during such migrations of data.

23. Security Awareness

All employees of JSFB and, where relevant, contractors and third-party users shall receive appropriate awareness training and regular updates in organisational policies and procedures, as relevant for their job function

24. Security monitoring

As per Cyber Security guidelines issued by RBI, a Security Operations Center shall be established for security monitoring of logs of critical IT Asset

25. Hardware Acquisition & Maintenance

These procedures and methods should delineate the various aspects of the procurement cycle while ensuring that hardware is of the required quality and meets the desired business objectives. Hardware, being a very important resource, should be maintained and supported systematically during its lifetime

26. HR Security Guidelines

To ensure that employees, contractors and third party users understand their responsibilities to reduce risk of theft, fraud or misuse of facilities, controls shall be implemented

27. Data Security

Physical, Technical and Organisational Security Measures

Appropriate physical, technical and organisational security procedures that restrict access to and disclosure of personal data within bank are implemented. Bank uses encryption, firewalls and other technology and security procedures to help protect the accuracy and security of sensitive personal information and prevent unauthorised access or improper use.

Bank adapts RBI best practice guidelines for Physical, Technical and Organisational measures to ensure the security of personal data including the prevention of their alteration, loss, damage, unauthorised processing or access.

28. Remote Access Policy

The purpose of this policy is to define standards for connecting to Bank network from any host. These standards are designed to minimise the potential exposure to bank from damages which may result from unauthorised use of bank resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical bank internal systems, etc.

29. Exception Handling Procedure

Information security policies and procedures constitute controls for protecting the Information assets. While every attempt should be made to comply with the policies and procedures there could be exceptions. The exception handling procedure should be followed for taking exceptions to the Information Security Policy.

30. Physical & Environmental security

To prevent unauthorised physical access, damage and interference to the organisations premises and information, critical or sensitive information processing facilities shall be housed in secure area, protected by secure parameters, with appropriate entry controls.

31. Desktop Security Guidelines

The objective of desktop security guideline is to provide a secure computing environment where data is processed. All desktops on Local Area Network (LAN) shall be configured as per these guidelines. These guidelines are also applicable to Laptops provided by JSFB to its employees / partner employees for its official use.

32. License Management Guidelines

Bank uses operating systems, applications and database software that is under license agreement and limits the use of the software to specific machines. Copies of such software are limited to backups only. It is important to have a control on the use of software on the computers.

33. Patch Management procedure

A Patch Management process needs to be in place to address technical system and software vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

34. Asset Security Testing Procedure

With rapid use of Information Technology for processing financial data, and its use in day to business processes, evaluation of Information Security measures and implementation of an effective security monitoring controls has been identified as key requirements as per Bank Information security policies.

35. Effective Measurement

This document defines the metrics for collection and analysis of meaningful and quantifiable data to measure the effectiveness of the ISMS implementation. Metrics are to identify areas of improvements and formulate security strategies for continuously improving the security processes for the Bank

36. Database Security Procedure

In accordance with the Information Security Policy, all databases owned by JSFB must be adequately protected to ensure confidentiality, integrity, availability, and accountability of such systems. Databases normally provide a data storage mechanism as a back-end to an application that provides access to the data. In addition to electronic data storage, databases typically are associated with management systems which organise data into a collection of schemes, tables, queries, reports, views and other objects.

37. Data Sanitisation Guidelines

Data Sanitisation is the process of protecting sensitive information in non- production databases from inappropriate visibility. After sanitisation, the database remains perfectly usable - the look-and-feel is preserved - but the information content is secure. Data Sanitisation establishes relationship between technology and the expectation of privacy in the collection and sharing of personally identifiable information.

38. Key Management Procedure

Key management is the set of techniques and procedures supporting the establishment and maintenance of cryptographic key relationships between authorised parties within Bank and its business partners, regulatory entities etc.

39. Information Security Guideline for Branches

This is an IT best practice guideline document that shall be followed at Branch locations to ensure secure information processing and handling, defined in line with Regulatory guidelines and JSFB Information security policies

Ref: ISMS-Information security Guideline for branches

40. Online Banking Channels Security - ATM, Internet Banking, Mobile & IVR Banking

The implementation of appropriate authentication method and security controls should be based on assessment of the risks posed, and considering customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and inter-operability with other systems.

41. New Technology Adoption

- Introduction of new technology and deployment of application & Infrastructure shall go through Risk assessment and sign off process before implementation in production.
- Procedures and guidelines for new technologies such as cloud computing, Social Banking etc. shall be developed.
- The risks associated with adoption of new & emerging technologies shall be assessed and approved.

42. Cloud computing

Cloud computing requirements shall be assessed in detail for data security, privacy, legal requirements, sustainability of the provider, service levels, geographical location of data storage and processing, including trans-border data flows, business continuity requirements, log retention, data retention, audit trails, etc, during the risk assessment process.

43. Social Media

i. Usage of Social Media within JSFB's network is restricted, unless approved specifically.

ii. Employees are personally responsible for the content they publish on- line, whether in a blog, social computing site or any other form of user- generated media.

iii. Employees are not authorised to publish or discuss the following on Social Media
- JSFB's confidential or other proprietary information
- To cite or reference Customers, partners or suppliers without their approval
- To use JSFB's logos or trademarks unless approved to do so.

44. Compliance

i. Compliance with Regulatory requirements

- Compliance to statutory, regulatory and contractual requirements such as Information Technology (IT) Act 2008, directives and recommendations given by Reserve bank of India shall be ensured
- Compliance with terms/conditions and license requirements for the usage of copyrighted software or any other proprietary information/material shall be maintained
- Cross border movement of data shall be in accordance with legal and regulatory requirements
- Records shall be retained and managed based on legal and regulatory requirements

ii. Compliance with Information Security policy and procedures

- Information processing facilities shall be used as per information security policy and acceptable usage policy
- While JSFB respects the privacy of its employees it reserves the right to audit and/or monitor the activities of its employees and information stored, processed, transmitted or handled on any assets/devices/services used by employee
- Exception to security policy and procedure shall be approved through the exception management process
- Policy exceptions shall be reviewed at least annually and as deemed necessary based on security risks envisaged, emerging threats etc.
- Violations or any attempted violations of security policies and procedures shall result in disciplinary actions

iii. Information Systems Audit

- Audits shall be conducted to ensure compliance with the information security policies, procedures and guidelines
- The use of information systems audit tools shall be controlled and authorised to prevent any possible misuse of tools.