Freemen Investments Private Limited

Information Technology & Cyber Security Policy

Table of Contents

1. Objective

The objective of this Information Technology & Cyber Security Policy is to establish a robust framework for safeguarding the Company's digital assets, IT infrastructure, and customer data. The policy aims to prevent cyber-attacks, unauthorized access, data breaches, and ensure regulatory compliance as per RBI guidelines.

2. Scope

This policy applies to all employees, contractors, vendors, and third-party service providers who have access to the Company's IT systems, data, and infrastructure. It covers all areas of IT operations, cyber security, data protection, and incident management.

3. Regulatory Framework

The policy is developed in compliance with:

- RBI's Master Directions for NBFCs
- RBI Guidelines on Cyber Security Framework for NBFCs (2017)
- RBI's IT Governance Framework (April 2022)
- RBI's Scale-Based Regulation (SBR) Framework for NBFCs
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011

4. IT Governance Framework

4.1. IT Governance Committee:

The Company will establish an IT Governance Committee responsible for overseeing the IT and cyber security functions. The committee will consist of:

- Chief Information Officer (CIO) or equivalent
- Heads of Key Departments (Credit, Finance, Operations)

4.2. Roles and Responsibilities:

- Oversee IT and cyber security risk management.
- Approve IT budgets, strategies, and policies.
- Ensure compliance with regulatory guidelines on IT and data security.
- Regularly monitor and review the effectiveness of IT controls, infrastructure, and security measures.

4.3. Frequency of Meetings:

The IT Governance Committee will meet at least quarterly to discuss IT risk management, cyber security, and compliance matters.

5. Information Technology Risk Management

5.1. IT Infrastructure:

The Company will maintain a secure IT infrastructure, which includes hardware, software, networks, and cloud services. The infrastructure will be regularly updated to ensure security, stability, and efficiency.

The IT department is responsible for maintaining the company's IT infrastructure, including hardware, software, and networking devices across all the branches

Any changes to the IT infrastructure (Permissions and access for certain roles) must be approved by the IT department and should be documented for future reference.

Regular maintenance and upgrades to the IT infrastructure will be scheduled and communicated to all employees across all branches.

Anyone who have access to online banking software portal should only be accessing the login in the office premises. Unauthorized logins and usage will be considered as a severe breach.

5.2. IT Asset Management:

The Company will maintain an inventory of all IT assets, including hardware, software licenses, and digital resources. All assets will be monitored for vulnerabilities, performance issues, and compliance with security protocols.

5.3. System Access Control:

Role-Based Access Control (RBAC):

System access will be based on roles and responsibilities, ensuring that employees only have access to the systems and data necessary for their jobs.

User Activity Monitoring:

User activities will be monitored to prevent unauthorized access and to detect anomalies in behavior.

Acceptable Use of IT Resources

All employees must use company IT resources for work-related tasks only, personal use of company IT resources is prohibited. The use of unauthorized software, hardware or network devices is strictly prohibited.

---

6. Cyber Security Framework

6.1. Cyber Security Policy:

A robust Cyber Security Policy will be in place to safeguard the Company's systems and data from cyber threats, data breaches, and malicious attacks.

6.2. Threat Identification & Risk Assessment:

The Company will conduct periodic risk assessments to identify potential cyber threats, vulnerabilities, and areas of risk. External assessments and penetration tests will be conducted annually to evaluate the security of the IT systems.

6.3. Cyber Security Controls:

Firewalls:

Implement firewalls to protect the network from unauthorized access.

Antivirus and Anti-Malware Software:

Ensure all systems are equipped with up-to-date antivirus and anti-malware programs.

Intrusion Detection and Prevention Systems (IDPS):

Utilize IDPS to monitor network traffic and prevent unauthorized access.

Encryption:

Data in transit and at rest will be encrypted using industry-standard encryption protocols to protect sensitive information.

6.4. Endpoint Security:

Endpoint devices such as desktops, laptops, and mobile devices will be secured using endpoint protection software, including antivirus, anti-malware, and data encryption tools. Regular patching and updates will be mandatory.

6.5. Data Backup & Disaster Recovery:

Data Backup:

The customer data will be uploaded, stored, and synchronized on the service provider's server, which is hosted on Amazon Web Services (AWS) and permanently stored in the cloud.

Disaster Recovery Plan (DRP):

A disaster recovery plan will be developed and tested regularly to ensure business continuity in the event of cyber-attacks or natural disasters.

Recovery Time Objective (RTO) & Recovery Point Objective (RPO):

RTO and RPO will be defined and reviewed to ensure minimal disruption during system failures.

---

7. Data Protection & Privacy

7.1. Data Classification:

The Company will classify its data based on sensitivity levels (e.g., confidential, sensitive, public) to ensure that appropriate security measures are in place for each classification.

7.2. Personal Data Protection:

The Company will comply with data protection laws, including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Customer data, especially sensitive personal information, will be securely stored and processed.

7.3. Data Retention & Disposal:

Data Retention:

The Company will define retention periods for different types of data based on regulatory and business requirements.

Data Disposal:

Data will be securely disposed of when no longer required, following RBI guidelines and data protection laws.

---

8. Incident Response & Management

8.1. Incident Response Team (IRT):

An Incident Response Team (IRT) will be constituted to handle cyber security incidents, data breaches, and system failures. The IRT will be responsible for:

Detecting, investigating, and responding to security incidents.

Containing and mitigating the impact of cyber incidents.

Reporting the incident to senior management and the RBI, as per regulatory requirements.

8.2. Incident Reporting:

All cyber incidents, including unauthorized access, malware attacks, and data breaches, will be documented and reported to the IT Governance Committee. The RBI must be informed within 24 hours of any major security breach.

8.3. Root Cause Analysis (RCA):

Post-incident, the IRT will conduct a root cause analysis to identify the source of the problem and implement measures to prevent future occurrences.

---

9. Cyber Security Awareness & Training

9.1. Employee Training:

All employees will receive mandatory cyber security training covering topics such as phishing, password management, data protection, and safe internet usage. Training will be conducted annually or when significant changes to systems or policies occur.

9.2. Vendor & Third-Party Training:

Vendors and third-party service providers with access to the Company's systems or data must adhere to the Company's cyber security policies and undergo regular training sessions.

---

10. Audit & Compliance

10.1. IT & Cyber Security Audits:

Regular of the IT and cyber security systems will be conducted to ensure compliance with RBI guidelines and identify areas for improvement.

Any violations of this policy will be investigated and addressed in accordance with the company's disciplinary policies and procedures.

10.2. RBI Compliance:

The Company will comply with all RBI circulars and guidelines on cyber security, including regular submission of reports on IT risk, cyber incidents, and audit findings.

---

11. Review of IT & Cyber Security Policy

This policy will be reviewed annually or when significant changes in technology, cyber threats, or regulatory guidelines occur. The IT Governance Committee will oversee the review process and recommend any necessary changes to the Board of Directors for approval.

---

12. Conclusion

The IT policy is designed to provide clear guidelines for the secure, efficient, and effective use of IT resources within the Organization. It ensures compliance with RBI's guidelines and industry best practices, minimizing the risk of cyber-attacks, data breaches, and unauthorized access. Adhering to these guidelines will help protect the Company's IT resources, data, and reputation, while ensuring compliance with applicable laws and regulations.