Security Policy

SECURITY POLICY

1. OBJECTIVE

To protect information assets and ensure confidentiality, integrity, and availability.

2. USER ACCESS CONTROL

Users must have unique IDs and passwords. Access is granted based on roles.

3. DATA PROTECTION

Sensitive data must be encrypted in transit and at rest. Unauthorized copying or transfer is not allowed.

4. INCIDENT RESPONSE

All security incidents must be reported immediately. An investigation will be conducted by the IT Security Team.

5. PHYSICAL SECURITY

Access to server rooms is restricted to authorized personnel only. Visitors must be escorted.

6. ANTIVIRUS AND PATCH MANAGEMENT

All systems must run updated antivirus software and be patched regularly.

7. NETWORK SECURITY

Firewalls, intrusion detection systems, and secure configurations must be maintained.

8. AUDITS

Regular audits will be conducted to ensure policy compliance.

9. TRAINING

Employees must complete annual security awareness training.

10. ENFORCEMENT

Violations may lead to disciplinary action or termination.