

# Bandhan Financial Services Ltd.

Head Office, Kolkata – 700 091



---

## IT 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

<b>Table of contents</b> .....	3
<b>1. INTRODUCTION</b> .....	4
<b>1.1 Role of Information Technology</b> .....	4
<b>1.2 Objective of IT Policy</b> .....	4
<b>2. IT STRATEGY COMMITTEE</b> .....	4
<b>3. IT ASSET MANAGEMENT POLICY</b> .....	6
<b>4. INFORMATION SYSTEMS AUDIT POLICY</b> .....	6
<b>5. BUSINESS CONTINUITY PLANNING &amp; DISASTER RECOVERY</b> .....	7

## **INFORMATION TECHNOLOGY POLICY**

IT Policy to be adopted and keeping in view the rapid changes in emerging technologies is not intended to enforce an inflexible rigidity. The IT Policy is in compliance with the directives contained in the Reserve Bank of India's Master Circular No. DNBS.PPD.No.04/66.15.001/2016-17 dated 08-06-2017.

### **1. INTRODUCTION**

#### **1.1 Role of Information Technology**

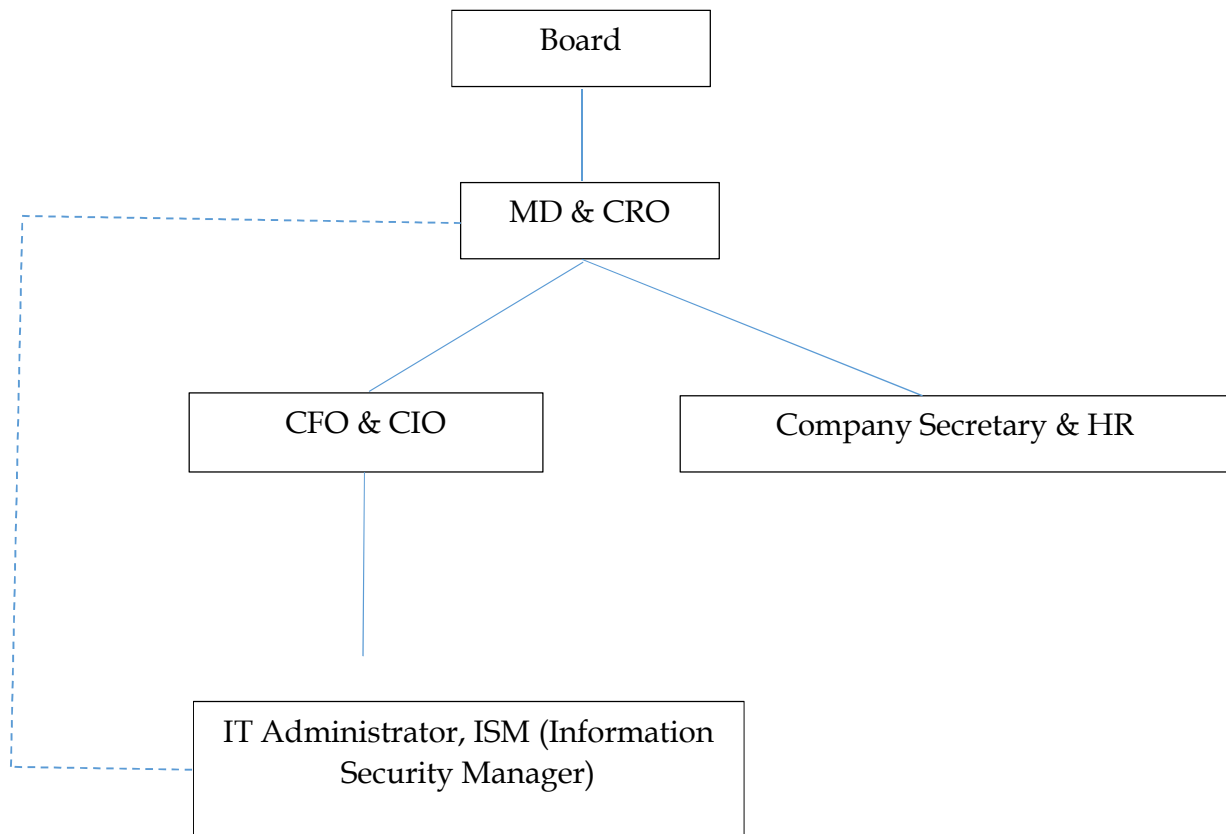
IT plays a pivotal role in any organization due to the changing technological environment and organizational needs. The Information needs of the organization are vast and complex.

#### **1.2 Objective of IT Policy**

- To provide IT infrastructure services and support to facilitate innovative use of technology for providing better service to the clients, if any.
- Integrate IT into business operations in line with the business objectives of the organization
- Explore and assess new and emerging technologies, if required.
- Provide infrastructure to COMPANY's users which is secure, personalized and timely access to information, services and support anytime anywhere.
- Provide users with the training, support, tools and information needed to foster innovative and effective use of technology, if required.

### **2. IT STRATEGY COMMITTEE**

In order to carry out review and amend the IT strategies in line with corporate strategies, Board Policy reviews, cyber security arrangements and any other matter related to IT Governance, an IT Strategy Committee is to be constituted comprising of an Independent Director as Chairman and CFO, Company Secretary, IT Administrator as member. The IT Strategy Committee is required to meet at frequent interval i.e., once in six months. In line with the above, COMPANY proposes to constitute IT Strategy Committee of comprising



The broad roles and responsibilities of the IT Strategy Committee will encompass:

- Approve IT strategy and policy documents and ensuring that the management has put an effective strategic planning process in place.
- Ascertaining that management has implemented processes and practices that ensure that the IT delivers value to the business.
- Ensuring IT investments represents a balance of risks and benefits and that budgets are acceptable.
- Monitoring the method and management uses to determine the IT resources needed to achieve strategic goals and provide high-level direction for sources and use of IT resources.
- Ensuring Proper balance of IT investments for sustaining COMPANY's growth and balancing aware about exposure towards It risks and controls.
- COMPANY CIO will ensure the implementation of IS policy to the operational level
- Technical competency of senior management personnel is up to the mark

### 3. IT ASSET MANAGEMENT POLICY

#### Overview and Purpose

IT Asset Management is an important business practice that involves maintaining an accurate inventory, licensing information, maintenance, and protection of hardware and software assets utilized by COMPANY.

The Asset Management Policy focuses on the following key activities of the asset life-cycle viz. planning, acquisition, operation & maintenance and disposal.

All IT assets of the COMPANY must be

- Acquired according to the needs.
- Recorded in the asset register in accordance with generally recognized accounting practices.
- Checked from the asset register to the individual asset and vice versa on a regular basis but not less than once per annum.
- Evaluated at least once per annum, to establish its condition as reflected on the asset register.
- Disposed of or scrapped, in the event that the asset
  - is no longer serviceable.
  - has reached the end of its useful life.
- The disposal or scrapping of assets as contemplated in must be approved by the competent authority.
- All the devices and Operating Systems support IPv6.

### 4. INFORMATION SYSTEMS AUDIT POLICY

The fundamental objective of the systems audit is to ensure that organization's assets are protected and suitable internal controls are in place to ensure protection against any unauthorized access to its information and information resources.

Information System (IS) audit evaluates the adequacy of the internal security controls with regards to System efficiency, standardization, Data integrity and safeguarding of information systems Assets / resources within COMPANY.

#### Policy

Protection of IT Assets

- Audit Trails are designed in the system to record the activity at the system, application, and user level to support security objectives namely -
  - Detecting unauthorized access to the system.
  - Facilitating the reconstruction of events.
- Preventive controls are designed to prevent an error, omission or malicious act. Some of the actionable for preventive control includes
  - Building Access control - Validation, edit checks in the application, implementing Passwords Policy.
  - Authorization of transaction.
  - Ensuring segregation of duties (SOD).
  - Appropriate Documentation for applications, application usage and various processes followed.
  - Firewalls.
  - Anti-virus software
- Asset and security Classification - An inventory of assets is being maintained which includes physical, software and information assets.

#### **IT controls regarding network security**

- This focuses on the various areas - like information security management, user account management, logical access security, authorization and authentication requirements, network infrastructure security.

**The COMPANY if required may take expert help to meet statutory IS audit requirement.**

## **5. BUSINESS CONTINUITY PLANNING & DISASTER RECOVERY**

BCP forms a significant part of an organization's overall Business Continuity Management plan, which includes policies, standards and procedures to ensure continuity, resumption and recovery of critical business processes. BCP shall be designed to minimize the operational, financial, legal, reputational and other material consequences arising from a disaster. COMPANY should follow Board approved BCP Policy. The functioning of BCP shall be monitored by the Board by way of periodic reports. The BCP may have the following salient features:

“Disaster Recovery (DR)” is the process of resuming, restoring or recovering the IT elements (computer systems, assets, and technological functionality) of a business process after an emergency, crisis, or other sudden calamitous event causing damage or loss to IT infrastructure.

## **5.1 Business Impact Analysis**

COMPANY shall first identify critical business verticals, locations and shared resources to come up with the detailed Business Impact Analysis. The process will envisage the impact of any unforeseen natural or man-made disasters on the COMPANY's business. The entity shall clearly list the business impact areas in order of priority.

## **5.2 Recovery strategy/ Contingency Plan**

COMPANY shall try to fully understand the vulnerabilities associated with interrelationships between various systems, departments and business processes. The BCP should come up with the probabilities of various failure scenarios. Evaluation of various options should be done for recovery and the most cost-effective, practical strategy should be selected to minimize losses in case of a disaster.

COMPANY shall consider the need to put in place necessary backup sites for their critical business systems and Data centers.

COMPANY shall test the BCP either annually or when significant IT or business changes take place to determine if the entity could be recovered to an acceptable level of business within the timeframe stated in the contingency plan. The test should be based on 'worst case scenarios'. The results along with the gap analysis may be placed before the Board. The GAP Analysis along with Board's insight should form the basis for construction of the updated BCP.