

Endpoint Security Policy Template

A free, fill-in-the-blank policy for laptops, desktops, servers, and phones: ten sections, a device baseline, a compromised-endpoint checklist, an evidence list, and a framework mapping guide.

Company: _____

Effective date: _____

Policy owner: _____

Review cycle: At least annually, and after any change to tooling or device mix

HOW TO USE THIS TEMPLATE

Replace every [bracketed field] with your own details, delete the guidance notes, then have leadership approve and date the final document. Sample times and numbers are illustrative starting points, not benchmarks or framework requirements. Personal devices belong in a separate BYOD policy, device lifecycle in an MDM policy, update timelines in a patch management policy, and network controls in a network security policy. This template is a starting point, not legal advice. See ComplyJet's [Endpoint Security Policy guide](#) for the reasoning behind each section.

1. Purpose and Scope

This policy sets the minimum security requirements for every endpoint that connects to [Company] systems or handles [Company] data, so that every device has a named owner, a known configuration, and auditable evidence.

It applies to all employees, contractors, and temporary staff, and to the following endpoints: company laptops and desktops; servers and virtual machines running an operating system [Company] manages; company-owned phones and tablets; and [contractor or personal devices, only where permitted, under the stated lighter baseline].

2. Roles and Responsibilities

Role	Responsibility
Policy Owner ([IT Lead])	Maintains this policy, the endpoint inventory, and the endpoint tooling. Triage alerts, approves elevation requests, and approves exceptions.
Endpoint User	Keeps the device secure, does not disable or bypass security tools, and reports a suspected compromise immediately.
Engineering Lead	Owns the baseline for servers, virtual machines, and cloud workspaces.
Leadership	Approves this policy and any standing exceptions.

3. Endpoint Baseline

Control	Requirement
Disk encryption	Full-disk encryption is enabled and enforced on every laptop, desktop, and phone.
Screen lock	Automatic lock after [5] minutes of inactivity, protected by a passcode that meets the [Access Control Policy].
Host firewall	Enabled on every endpoint, with inbound connections denied by default.
Supported operating system	Only vendor-supported versions are permitted. Update timelines follow the [Patch Management Policy].
Malware protection and EDR	See Section 4.
Administrator rights	No standing administrator rights. See Section 5.
Approved software	Installed only from [approved sources or an allowlist].
Central reporting	Every endpoint reports to [management or protection console]. A device that has not reported for [7] days is non-compliant.

4. Malware Protection and Endpoint Detection and Response

All in-scope endpoints must run [approved endpoint protection tool] with real-time protection, automatic updates, and tamper protection enabled. The tool must report to the central console. Users must not disable, uninstall, or bypass it.

The Policy Owner reviews alerts and triages each within [24 hours]. Agent updates are rolled out to a pilot group of [number] devices before the wider fleet. Where an operating system is not supported by the tool, the alternative controls are documented as an exception under Section 10.

5. Administrator Rights and Software Installation

Users do not hold standing administrator rights on company endpoints. A user who needs elevated rights for a specific task must request them from the Policy Owner, who may approve elevation for no longer than [8] hours. Every request and approval is logged. Standing administrator rights require a written exception under Section 10.

Software may be installed only from [approved app stores, a managed catalog, or the approved software list]. Software outside that scope requires approval from the Policy Owner.

6. Removable Media

Removable storage devices are blocked on company endpoints by default. A user who needs one must obtain approval from the Policy Owner, who records the business reason and the device. Approved drives must be encrypted. Unknown media found or received from outside the company must not be connected to any company device.

7. Hardening and Configuration

Each supported operating system has a documented configuration baseline based on [CIS Benchmark or internal standard]. At minimum: unused services disabled, default accounts removed or disabled, host firewall enabled, secure boot and disk encryption enabled where supported, and automatic session lock configured. Baselines are reviewed at least annually.

8. Logging and Monitoring

Endpoint protection and management tools must log malware detections, tamper attempts, administrator elevation, and removable media events. Logs are retained for [12] months and reviewed by the Policy Owner [weekly]. See the [Logging and Monitoring Policy].

9. Compromised Endpoint Response

A user who suspects an endpoint is compromised must report it to [IT Lead] immediately. The Policy Owner is authorized to isolate the device without prior approval, with a target of [1 hour] from confirmation. The steps below are followed in order, and the event is assessed under the [Incident Response Plan].

1. Isolate the device from the network.
2. Revoke access: sign out sessions, reset credentials, revoke tokens.
3. Collect evidence before wiping: logs, alert records, and a disk image if warranted.
4. Rebuild from a known-good image rather than cleaning in place.
5. Review whether data was exposed and whether the event is a reportable breach.

10. Exceptions, Review, and Enforcement

An endpoint that cannot meet this policy may be used only under a written exception stating the reason, compensating controls, an expiry date not longer than [12] months, and approval by [Leadership role]. The Policy Owner reviews this policy at least annually and after any change to tooling or device mix. Violations are handled under [disciplinary / HR security policy]. Users acknowledge this policy when they receive or re-receive a device.

User acknowledgment: I have read and understand this policy. Name: _____ Date:

Endpoint Inventory Layout

Device ID	Type	Owner	OS	Encrypted	Protection reporting	Admin rights

Compromised Endpoint Checklist

Step		Done by / time
☐	Report received and logged	
☐	Device isolated from the network	
☐	Sessions, tokens, and credentials revoked	
☐	Evidence collected before wipe	
☐	Device rebuilt from known-good image	
☐	Data exposure and breach assessment documented	

Audit Evidence List

Control	Evidence to keep
Endpoint inventory	Current list of in-scope endpoints with owner and status
Disk encryption	Console or system report showing encryption per device
Malware protection and EDR	Deployment report, last check-in dates, alert triage records
Administrator rights	List of users with admin rights, elevation and exception records
Removable media	Setting evidence or log of approved devices
Compromised endpoint response	Incident tickets or tabletop test record
Policy governance	Approved policy with version, acknowledgments, and review date

Framework Mapping Guide

Framework	Where it applies	What it expects	Sections above
SOC 2	CC6.1, CC6.7, CC6.8, CC7.2	Logical access, restricted movement of information, prevention and detection of malicious software, monitoring	3, 4, 5, 6, 8
ISO 27001:2022	Annex A 8.1, 8.7, 8.9 (also 8.19, 7.7, 7.10)	User endpoint devices, malware protection, configuration management, software installation, clear screen, storage media	3, 4, 5, 6, 7
HIPAA	45 CFR 164.310(b), 164.310(c), 164.308(a)(5)(ii) (B), 164.312(a)(2)(iv)	Workstation use and security; protection from malicious software (addressable); encryption of ePHI (addressable)	3, 4, 9
PCI DSS 4.0.1	Requirements 5.2.1, 5.3.1, 1.5.1	Anti-malware on in-scope components, kept current by automatic updates; security controls on computing devices	3, 4
GDPR	Article 32	Appropriate technical measures to secure personal data	3, 4, 9
CIS Controls v8	Safeguards 10.1, 4.3, 3.6	Anti-malware software, automatic session locking, encryption on end-user devices	3, 4

Endpoint Security Policy Template | ComplyJet | complyjet.com. A starting point, not legal advice. Review with your own counsel and auditor.