INFORMATION TECHNOLOGY POLICY

Ajivika Finance Limited RBI Registered NBFC | RBI CoR No.: B-12.00476

Date of Policy Approval: 1st October 2026

1.0 INTRODUCTION AND POLICY STATEMENT

This policy sets out the requirements for protecting the Information Technology (IT) network, hardware (including portable media), system and application software, communication components, documentation, physical environment and other information assets of Ajivika Finance Limited.

2.0 SCOPE

The following equipment and infrastructure are covered by this policy:

- **Network infrastructure:** Equipment housed internally to provide the IT network, including servers, enclosures, racks, cabling, switches/hubs, routers, wireless access points, firewalls, proxies, authentication systems and devices.
- **Laptops and/or Desktops:** Personal computers (PCs) provided to staff to carry out their duties.
- **Media and portable media:** Electronic storage devices, such as pen drives and hard drives, provided to staff to carry out their duties.
- **External communications infrastructure:** Equipment and services used to connect to external networks, including the Wide Area Network, analogue and digital telephone lines, leased lines and related equipment and services.

3.0 POLICY OBJECTIVES

This policy aims to ensure:

- **Confidentiality:** Data and information assets are protected against unauthorised disclosure, and incidents are promptly reported.
- **Integrity:** Data and information assets are protected against unauthorised or accidental modification.
- **Availability:** IT systems are available and accessible to staff when required.

4.0 ROLES AND RESPONSIBILITIES

Defined responsibilities ensure that all users of IT systems understand their obligations to minimize risks to IT security and operations.

4.1 Business Planning Department

The Business Planning department is responsible for ensuring that:

- Electronic filing systems and documentation are maintained for all critical job functions to ensure continuity.
- Unauthorised staff cannot access IT systems at any location, as such access could compromise data integrity.
- Named individuals are authorised to administer specific computer systems according to their job function and role, following the principle of least privilege.

- All current and new users are instructed in their security responsibilities.
- Procedures are implemented to minimize exposure to fraud, theft or system disruption, including segregation of duties, dual control and staff rotation in critical, susceptible areas.

4.2 Human Resources Department

The Human Resources department is responsible for ensuring that:

- All staff sign confidentiality (non-disclosure) undertakings as part of their employment contracts, and contractors and temporary staff also sign confidentiality undertakings.
- New staff receive basic IT security training as part of their induction.

4.3 Users Without Administration Rights

Users who do not have administration rights over their issued equipment are responsible for ensuring that:

- Computer security breaches do not arise from their negligence. Passwords and remote login details must be kept secure, particularly when working from home or using wireless networks.
- Reasonable care is taken to protect issued IT equipment and the confidential data stored on it when the equipment is taken outside secure offices.
- Sensitive data stored on portable IT equipment is limited to what is required for business use and is encrypted to minimize the risks and impact of a security breach or loss of equipment.

5.0 SECURITY CONTROLS

5.1 Technical and Operational Security

- Technical security measures must protect systems against viruses and other malicious software. All IT systems must be monitored for potential security breaches.
- Email and internet use must comply with the Email and Internet policy.
- All IT equipment, including virtual systems, must be uniquely identified and recorded.
- Environmental controls must be maintained in server and communications rooms at all premises to protect key equipment. Smoking, drinking and eating are prohibited in these areas.
- Records of all faults and suspected faults must be maintained.

5.2 Physical Access Controls

Server and communications rooms, and IT equipment storage rooms, must remain locked at all times. Keys and access codes must be held securely by the IT department.

5.3 Third-Party Remote Access

Third parties must not be given remote access to systems unless specific authorization has been received.

6.0 DISPOSAL AND REALLOCATION OF EQUIPMENT

Equipment allocated to an individual user must not be reallocated within a department. It must always be returned to the IT department for reallocation to ensure that sensitive data is managed correctly.

7.0 SECURITY INCIDENT INVESTIGATION AND REPORTING

7.1 Objective and Incident Definition

The objective of security incident investigation is to identify, detect, investigate and resolve suspected or actual computer security breaches.

A security incident is an event that may result in:

- Degraded system integrity.
- Loss of system availability.
- Disclosure of confidential information.
- Disruption of activity.
- Financial loss.
- Legal action.
- Unauthorised access to applications.
- Loss of data.

7.2 Reporting and Recording

All users must report actual security breaches, and any concerns or suspicions about security breaches, as soon as they arise.

The IT department must formally log all actual security incidents, categorize them by severity, record the actions taken and report them to the Directors.

8.0 DATA BACKUP AND PERIODIC RESTORATION TESTING

8.1 Backup Responsibilities and Schedule

Periodic backups must be carried out to prevent information loss caused by destruction of the storage media. Network administrators are responsible for backing up information held on shared-access servers.

- **Daily:** Full backups of all critical business applications.
- **Weekly:** Complete full backups, including file servers and older data stored on servers.

8.2 Restoration Testing

Restoration testing must be carried out periodically, as hard disks and magnetic tapes are prone to errors.

9.0 POLICY MONITORING AND REVIEW

The IT department must monitor this policy to ensure that it remains fit for purpose. The policy must be reviewed every three years.