AQUILA FINANCE LIMITED

INFORMATION TECHNOLOGY POLICY

AFL/POL/10/25-R003-07

History of the Document	Adopted by	Date of Adoption/Review
Originally Adopted	Board of Directors	10-06-2023
Review	Board of Directors	01-04-2025
Review and Amended	Board of Directors	25-10-2025

1. INTRODUCTION AND OBJECTIVE

Information Technology plays a vital role in ensuring operational efficiency, data security, and customer service excellence. Aquila Finance Limited recognizes that an effective IT governance and control framework is essential for ensuring integrity, reliability, and security of its systems and data. This Policy aims to establish structured guidelines for managing IT resources, addressing risks, and ensuring regulatory compliance.

This Information Technology (IT) Policy outlines the governance, operational, and security framework for managing the Company's information systems, IT infrastructure, and data. It provides detailed guidance on IT management practices aligned with the Reserve Bank of India's Master Direction on Information Technology Framework for NBFCs (RBI/DNBS/2016-17/53; DNBS.PPD.No.04/66.15.001/2016-17 dated June 8, 2017).

2. SCOPE AND APPLICABILITY

This Policy applies to all employees, departments, branches, outsourced vendors, consultants, and third-party service providers engaged with the Company in any capacity involving access to IT systems, applications, or data. The scope includes all hardware, software, networks, databases, and communication devices owned or operated by the Company.

3. IT GOVERNANCE AND ROLES

The Board of Directors is responsible for overall IT strategy, risk management, and policy approval. The Board delegates operational oversight to the Audit Committee, which periodically reviews IT controls, risks, and incidents. The it department is responsible for IT implementation, cyber security, and compliance with regulatory norms.

Key responsibilities:
• The Board – Approves IT strategy and reviews performance.
• IT department – Oversees IT operations, system development, data security, and business continuity, Manages servers, access controls, and system update, Provides end-user assistance and system maintenance.
• Department Heads – Ensure compliance with IT policy and data security procedures.

4. INFORMATION SECURITY FRAMEWORK

The Company’s Information Security Framework ensures confidentiality, integrity, and availability of all information assets. The framework covers asset identification, risk assessment, access control, and monitoring.

Key components include:
- Asset inventory and classification.
- Role-based access controls.
- Logical and physical security controls.
- Logging, audit trails, and monitoring.
- Annual vulnerability and penetration testing.
- Compliance with applicable RBI and data protection guidelines.

5. NETWORK SECURITY

Network security measures shall ensure that communication channels, data transfers, and networked systems are safeguarded from intrusion, malware, and unauthorized access. Firewalls, routers, and switches shall be configured securely, and access to network devices shall be restricted to authorized personnel only.

Periodic network scans, intrusion detection systems (IDS), and antivirus tools shall be deployed and updated regularly. Remote access shall be controlled through VPNs and multi-factor authentication.

6. ACCESS CONTROL AND PASSWORD MANAGEMENT

Access to systems shall be based on the principle of least privilege. Each user shall have a unique login ID. Passwords shall be complex (minimum 8 characters, mix of upper/lowercase letters, numbers, and symbols) and changed every 30 days. User sessions shall auto-lock after 10 minutes of inactivity.

7. IT ASSET MANAGEMENT

All IT assets, including hardware, software, and network equipment, shall be properly recorded in an asset register. Each asset shall have a unique identification number and lifecycle record from procurement to disposal. Periodic verification of assets shall be conducted to ensure accuracy and accountability.

8. DATA PROTECTION, STORAGE, AND RETENTION

The Company shall maintain strict control over data collection, processing, and storage. Sensitive data shall be encrypted both in transit and at rest. Backup data shall be securely stored offsite or on cloud infrastructure with restricted access. Data retention shall comply with regulatory requirements and be destroyed securely after the retention period.

9. SOFTWARE AND PATCH MANAGEMENT

Only licensed software approved by the CIO shall be installed. The IT team shall monitor and apply security patches, updates, and version upgrades in a timely manner. Unauthorized software installation or downloads are strictly prohibited.

10. CYBER SECURITY AND THREAT MANAGEMENT

The Company maintains a proactive cyber security framework for protection against phishing, ransomware, and data breaches. An incident detection and response plan shall be in place for identification, containment, eradication, and recovery from threats. Regular cyber awareness training shall be conducted for employees.

11. EMAIL, INTERNET, AND MOBILE USE POLICY

Official email accounts are for business use only. Users must not share credentials, click unknown links, or open suspicious attachments. Internet use shall be restricted to official purposes. Company-provided mobile devices must comply with mobile device management (MDM) controls.

12. INCIDENT AND BREACH RESPONSE

All security incidents, including unauthorized access or data loss, shall be immediately reported to the CIO. The CIO shall document, investigate, and report major incidents to the Board and RBI. Lessons learned shall be incorporated into control improvements.

13. OUTSOURCING AND VENDOR MANAGEMENT

The Company shall conduct due diligence before engaging third-party service providers. Service Level Agreements (SLAs) must define data ownership, confidentiality, access control, and termination rights. Vendors must follow equivalent IT security standards as the Company.

14. BUSINESS CONTINUITY AND DISASTER RECOVERY

A comprehensive Business Continuity Plan (BCP) and Disaster Recovery (DR) framework shall ensure continued operations in case of system failure, disaster, or cyber incident. Critical data and systems shall be backed up weekly, and restoration tests shall be performed quarterly. Alternate processing sites shall be identified.

15. MONITORING, AUDIT, AND REPORTING

Internal and external audits shall assess IT controls, data integrity, and system performance. The CIO shall submit quarterly IT compliance reports to the Audit Committee. Audit observations shall be acted upon promptly.

16. POLICY REVIEW AND UPDATION

This Policy shall be reviewed annually or upon significant technological, regulatory, or operational changes. The CIO is responsible for initiating the review and recommending updates to the Board.

BY THE ORDER OF THE BOARD OF DIRECTORS

For AQUILA FINANCE LIMITED