S10 Supplies Ltd,

Information Security Policy

1. Introduction

1.1 Purpose

This Information Security Policy establishes guidelines and requirements to ensure the protection of S10 Supplies Ltd, information assets. The policy aims to safeguard the confidentiality, integrity, and availability of information, thereby reducing the risk of data breaches, unauthorized access, and other security incidents.

1.2 Scope

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at S10 Supplies Ltd, including all personnel affiliated with third parties. It covers all information systems, networks, applications, and data owned or managed by S10 Supplies Ltd.

2. Policy Statement

S10 Supplies Ltd, is committed to protecting its information assets from all threats, whether internal or external, deliberate or accidental. All information must be protected in a manner consistent with its sensitivity, value, and criticality.

3. Information Security Principles

3.1 Confidentiality

Information must be accessible only to those authorized to have access.

3.2 Integrity

Information must be accurate and complete, and IT systems must be maintained to ensure data integrity.

3.3 Availability

Information must be available and usable when required and systems must function as needed.

4. Responsibilities

4.1 Management

- Establish and maintain the information security policy.
- Provide necessary resources to implement and enforce the policy.
- Ensure that security policies and procedures are communicated to all relevant parties.

4.2 IT Department

- Implement technical controls to protect information assets.
- Monitor and respond to security incidents.
- Conduct regular security audits and vulnerability assessments.

4.3 Employees

- Comply with all security policies and procedures.
- Report any security incidents or suspicious activities.
- Protect login credentials and other sensitive information.

5. Risk Management

5.1 Risk Assessment

Regular risk assessments must be conducted to identify and evaluate potential threats to information assets.

5.2 Risk Mitigation

Appropriate measures must be taken to mitigate identified risks, including implementing technical, administrative, and physical controls.

6. Access Control

6.1 User Access Management

- User access must be controlled through formal procedures to ensure authorized use of information systems.
- Access rights must be assigned based on the principle of least privilege.

6.2 Password Management

- Passwords must meet complexity requirements and be changed regularly.
- Users must not share passwords or write them down.

7. Data Protection

7.1 Data Classification

- Information must be classified based on its sensitivity and criticality.
- Appropriate security controls must be applied according to the classification level.

7.2 Data Encryption

- Sensitive data must be encrypted both in transit and at rest.
- Encryption keys must be managed securely.

8. Incident Management

8.1 Incident Response

- An incident response plan must be established and maintained.
- All security incidents must be reported, documented, and investigated promptly.

8.2 Breach Notification

- Affected parties must be notified of security breaches in accordance with legal and regulatory requirements.

9. Training and Awareness

9.1 Security Awareness Training

- All employees must receive regular security awareness training.
- Training must cover key security policies, procedures, and best practices.

9.2 Specialized Training

- Employees with specific security roles must receive specialized training relevant to their responsibilities.

10. Compliance and Monitoring

10.1 Legal and Regulatory Compliance

- All information security practices must comply with applicable laws and regulations.
- Regular audits must be conducted to ensure compliance.

10.2 Continuous Monitoring

- Security systems and networks must be continuously monitored for threats and vulnerabilities.
- Logs must be maintained and reviewed regularly.

11. Review and Revision

11.1 Policy Review

- This policy must be reviewed annually or whenever significant changes occur in the organization or its environment.
- Revisions must be approved by senior management.

12. Enforcement

12.1 Disciplinary Actions

- Violations of this policy may result in disciplinary action, up to and including termination of employment.
- Legal actions may be taken in cases of unlawful behavior.

By following this Information Security Policy, S10 Supplies Ltd, aims to protect its information assets and ensure the security and privacy of its data. This policy will be reviewed and updated regularly to adapt to evolving threats and business needs.