alocalprinter

Information/Cyber Security Policy

Purpose

The purpose of this Information Security Policy is to protect A Local Printer Ltd's information assets from threats, whether internal or external, deliberate or accidental. This policy ensures the confidentiality, integrity, and availability of information, while complying with applicable legal, regulatory, and contractual requirements.

Scope

This policy applies to:

- All employees, contractors, consultants, temporary staff, and third-party service providers.
- All information systems, networks, applications, and devices owned, leased, or managed by A Local Printer Ltd
- All information assets, including data in electronic, paper, or verbal form.

Information Security Objectives

- Protect information against unauthorised access and disclosure.
- Maintain the accuracy and completeness of information.
- Ensure availability of information when required.
- Comply with all applicable laws, regulations, and contractual obligations.
- Promote security awareness and accountability among staff.

Roles and Responsibilities

Management:

- Provide leadership and resources to implement and maintain information security.
- Ensure staff compliance with this policy.

Information Security Officer (ISO Miranda Barnett):

- Develop, maintain, and enforce security policies, procedures, and standards.
- Conduct risk assessments and audits.
- Report security incidents to management.

Employees and Contractors:

- Follow all information security policies and procedures.
- Report security incidents or weaknesses immediately.
- Protect access credentials and sensitive information.

Acceptable Use

- Company resources, including IT systems and devices, are to be used for business purposes only.
- Personal use must be minimal and not interfere with work or security.
- Unauthorised installation of software or hardware is prohibited.

Data Classification and Handling

All information must be classified and handled according to its sensitivity:

Classification	Description	Handling Requirements
Public:	Information available to anyone	No special controls
Internal:	Company operational information	Limited access; encrypted if stored electronically
Confidential:	Sensitive business or customer data	Access strictly controlled; encryption required; secure disposal

Access Control

- Access to information and systems must be granted based on job role and the principle of least privilege.
- Unique user IDs and strong passwords are required.
- Multi-factor authentication (MFA) must be used where possible.
- Terminated employees must have access revoked immediately.

Physical Security

- Facilities must be secured to prevent unauthorised access.
- Sensitive areas must have restricted access, monitored by security systems or personnel.
- Equipment must be protected from theft, damage, or environmental hazards.

Network and System Security – Regis IT

- Firewalls, antivirus, and intrusion detection systems must be implemented and maintained by Regis IT.
- Systems will be patched and updated regularly.
- Remote access will use secure methods, such as VPNs or encrypted connections.
- Regular backups will be conducted and tested for recovery.

Incident Management

- All security incidents must be reported immediately to the ISO (Miranda Barnett) or designated security contact (Adam Lavery, Regis IT).
- Incidents will be investigated, documented, and resolved according to the Incident Response Plan.

Awareness and Training

- All personnel to receive regular training on information security policies and procedures.
- Training to cover topics such as phishing, password security, data handling, and incident reporting.

Compliance

- Compliance with this policy is mandatory.
- Non-compliance may result in disciplinary action, including termination.
- Regular audits will be conducted to ensure adherence to this policy.

Policy Review

- This policy will be reviewed at least annually or after significant changes to business operations, technology, or regulations.
- Updates must be approved by senior management.

Approved by: M. Barnett

Date: 18 June 2025