Berar Finance Limited
Data Protection and Security Policy

RECORD OF REVIEW:

Document Number	01
Version Number	01
Document Classification	External
Originally formulated	August 12, 2025
Created by	Information Technology (IT) Department
Reviewed by	IT Strategy Committee
Approved by	Board of Directors

1. Data Protection and Security Policy

1.1 Introduction

The 'Data Protection and Security Policy' of Berar Finance Limited ("Berar Finance)" or "Company") describes guidelines for collection, management, storage, security and protection of sensitive data or information related to customers, clients, employees and associates.

1.2 Responsibility

The responsibility of data protection and security policy at Berar Finance Limited ("Berar Finance)" or "Company") shall compromise of the following:

- IT Strategy Committee Members
- IT Steering Committee Members
- Chief Information Security Officer (CISO)
- Chief Technology Officer (CTO)

1.3 Objective

The objectives of data protection and security policy related to sensitive data or information are to:

- Maintain privacy
- Ensure security and protection
- Define roles and responsibilities for access, authorization and authentication
- Develop and implement IT infrastructure and systems for security and protection
- Address regulatory standards and compliance requirements

1.4 Scope

The scope of data protection and security policy covers sensitive data and information related to:

- Customers
- Company
- Employees (permanent / contract based)
- Vendors, service providers and contractors
- Associates and partners

1.5 Roles and Responsibilities

The roles and responsibilities are as follows for the data protection and security policy at Berar Finance Limited:

Roles	**Responsibilities**
IT Strategy Committee Members	▪ Review and approve policies related to security and protection of sensitive data or information coming under the roles, responsibilities and scope of the Committee

IT Steering Committee Members	▪ Review and propose policies to IT Strategy Committee, related to security and protection of sensitive data or information coming under the roles, responsibilities and scope of the Committee
CISO / CTO	▪ Formulate policies related to data protection and security and propose to IT Steering Committee and IT Strategy Committee ▪ Develop and implement standard practises and IT systems for security and protection of sensitive data and information ▪ Make provisions for addressing regulatory standards and compliance requirements with respect to sensitive data and information security and protection

1.6 Applicability

The applicability of data protection and security policy relates to the following segments at Berar Finance Limited:

Content	**Description**
Customer / Clients Sensitive data and information	Name, Age, Address, Gender, Financial Information, Email, Contact number, Geographical location, Photo, Video and any other personally identifiable information.
Company / Organisation data and information	Official and business-related data and information. Other data or information directly and indirectly belongs to the Company.
Vendors, Service Providers, Partners and Associates	IT systems of vendors (involved in collection, storage, utilization, processing and managing data or information related to Berar Finance Limited).
IT Systems	Softwares & Applications (Standalone, Cloud based), Servers, Networks, Laptops & desktops, storage devices and mobile phones.

1.7 Guidelines

For IT Department:

- Ensure sensitive data or information protection devices are at place
  - Servers (for centralized access and storage)
  - Firewalls (for network protection and prevention of cyber threats)
  - Antivirus (for server and endpoint devices protection)
  - Encryption technology (for data and information protection)
  - Data leakage prevention tools
  - Login credentials for access controls and security (Use strong & complex password and renew periodically)
  - System scanning and monitoring (for neutralizing viruses, malware, ransomware and cyber threats)
  - The data backup frequency shall include daily weekly and monthly time periods
  - Sensitive data or information shall be archived for the period of 3 to 5 years and data or information which is no longer required to be disposed of in a secure manner.

- Ensure all IT systems, services and equipments used for storing data or information meet acceptable security standards and regulatory compliance requirements (e.g. masking customer PI).
- Perform periodic inspection of IT systems and prepare reports as well as all sorts of documentation.
- Evaluating vendors and 3rd party services providers involved in collection, storage, processing and management of customer and company's' data or information with respect to business as well as regulatory compliances requirements.
- Designated Chief Information Security Officer (CISO) shall also be presented as a 'Data Protection Officer' and a 'Grievance Officer' and the same details shall be present on the company's website.
- Compliance related to relevant data protection acts, guidelines and practices shall be implemented. Guidelines such as Reserve Bank of India (RBI) guidelines issues through circulars and advisories. Acts such as Digital Personal Data Protection Act (DPDP Act), 2023 and Information Technology related Acts.

For Employees (permanent and contract based):

- Take customer or clients' consent by providing proper clarification and disclosing official & business objectives before collecting sensitive personal data or information through well defined, transparent and secure medium.
- Handle customer data in careful and responsible manner.
- Do not share customer data informally and misuse it.
- Do not share login credentials (user id & password) with other people.

For Vendors and service providers:

- Shall especially engage with Berar Finance Limited ("Berar Finance)" or "Company") through service level agreement (non-disclosure agreement) if involved in customer sensitive data or information collection, storage, processing, management and transmission.
- Shall only use customer data for intended business purpose.
- Shall not share data with subcontractors, associates and other third parties without informing to Berar Finance Limited ("Berar Finance)" or "Company").
- Shall cooperate in meeting and addressing all sorts of regulatory compliance requirements applicable to Berar Finance Limited ("Berar Finance)" or "Company").
- Shall keep data security and protection related IT systems at place for customers and company's data protection.

Data Disclosure:

- Any employee seeking sensitive data and information for legal and law enforcement works shall obtain written approval from senior management and share the same approval with IT department to get the data (as per the policy guidelines).

1.8 Training and Awareness

IT Department shall timely conduct training session for the employees to make them aware about data protection and security related standard practices followed in Berar Finance Limited ("Berar Finance)" or "Company") as well as cyber and information security related topics.

1.9 Policy Review

Data protection and security policy shall be reviewed and updated annually.