Operating System and Infrastructure Policies

This policy outlines the organization's approach to securing all operating systems (OS) and underlying infrastructure components by reducing the attack surface, implementing secure configurations, and maintaining a high level of security assurance.

1. Scope and Policy Objectives

This policy applies to **all information system components**, including but not limited to:

- Servers (physical and virtual, on-premise and cloud-hosted)
- Network devices (routers, switches, firewalls, load balancers)
- Workstations and end-user devices
- Operating Systems (Windows, Linux, macOS, mobile OS)
- Middleware, firmwares, and virtual machine hosts (hypervisors)

The primary objective is to move all systems from their default vendor configurations to a secure "hardened" state that minimizes vulnerabilities and reduces the potential attack surface.

2. Hardening Standards and Baseline Configuration

2.1. Establishing a Secure Baseline

1. **Mandatory Baselines:** All systems and infrastructure components must be deployed using an **IT-approved Secure Baseline Configuration Standard**. This standard is based on industry-recognized frameworks, such as the Center for Internet Security (CIS) Benchmarks or specific vendor/regulatory security guides (e.g., NIST, Microsoft Security Baselines).
2. **Image Management:** Secure, hardened installation images or templates (e.g., virtual machine images, cloud formation templates) must be created and used for

all new deployments to ensure consistency and compliance. These images must be stored securely with restricted access.

3. **No Default Credentials:** The use of default vendor passwords, user accounts, or configurations is strictly **prohibited**. All default credentials must be changed or disabled during the initial build process.

2.2. Operating System (OS) Hardening Requirements

Area	Requirement
Component Removal	All unnecessary software, drivers, services, protocols, and libraries that are not essential for the system's primary function must be uninstalled or permanently disabled to minimize the attack surface.
Patch Management	The OS must be kept up-to-date with all security patches and firmware updates according to the organization's **Patch Management Policy**.
File System Security	Secure permissions must be enforced on all critical system files and directories, adhering to the **Principle of Least Privilege**.
Local Storage Encryption	Full disk encryption (FDE) must be enabled on all workstations and servers storing sensitive data, including local boot volumes.
Account Management	Guest accounts must be disabled. Only necessary local user accounts are permitted, and default administrator accounts must be renamed or disabled where practical.
System Boot Security	Secure Boot must be enabled on all compatible hardware to prevent unauthorized code execution during the boot process.

2.3. Infrastructure and Network Hardening Requirements

Area	Requirement
Firewall Configuration	Host-based and network firewalls must be configured to deny all traffic by default and only explicitly permit necessary ports, protocols, and services. All open ports must be documented and justified.

Area	Requirement
Network Segmentation	Critical systems and sensitive data networks must be logically or physically separated (segmented) from general-purpose networks and the internet.
Remote Access	Remote administrative access must be restricted to a limited set of administrative hosts or a secure jump server/VPN connection. Unsecured remote management protocols (e.g., Telnet, FTP) are **prohibited**.
Device Firmware	Firmware (including BIOS/UEFI) on all servers and network devices must be regularly updated and protected with strong passwords.
Log Management	System, application, and security logs must be configured to capture sufficient detail and be sent immediately to a central, protected Log Management/SIEM system, ensuring that logs cannot be tampered with locally.

---

3. Maintenance and Assurance

3.1. Ongoing Compliance and Change Control

1. **Configuration Management:** All systems must maintain a record of their hardened state. Any deviation from the approved baseline configuration must be identified, documented, and remediated immediately.
2. **Change Management:** Any changes to the hardened configuration or deployment baselines must follow the **Change Management Process**, including testing in a non-production environment, review by system owners, and formal authorization.
3. **Re-Hardening:** Systems that are found to be non-compliant with the secure baseline must be remediated (re-hardened) as a high-priority security action.

3.2. Verification and Audit

1. **Vulnerability Scanning: Authenticated vulnerability scans** must be performed regularly (at least monthly) against all systems to identify any missing patches, configuration drift, or new vulnerabilities. Critical findings must be remediated per the Patch Management Policy timescales.

2. **Periodic Audits:** Compliance with this hardening policy must be formally audited and documented **at least annually** by the Security team or an independent party.
3. **Review:** This Operating System and Infrastructure Hardening Policy will be reviewed and updated **at least annually** to align with evolving threats and industry best practices.