IT Security Policy

1. Purpose

The purpose of this IT Security Policy is to protect the organization's information assets from unauthorized access, disclosure, alteration, or destruction, ensuring confidentiality, integrity, and availability of data.

2. Scope

This policy applies to all employees, contractors, and third-party vendors who access the company's IT systems, networks, and data.

3. Roles & Responsibilities

- Employees: Must follow security procedures, report security incidents, and use company IT resources responsibly.
- IT Department: Responsible for implementing security controls, monitoring systems, and providing training.
- Management: Ensure compliance with IT security policies and support security initiatives.

4. Access Control

- Access to systems and data is based on role-based permissions.
- Passwords must follow strong complexity rules and be updated regularly.
- Multi-factor authentication (MFA) is mandatory for critical systems.

5. Data Security

- Confidential data must be stored securely and encrypted where necessary.
- Sensitive information must not be shared outside authorized personnel.
- Backup procedures must be followed to ensure data recovery.

6. Network Security

- Firewalls and antivirus software must be active and updated.
- Remote access to the network requires secure VPN connections.
- Unauthorized devices are not allowed on the corporate network.

IT Security Policy

7. Incident Management

- All security incidents must be reported immediately to the IT department.

- IT will investigate incidents and take corrective actions.

- Employees must cooperate with investigations and follow instructions.

8. Training & Awareness

- Employees will receive regular IT security training.

- Awareness programs will be conducted to ensure understanding of policies.

9. Compliance

- Non-compliance with this policy may result in disciplinary action.

- This policy is aligned with legal and regulatory requirements applicable to the organization.

10. Review & Updates

- The IT Security Policy will be reviewed annually or whenever significant changes occur in the IT environment.

- Updates will be communicated to all relevant personnel.

Approved by: _____

Date: _____