

Bandhan Financial Services Ltd.

Head Office, Kolkata – 700 091



IS POLICY

Prepared By: Chief Financial Officer

Reviewed By: Managing Director

Recommended By: Company Secretary

Date of Approval of the Board:

Effective Date of the Policy:

Revision History

Date	Version	Description
23-March-2020	1.0	Base document

Table of contents

Table of contents	3
1. INTRODUCTION	5
1.1 Role of Information Security.....	5
1.2 Objective of IS Policy.....	5
2. IT SECURITY POLICY	5
2.1 Physical Security.....	6
2.2 Security at the Network Gateway.....	6
2.3 Security against Viruses/Spyware	6
2.4 Security built into Application Systems.....	7
2.4.1 Users and Logins.....	7
2.4.2 Username and password.....	7
2.4.3 IT Administrator.....	7
2.4.4 Application user.....	8
2.4.5 Access levels (Application System/Form/Menu)	8
2.4.6 Unsuccessful login attempts.....	9
2.4.7 Current logins.....	9
2.4.8 Login history	9
2.4.9 Application-wise login history	9
2.4.10 Password History	9
2.4.11 User Account Log.....	9
2.4.12 Application Systems' Audit Trails:.....	10
2.4.13 Application Systems Modification.....	10
2.5 Data Security	10
2.5.1 Data Backup Policy.....	10
2.6 Role based Access Control.....	11
2.7 Maker-checker.....	11
2.8 Incident Management	11
2.9 Public Key Infrastructure (PKI)	11
2.10 Trails.....	11
2.11 Cyber Security.....	12
2.12 Vulnerability Management.....	12
2.13 Cyber Crisis Management Plan	12

2.14 Digital Signatures	13
2.15 IT Risk Assessment	13
2.16 Mobile Financial Services	13
2.17 E-mail and Internet Browsing Policy	13
2.18 Staff Training Policy	14
2.19 IT Procurement Policy (Hardware/ Software)	14
3. Information Security Audit	15
4. IT Services Outsourcing	15

1. INTRODUCTION

1.1 Role of Information Security

The role of Information Security is to design, implement and maintain an information security program that protects the COMPANY's systems, services and data against unauthorized use, disclosure, modification, damage and loss.

1.2 Objective of IS Policy

- Protecting the confidentiality of data
- Preserving the integrity of data
- Promote the availability of data for authorized use
- Proactively identify risks and propose viable mitigation steps
- Cultivate a proactive risk management culture
- Implement "best practice" threat management strategies and processes to reduce threats

2. IT SECURITY POLICY

Information is an asset to all COMPANYS and Information Security (IS) refers to the protection of these assets in order to achieve organizational goals. The purpose of IS is to control access to sensitive information, ensuring use only by legitimate users so that data cannot be read or compromised without proper authorization. IS Policy with the following basic tenets:

- a) Confidentiality - Ensuring access to sensitive data to authorized users only.
- b) Integrity - Ensuring accuracy and reliability of information by ensuring that there is no modification without authorization.
- c) Availability - Ensuring that uninterrupted data is available to users when it is needed.
- d) Authenticity - For IS it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine.

IT security is created under the following security heads: -

- Physical Security
- Security at the Network Gateway
- Security against Viruses/Spyware
- Security built into the Application Software/Database
- Data Security
- Role based Access Control, if required

- Maker-checker
- Incident Management
- Public Key Infrastructure (PKI)
- Trails

Information may be categorized as Top secret, Restricted, Internal and Public. A broad classification of information is made as under:

- Top Secret/Confidential: Applicable to the class of Information, unauthorized disclosure/use of which could cause serious damage to the COMPANY.
- Restricted: It is the class of information, unauthorized disclosure /use of which would not be in the best interest of the COMPANY &/or its customers.
- Internal: The information that is sharable within COMPANY.
- Public: This information can be share outside of the COMPANY

2.1 Physical Security

The confidentiality, integrity, and availability of information can be impaired through physical access and damage or destruction to physical components. COMPANY should have a secured environment for the physical security of IS Assets.

2.2 Security at the Network Gateway

The Fire-wall/Router should provide the following minimum security features, if situation demands: -

- Intrusion Detection
- Intrusion Prevention
- Virus/Spy-ware Protection
- Access Control
- Content Filtering
- Spam Filtering
- Network Address Translation

2.3 Security against Viruses/Spyware

- Prevention/Detection of Viruses at the Network Gateway (Firewall)
- Selection of suitable Anti-virus solutions.
- Installation of Anti-virus Software on Servers as well as Nodes.
- Periodic/regular updation of Anti-virus software on all the machines.
- Updation of Virus definition/Spyware/Prohibited Content at Firewall.
- Educating the users in virus protection measures.

2.4 Security built into Application Systems

Application systems shall have security features like:

- User Ids
- Passwords
- Access Permissions
- Login History
- User Account Log
- Audit trails
- System Modification Controls
- System Documentation

A detailed Security Policy, as per the above parameters, is as follows:
Application Systems Security Policy

2.4.1 Users and Logins

Applications will be accessed through a single-entry point.

2.4.2 Username and password

- Each user should be provided with a unique username and a password.
- No user without a valid username and password can login to the system.
- A user should not be allowed to have multiple concurrent logins.
- The user should also have the privilege to change his password as and when he/she feels necessary.

2.4.3 IT Administrator

Officer designated as IT Administrator is to be provided with valid User Names and Passwords with system administration privileges. The responsibilities / privileges of a system administrator should include:

- Creation/Dropping of users (usernames).
- Activation / Deactivation of users.
- Granting / Revoking of Application Administrator privilege.
- Unlocking locked user accounts.
- Setting / Changing system parameters.
- All application administrator privileges.

IT Strategic committee will designate suitable personas System Administrator of COMPANY.

2.4.4 Application user

- An employee with a valid username and password and having access to any application system will be an application user for that application.
- There must exist a record with status as regular and valid office code in the employee directory of the payroll system.
- Whenever the system detects a mismatch between the office code of the user in the employee directory of the payroll system and office code as per security module, the user account should automatically get deactivated.
- Application user, on successful log in, should only be allowed access to the systems for which he has been granted permissions.
- The application user should not be allowed to have multiple logins.
- As soon as a user ceases to be an employee of COMPANY, his/her user account should be de-activated immediately and he should not be able to access any of the application systems.
- Users should be able to lock their login account for any number of days.
- During the locking period the user accounts cannot be accessed. User will be allowed to login to the system after the expiry of locking period.
- However, System administrator can unlock the accounts, if required.
- Maximum three login attempts should be allowed at a time. After three unsuccessful attempts login screen should be closed.
- The system should have the provision to lock the user account for those users making continuous attempts for a specified number of times (captured as system parameter) with invalid passwords.

2.4.5 Access levels (Application System/Form/Menu)

The following should be the broad access levels, if require:

- Control
- Passing / Authorization
- Preparation

- Query/View only
- No access

2.4.6 Unsuccessful login attempts

The system should keep track of all unsuccessful login attempts. The details of date, time, terminal / machine id, user id and the reason for denial for login should be recorded.

2.4.7 Current logins

The system should keep track of all current login. The system should record the date and time of login, user id, employee code/name, terminal, session id, etc.

2.4.8 Login history

The system should keep record of all past logins. The details of user id, employee code/name, terminal, session id, date and time of login, date, time nature of logout, etc. should be recorded by the system.

2.4.9 Application-wise login history

The system should also keep track of all application-wise login detail. The details of user id, employee code/name, terminal, session id, date and time of login, date, time, nature of logout, etc. should be recorded by the system.

2.4.10 Password History

The system should preserve all old passwords.

2.4.11 User Account Log

The system should keep trail of the followings along with details of date and time of changes, reason and changing authority.

- Creation of user id.
- Dropping of user id.
- Deactivation of user id.

- Reactivation of user id.
- Locking of user id.
- Unlocking of user id.
- Granting system administrator privilege
- Revoking system administrator privilege.
- Granting application administrator privilege.
- Revoking application administrator privilege.
- Changes in user profile in terms of:
 - Reporting officer
 - Access level
 - Department
 - Changes in user access to forms/reports/menu/sub-menu.
- Changes in system parameters (The old values will also be stored).

2.4.12 Application Systems' Audit Trails:

- Each Application System should have audit trail in respect of the fields as stipulated by the user department. Each system should also provide for generation of Audit Trail Reports.
- The Audit Trail Reports for the Systems like Financial Accounting, Loan Accounting and Payroll would be generated every month and would be perused by the user in-charge (Application Administrator) of the respective systems. These reports would be stored at least for one year till the annual audit of the office is complete.
- Audit trail data of all the Systems would remain on line for a minimum period of at least 400 days i.e. till the annual audit has been completed.

2.4.13 Application Systems Modification

Any new report required to be generated from any of the application systems should be provided by IT Department. However, if some major modifications required shall be undertaken by the Application Service Provider.

2.5 Data Security

2.5.1 Data Backup Policy

- Full export dump of the database to be taken on an external hard disk and/or on CD/DVD.
- Daily back-up would be preserved for one month.
- Backup disk will be kept in a secured and separate place

2.6 Role based Access Control

Access to information should be based on well-defined user roles (system administrator, user manager, application owner etc.), COMPANY should avoid dependence on one or few persons for a particular job. There will be clear delegation of authority for right to upgrade/change user profiles and permissions and also key business parameters (e.g. interest rates) which will be documented.

2.7 Maker-checker

Maker-checker is one of the important principles of authorization in the information systems of financial entities. For each transaction, there will be at least two individuals necessary for its completion as this will reduce the risk of error and will ensure reliability of information.

2.8 Incident Management

Incident Management - The IS Policy should define what constitutes an incident. COMPANY should have developed and implement processes for preventing, detecting, analyzing and responding to information security incidents. All incidents should be immediately reported to appropriate authorities as per Incident management policy.

All security violations including suspected or attempted violations should be reported and a root cause analysis / follow up action should be undertaken where applicable as per Incident Management Policy.

2.9 Public Key Infrastructure (PKI)

COMPANY may increase the usage of PKI to ensure confidentiality of data, access control, data integrity, authentication and non-repudiation.

2.10 Trails

COMPANY should ensure that audit trails exist for IT assets satisfying its business requirements, if any, including regulatory and legal requirements, facilitating audit, serving as forensic evidence when required and assisting in dispute resolution. If an

employee, for instance, attempts to access an unauthorized section, this improper activity should be recorded in the audit trail.

2.11 Cyber Security

Cyber security plays a crucial role in non-banking finance companies as they are most prone to cyber threats. Information security controls and protects the business function of the COMPANY and it must be considered throughout the business life cycle. Our COMPANY should abide by the IT framework which has been framed by reserve bank of India for protecting their companies from cyber threats.

COMPANY should review the organizational arrangements so that the security concerns are appreciated, receive adequate attention and get escalated to appropriate levels in the hierarchy to enable quick action.

2.12 Vulnerability Management

A vulnerability is an inherent configuration flaw in an organization's information technology base, whether hardware or software, which can be exploited by a third party to gather sensitive information regarding the organization.

Vulnerability management is an ongoing process to determine the process of eliminating or mitigating vulnerabilities based upon the risk & cost associated with the vulnerabilities. Our COMPANY should have a plan and approach for managing and eliminating vulnerabilities and such a strategy is clearly communicated in the Cyber Security policy document.

2.13 Cyber Crisis Management Plan

A Cyber Crisis Management Plan (CCMP) instantly evolved & a part of the overall Board permitted strategy. CCMP mainly report the following four aspects: (i) Detection (ii) Response (iii) Recovery and (iv) Containment.

COMPANY need to take effective measures to prevent cyber-attacks and to promptly detect any cyber-intrusions so as to respond/ recover/contain the fallout. COMPANY is expected to be well prepared to face emerging cyber-threats such as 'zero-day' attacks, remote access threats, and targeted attacks.

Thus, COMPANY would take essential preventive & corrective measures in addressing several kinds of cyber threats including, but not limited to, denial of service, distributed denial of services, ransom-ware / crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, visiting frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

2.14 Digital Signatures

A Digital Signature Certificate authenticates entity's identity electronically. It also provides a high level of security for online transactions by ensuring absolute privacy of the information exchanged using a Digital Signature Certificate. CPMPANY may consider use of Digital signatures to protect the authenticity and integrity of important electronic documents and also for high value fund transfer.

2.15 IT Risk Assessment

COMPANY should undertake a comprehensive risk assessment of their IT systems at yearly basis. The assessment should make an analysis of the threats and vulnerabilities to the information technology assets of the COMPANY and its existing security controls and processes.

The outcome of the exercise should be to find out the risks present and to determine the appropriate level of controls necessary for appropriate mitigation of risks.

The risk assessment should be brought to the notice of the Board of the CPMPANY and should serve as an input for Information Security Auditors.

2.16 Mobile Financial Services

COMPANY that already using or intending to use Mobile Financial Services should develop a mechanism for safeguarding information assets that are used by mobile applications to provide services to customers. The technology used for mobile services should ensure confidentiality, integrity, authenticity and must provide for end-to end encryption.

2.17 E-mail and Internet Browsing Policy

- E-mail/Internet facility for official purposes only.
- The Administrator would have the right to examine the contents of the official e-mails.
- The Administrator would also have the right to monitor the usage of internet facility by any user.
- No Spoofing.
- No unsolicited e-mail.
- All gambling/auction/pornographic sites would be blocked and not made available to users.

- The users would not be allowed to download big files which would choke the network.

2.18 Staff Training Policy

If the Company develops new application system, the company will have :

- Training on operational aspects of the application systems by the System Administrator/ concerned IT service provider.
- Training to IT professionals through training programs for upgradation of knowledge and exposure to new technologies.
- Periodic assessment of the IT training requirements should be formulated by the Human Resource Department on the recommendations of System Administrator/Chief Financial Officer to ensure sufficient, competent and capable human resources availability.

2.19 IT Procurement Policy (Hardware / Software)

- Preparation of specifications.
- Identification of suitable vendors
- Calling of quotations and placing the same for approval
- Approvals by Competent Authority as per delegation chart.
- Placement of orders
- Installation and Acceptance Testing.

3. Information Security Audit

IS audit will be performed by independent 3rd party auditors on a periodic basis. IS audit will be done through manual process and CAATs (Computer-Assisted Audit Techniques) IS audit will cover a wide area of IT processing and infrastructure such as:

- Security System
- IT Management process
- Software application
- Change / Incident Management system
- Disaster recovery plan

The IS audit report will be submitted to IT Strategy Committee and the audit findings will be resolved as per priority basis.

4. IT SERVICES OUTSOURCING

Outsourcing of IT related business process can provide the COMPANY opportunity to realize valuable strategic and economic benefits. However, prior to commencement of any outsourcing arrangement, careful consideration of risks, threats of contractual arrangements and regulatory compliance obligations must take place. Companies usually outsource their IT related business process to a third party vendor because of higher efficiency, inadequate resources and lack of specialized knowledge. The COMPANY's decision to outsource IT Services should fit into the institution's overall strategic plan and corporate objectives.

The terms and conditions governing the contract between the COMPANY and the Outsourcing service provider should be carefully defined in written agreements and vetted by COMPANY's legal counsel on their legal effect and enforceability. The contractual agreement may have the following provisions.

Monitoring and Oversight:

COMPANY should provide continuous monitoring and assessment of the service provider so that any necessary corrective measure can be taken immediately. Outsourcing service provider should have adequate systems and procedures in place to ensure protection of data/application outsourced.

b) Access to books and records / Audit and Inspection: This would include:

- Ensure that the COMPANY has the ability to access all books, records and information relevant to the outsourced activity available with the service provider. For technology outsourcing, requisite audit trails and logs for administrative activities should be retained and accessible to the COMPANY based on approved requests.
- Provide the COMPANY with the right to conduct audits on the service provider whether by its internal or external auditors, or by external specialists appointed to act on its behalf and to obtain copies of any audit or review reports and findings made on the service provider in conjunction with the services performed for the COMPANY.
- The contractual agreement may include clauses to allow the Reserve Bank of India or persons authorized by it to access the COMPANY's documents, records of transactions, and other necessary information given to, stored or processed by the service provider within a reasonable time. This includes information maintained in paper and electronic formats.

The Board and senior management are ultimately responsible for 'outsourcing operations' and for managing risks inherent in such outsourcing relationships. The Board of Directors of COMPANY is responsible for effective due diligence, oversight and management of outsourcing and accountability for all outsourcing decisions. The Board and IT Strategy committee have the responsibility to institute an effective governance mechanism and risk management process for all IT outsourced operations.

The Role of IT Strategy committee in respect of outsourced operations shall include

- a) Instituting an appropriate governance mechanism for outsourced processes, comprising of risk-based policies and procedures, to effectively identify, measure, monitor and control risks associated with outsourcing in an end to end manner;
- b) Defining approval authorities for outsourcing depending on nature of risks and materiality of outsourcing;
- c) Developing sound and responsive outsourcing risk management policies and procedures commensurate with the nature, scope, and complexity of outsourcing arrangements;
- d) Undertaking a periodic review of outsourcing strategies and all existing material outsourcing arrangements;
- e) Evaluating the risks and materiality of all prospective outsourcing based on the framework developed by the Board;
- f) Periodically reviewing the effectiveness of policies and procedures;
- g) Communicating significant risks in outsourcing to the COMPANY's Board on a periodic basis;
- h) Ensuring an independent review and audit in accordance with approved policies and procedures;
- i) Ensuring that contingency plans have been developed and tested adequately;
- j) COMPANY should ensure that their business continuity preparedness is not adversely compromised on account of outsourcing. COMPANY is expected to adopt sound business continuity management practices as issued by RBI and seek proactive assurance that the outsourced service provider maintains readiness and preparedness for business continuity on an ongoing basis.