IT Security Policy

Policy Title

IT Security Policy

Policy ID

POL-SEC-001

Effective Date

01-Jan-2025

Last Reviewed

01-Aug-2025

Owner

IT Department

Approved By

Compliance Officer

1. Purpose

This policy outlines the security measures and responsibilities to protect the organization's information systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction.

2. Scope

This policy applies to all employees, contractors, and third-party users who access the organization's IT systems, including hardware, software, networks, and data.

3. Policy Statements

3.1 Access Control

- Users must use unique credentials.

- Access rights are granted based on job roles.

- Multi-factor authentication is mandatory for sensitive systems.

3.2 Data Protection

- All sensitive data must be encrypted at rest and in transit.

- Personal data must be handled in accordance with applicable data protection laws.

3.3 Device Security

- Company devices must have antivirus and endpoint protection installed.

- Lost or stolen devices must be reported within 24 hours.

3.4 Network Security

- Firewalls and intrusion detection systems must be maintained.

- Remote access must be via secure VPN.

3.5 Incident Reporting

- Security incidents must be reported immediately to the IT Helpdesk.

- A formal investigation will be conducted for all incidents.

4. Compliance

Failure to comply with this policy may result in disciplinary action, including termination of employment or legal action.

5. Review and Updates

This policy will be reviewed annually or upon significant changes to IT infrastructure or regulations.