

Company IT Security Policy Draft

Effective Date: [MM/DD/YYYY]

1. Purpose

This IT Security Policy defines the requirements and responsibilities to protect Company information, assets, and resources from unauthorized access, disclosure, modification, destruction, or disruption.

2. Scope

This policy applies to all employees, contractors, and third-party users who have access to Company information systems, data, and networks.

3. Policy

3.1 Acceptable Use

- Information systems are to be used only for business-related activities.
- Unauthorized use, sharing, or transmission of confidential information is strictly prohibited.
- Personal use of Company IT resources should be minimal and must not interfere with business operations.

3.2 Access Control

- Users must have unique user IDs and strong passwords for system access.
- Access rights are assigned based on the principle of least privilege.
- Accounts must be disabled or removed in a timely manner upon employee departure or role change.

3.3 Data Protection

- Sensitive data must be encrypted in storage and transit where applicable.
- Regular backups must be performed and stored securely.
- Disposal of information or assets must follow appropriate data destruction procedures.

3.4 Physical and Environmental Security

- Access to IT equipment and server rooms must be restricted to authorized personnel.
- Devices must not be left unattended when logged in.

3.5 Incident Management

- All suspected or confirmed security incidents must be reported immediately to IT.
- Incident responses will be coordinated by the IT Security team.

4. Responsibilities

- All users are responsible for complying with this policy.
- IT is responsible for implementing, monitoring, and updating security controls.
- Managers are responsible for communicating the policy and ensuring team adherence.

5. Enforcement

Violations of this policy may result in disciplinary action up to and including termination, as well as legal consequences.

6. Review and Revision

This policy will be reviewed annually and updated as necessary.

Approved by: _____

Date: _____