

# Configuration Management Policy

---

## Purpose

Unmanaged or inconsistently configured systems are one of the most common paths to compromise. This policy defines how Your Organization establishes, documents, hardens, and maintains secure baseline configurations for its information systems, and how changes to those baselines are controlled over the system lifecycle.

## Scope

This policy applies to all Your Organization information systems that store, process, or transmit company or customer data, including servers, endpoints, network devices, containers, cloud infrastructure, and the software images and templates used to provision them. It applies to IT Operations, Engineering, and any workforce member who provisions or administers infrastructure.

## Baseline configurations

- Every system class (server role, container image, endpoint image, network device type) has a documented, version-controlled baseline configuration before it is deployed to production.
- Baselines are built from Your Organization-approved hardening standards (e.g., CIS Benchmarks or vendor security guides), adapted to the system's function.
- Baseline configurations are stored under version control alongside a record of who approved them and when.
- Deviations from baseline must be documented, justified, and tracked as a formal exception.

## Least functionality

- Systems are configured to provide only the capabilities required for their intended function. Unnecessary services, ports, protocols, and software are disabled or removed prior to deployment.
- Your Organization maintains an allow-list approach for software and network services on systems that process sensitive or regulated data — nonessential functionality is denied by default.
- Application execution on managed endpoints and servers is restricted to an approved software list; unauthorized software installation is blocked or flagged for review.

## Configuration enforcement and drift detection

- Automated configuration management tooling (e.g., infrastructure-as-code, endpoint management, container image scanning) enforces baselines and detects drift.
- Configuration drift is reviewed on a regular cadence; unauthorized deviations are remediated or formally exempted within a defined window.

- Golden images and infrastructure-as-code templates are rebuilt and re-validated against current hardening standards at least annually or upon a material vulnerability disclosure affecting the base image.

## Change control for configuration

- Changes to baseline configurations follow the Your Organization Change Management Policy, including security impact analysis prior to approval.
- Access to modify production baseline configurations and infrastructure-as-code repositories is restricted to authorized personnel and logged.
- Emergency configuration changes made outside normal change control must be documented and retroactively reviewed within one business day.

## User-installed software

Workforce members do not have standing local administrator rights on managed endpoints unless their role requires it and the exception is approved. Where elevated rights are granted, installed software is periodically audited against the approved software list.

## Roles and responsibilities

- **IT and Security Operations.** Own the baseline hardening standards, configuration management tooling, and drift remediation process.
- **Engineering.** Owns infrastructure-as-code templates and container/VM images for the services they build, and keeps them aligned to current baselines.
- **System Owners.** Approve deviations from baseline for their systems and ensure compensating controls are in place.

## Review cadence

This policy and the underlying baseline standards are reviewed annually by IT Operations and Information Security, or sooner following a significant platform change or a vulnerability disclosure affecting a widely deployed baseline.

*Effective date: [the date this policy takes effect]*