NORTH EAST HIRE PURCHASE CO INDIA PRIVATE LIMITED

IT Policy

1. Introduction

This IT Policy is established to ensure the secure, efficient, and compliant use of information technology (IT) within North East Hire Purchase Co India Private Limited (hereinafter referred to as NEHPCIPL"). It is designed to align with the guidelines provided by the Reserve Bank of India (RBI) and is applicable to all employees, contractors, and third-party service providers.

2. Objectives

The primary objectives of this IT policy are:

- To ensure the confidentiality, integrity, and availability of information assets.
- To safeguard against unauthorized access, data breaches, and cyber threats.
- To comply with RBI guidelines and other applicable regulations.
- To promote efficient use of IT resources.

3. Scope

This policy applies to all IT systems, networks, and data owned or managed by NEHPCIPL, including those provided by third-party vendors.

4. IT Governance

- **IT Strategy:** The IT strategy shall be reviewed annually by the IT Committee and updated as necessary.
- **Risk Assessment:** Regular IT risk assessments shall be conducted to identify and mitigate potential threats.

5. Information Security

- **Access Control:** Access to systems and data shall be restricted based on role requirements. Multi-factor authentication (MFA) shall be implemented for critical systems.
- **Data Encryption:** All sensitive data shall be encrypted both at rest and in transit using industry-standard encryption protocols.
- **Security Monitoring:** Continuous monitoring of IT systems shall be conducted to detect and respond to potential security incidents.

6. Data Privacy

- **Personal Data Protection:** Personal data of customers, employees, and stakeholders shall be handled in accordance with applicable data protection laws.
- **Data Retention:** Data shall be retained only for as long as necessary for business or legal purposes. A data deletion process shall be in place for the secure disposal of data.

7. Vendor Management

- **Third-Party Due Diligence:** Vendors providing IT services shall undergo due diligence to assess their security posture. Contracts shall include provisions for data protection and compliance with this policy.
- **Service Level Agreements (SLAs):** SLAs with vendors shall be established, monitored, and reviewed regularly to ensure performance meets the company's standards.

8. Incident Management

- **Incident Response Plan:** An incident response plan shall be in place to address IT security breaches, data leaks, and other emergencies. The plan shall be tested annually.
- **Reporting:** Employees and contractors are required to report any suspected security incidents or breaches immediately to the IT department.

9. Training and Awareness

- **Employee Training:** All employees shall receive regular training on IT security best practices, data protection, and compliance requirements.
- **Awareness Programs:** The company shall conduct ongoing awareness programs to keep employees informed about the latest security threats and preventive measures.

10. Review and Updates

This IT policy shall be reviewed annually or as required by changes in regulatory requirements or business needs.