Information Security Policy

LinkIT Advanced Solutions Ltd
Version: 1.0
Date: 25 February 2026
Review Date: 25 February 2027
Approved by: Ian Sloan – Chairman and Managing Director

---

1. Purpose

The purpose of this policy is to protect the confidentiality, integrity, and availability of information handled by LinkIT Advanced Solutions Ltd ("the Company") and to ensure that information is managed securely in line with recognised good practice, including principles from ISO/IEC 27001.

This policy applies to all employees, contractors, and third parties working on behalf of the Company.

---

2. Scope

This policy covers:

- Customer information (including scanned and stored copier data)
- Employee data
- Supplier data
- Electronic and paper records
- IT systems, email, and cloud services
- Multi-function devices (MFDs), copiers, and associated storage devices

---

3. Management Commitment

Senior management is committed to:

- Protecting information assets from unauthorised access, disclosure, alteration, or destruction
- Complying with UK data protection legislation
- Maintaining appropriate technical and organisational security measures
- Reviewing this policy annually or when significant changes occur

---

4. Information Security Objectives

The Company aims to:

1. Prevent data breaches.
2. Ensure secure configuration and deployment of copier devices.
3. Protect customer data stored on hard drives or internal memory.
4. Ensure secure disposal or wiping of devices before resale or return.
5. Respond effectively to security incidents.

---

5. Roles and Responsibilities

Director

- Overall responsibility for information security.
- Ensures compliance with legal and contractual requirements.
- Approves and reviews this policy.

Employees and Engineers

- Follow security procedures.
- Protect passwords and access credentials.
- Report incidents immediately.

---

6. Risk Management

The Company conducts periodic risk assessments to:

- Identify potential threats to information.
- Assess likelihood and impact.
- Implement proportionate controls.

Risks are reviewed at least annually.

---

7. Access Control

- Access to company systems is restricted to authorised personnel only.

- Unique user accounts are used.
- Strong passwords are required.
- Access is removed promptly when staff leave.

---

8. Device & Copier Security

As a copier and printer managed services supplier, the Company recognises that multi-function devices may store sensitive data.

Controls include:

- Secure configuration of devices before deployment.
- Enabling encryption features where available.
- Password protection of admin interfaces.
- Removal of stored data before returning devices.
- Secure wiping or destruction of hard drives prior to resale or disposal.
- Engineer procedures for secure handling of customer data.

---

9. Data Protection

The Company:

- Processes personal data lawfully and fairly.
- Collects only necessary data.
- Stores data securely.
- Retains data only as long as required.
- Ensures secure deletion when no longer needed.

---

10. Incident Management

All suspected or actual information security incidents must be reported immediately to the Director.

Incidents will be:

- Assessed promptly.
- Contained and mitigated.

- Documented.
- Reported to customers or authorities where legally required.

---

11. Business Continuity

The Company maintains basic business continuity measures including:

- Secure cloud backups of critical business data.
- Alternative communication methods.
- Ability to continue essential support services in the event of disruption.

---

12. Supplier Security

Where third-party providers are used (e.g., IT support, cloud services), the Company ensures they:

- Provide appropriate security controls.
- Comply with relevant data protection requirements.
- Are assessed proportionately before engagement.

---

13. Training & Awareness

Staff receive information security guidance appropriate to their role, including:

- Password security
- Phishing awareness
- Secure device handling
- Data protection obligations

---

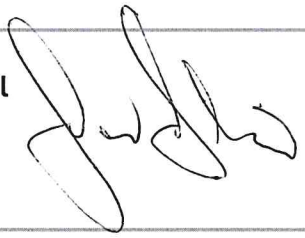
14. Policy Review

This policy is reviewed annually or following:

- A significant security incident
- Regulatory change
- Business expansion

- Framework or contractual requirement updates

Approval

Signed: 

Ian Sloan
Chairman and Managing Director
LinkIT Advanced Solutions Ltd

Date: 26/2/26