# Remote Device Security Configuration Policy

**Document Version:** 1.0
**Effective Date:** [Insert Date]
**Owner:** [Insert Owner]

---

## 1. Purpose

This policy defines security requirements for configuration and use of remote devices accessing organizational information systems and resources.

## 2. Scope

This policy applies to all employees, contractors, consultants, and other authorized users with access to company data and systems using remote devices, including but not limited to laptops, tablets, and smartphones.

## 3. Policy

- All remote devices must use up-to-date operating systems and security patches.
- Devices must be protected with passwords, PINs, or biometric authentication.
- Full device encryption must be enabled on all remote devices handling sensitive company data.
- Anti-malware and endpoint protection must be installed and regularly updated.
- Connections to company resources must use secure VPN or equivalent secure connections.
- Users must not share devices used for company business without explicit approval.
- Lost or stolen devices must be reported to IT immediately.
- Remote wipe capability must be enabled where technically feasible.
- Access to company data must be removed from devices before decommissioning or transfer.

## 4. Responsibilities

- Users are responsible for adhering to this policy and reporting any incidents or violations.
- IT is responsible for ensuring compliance through regular audits and providing user support.

## 5. Enforcement

Violation of this policy may lead to disciplinary action, up to and including termination of employment or contract.

## 6. Review

This policy will be reviewed annually and updated as required.