

Maintenance Policy

Purpose

Routine and emergency maintenance touches the same systems that everyday security controls protect — patching, hardware servicing, diagnostics, and vendor support sessions all require privileged access and can bypass normal safeguards if not controlled. This policy defines how Your Organization performs and controls system maintenance so that maintenance activity itself does not become a security gap.

Scope

This policy applies to all maintenance activity — routine, preventive, and corrective — performed on Your Organization information systems, servers, network equipment, and endpoints, whether performed by internal staff, vendors, or manufacturer support personnel, on-site or remote.

Scheduled maintenance

- Routine maintenance (patching windows, hardware servicing, firmware updates) is scheduled through the Your Organization change management process, with advance notice to affected system owners and, where user-facing impact is expected, to end users.
- Maintenance windows are logged, including scope, systems affected, personnel involved, and outcome.

Maintenance tools

- Diagnostic and maintenance tools brought onto Your Organization systems or networks must be approved in advance and inspected for malicious code before use, where practical.
- Media used for maintenance and diagnostics (USB drives, install media) is scanned for malware and, if it has left Your Organization's control, is checked before reconnection.

Remote maintenance

- Remote maintenance sessions — including vendor and manufacturer remote support — require strong authentication (MFA) and are established through an approved, monitored access channel rather than direct exposure of management interfaces to the internet.
- Remote maintenance sessions are logged, and session recordings or logs are retained consistent with the Data Retention Policy.
- Remote access credentials for maintenance are disabled by default and enabled only for the duration of an approved session.

Maintenance personnel

- Only authorized personnel — internal staff with a documented role or vendor personnel under an active support agreement — may perform maintenance on Your Organization systems.
- Non-organizational maintenance personnel working on-site are escorted or supervised while accessing systems that store or process Confidential or Restricted data, consistent with the Physical Security and Environmental Protection Policy.
- Vendor and third-party maintenance personnel are subject to the applicable terms of the Vendor Risk Management Policy, including confidentiality obligations.

Equipment sanitization

Equipment leaving Your Organization custody for off-site maintenance or repair is sanitized of Confidential or Restricted data beforehand where feasible; where not feasible (e.g., hardware failure preventing wipe), the repair is performed under an agreement that obligates the vendor to appropriate handling, or the equipment is scheduled for destruction rather than repair.

Post-maintenance verification

After maintenance affecting security-relevant configuration, the system is verified against its baseline configuration (see the Configuration Management Policy) before being returned to production use.

Roles and responsibilities

- **IT Operations.** Schedules and performs routine maintenance, approves maintenance tools, and maintains maintenance logs.
- **System Owners.** Approve maintenance windows for their systems and verify post-maintenance functionality.
- **Information Security.** Reviews remote maintenance access controls and investigates anomalous maintenance activity.

Review cadence

This policy is reviewed annually by IT Operations and Information Security, or sooner following a maintenance-related security incident.

Effective date: [the date this policy takes effect]