Endpoint Encryption Standards for Home Offices

1. Purpose

This document outlines the minimum requirements for encrypting endpoint devices used in home offices to protect sensitive organizational data.

2. Scope

These standards apply to all endpoint devices (e.g., laptops, desktops, mobile devices, USB drives) used for storing, processing, or transmitting company data outside official office premises.

3. Device Coverage

Device Type	Encryption Requirement	Minimum Standard
Laptops / Workstations	Full Disk Encryption	AES-256
Mobile Devices	Device Encryption	AES-128 or higher
External Storage (USB, HDD)	Hardware/Software Encryption	AES-256

4. Encryption Implementation

- Devices must use company-approved encryption solutions (e.g., `BitLocker`, `FileVault`, `VeraCrypt`).
- Encryption must be enabled before storing any company data locally.
- Removable media must be encrypted prior to use or data transfer.
- Encryption keys must be stored securely, not on the encrypted device.

5. Key Management

- Ensure that recovery keys are generated and securely backed up.
- Never share encryption passwords or keys in plain text.
- Use a centralized or company-approved key management system where feasible.

6. Compliance & Verification

- Device encryption status must be verified during device onboarding and at regular intervals.
- Non-compliant devices must not access company resources or networks.
- Report lost, stolen, or compromised devices immediately to IT security.

7. Exceptions

Any exception to these standards requires written approval from the IT security team and must detail compensating controls.

8. Review & Updates

These standards are subject to annual review or as required due to regulatory or organizational changes.