Device & Endpoint Management policy

Version 4

REZOLVE.ai

Document Information

Name of the document	Device & Endpoint Management Policy
Release date	23-May-2025
Owned by	Mayank Baghel
Governed by	Udaya Bhaskar Reddy

Revision History

Version No	Version Date	Details of Change
1	21-May-2025	Initially Drafted
2	22-May-2025	Final
3	25-June-2025	Updated Document information
4	29-May-2026	Reviewed and updated

Reviewer and Approver

Name	Title	Comments	Date Reviewed
Mr.Udaya Bhaskar Reddy	Co-Founder & CTO	Approved	04-June-2026

Contents

1.Purpose
2.Scope
3.Policy requirements
4.Review and Maintenance
5.Enforcement
6. Appendices to be maintained

1. Purpose

To define security requirements for endpoint devices (laptops, desktops, mobile phones, tablets) used to access, store, transmit, or process company data, in order to protect against loss, theft, malware, or unauthorized access.

2. Scope

This policy applies to all employees, contractors, and vendors with access to company data.

- All company-managed devices
- BYOD devices used for accessing organizational assets
- Third-party/vendor systems with access to company environments

3. Policy Requirements

3.1 Device Enrollment & Inventory

- All company-issued devices must be registered in the endpoint inventory system (e.g., Seqrite).
- BYOD devices must be pre-approved and recorded with security attestation.

3.2 Baseline Security Controls

All endpoints must have the following:

- Full disk encryption (e.g., BitLocker, FileVault)
- Anti-virus and anti-malware protection
- Software firewall enabled
- Data Loss Prevention (DLP) controls based on user role
- Screen auto-lock enabled after 5–10 minutes of inactivity
- OS auto-updates enabled or centrally managed via patching tools

3.3 Approved Applications and Stores

- Only applications listed in the Approved Applications List may be installed or used for company work.
- App installation is only permitted from official sources (Microsoft Store, Apple App Store, etc.)

3.4 Remote Work and Mobile Devices

- Mobile endpoints (iOS/Android) accessing company systems must:
  - Be protected with PIN/biometric
  - Allow remote wipe if lost or compromised
  - Preferably be enrolled in MDM (e.g., Intune, Jamf, Kandji)
- No mobile app should store company data unencrypted.

3.5 BYOD Requirements

- BYOD usage is allowed only after written approval and completion of a Security Readiness Checklist.
- Must meet the same controls as company devices (encryption, AV, firewall).
- May be subject to remote wipe or access revocation if data risk is identified.

3.6 Third-Party Devices

- Third-party access to systems (e.g., support vendors) must go through:
  - Signed Data Processing Agreement (DPA)
  - Device security declaration
- Company reserves the right to audit or terminate third-party access if non-compliance is observed.

3.7 Change Management

- OS upgrades, security patches, and software changes must follow the Change Tracker process.
- Unauthorized modification of system configurations is prohibited.

3.8 Device Loss or Theft

- Employees must report loss or theft of any device within 4 hours.
- IT/Security will trigger remote wipe and revoke access where possible

4. Review and Maintenance

- This policy will be reviewed annually or upon major security events.
- Updates will be communicated to all employees via email and internal channels.

5. Enforcement

Violation of this policy may result in:

- Access suspension
- Disciplinary action
- Contract termination for third parties

6. Appendices (To Be Maintained Separately)

- Approved Application & Software List
- Endpoint Compatibility Checklist
- BYOD Security Readiness Checklist
- List of MDM/Endpoint Tools in Use

NOTE – Next review cycle for this policy is **March 2027**.
Management can review the policy at any time and can make changes depending on the situation.

All documents related to policies and procedures - any reference to Actionable Science is as good as Rezolve.ai.