

System and Information Integrity Policy

Purpose

This policy sets how Your Organization finds and fixes system flaws, protects against malicious code, tracks security alerts, and monitors systems for attacks and unauthorized use. It covers the System and Information Integrity requirements of NIST SP 800-171: practices 3.14.1 to 3.14.7 of Revision 2, as used by CMMC Level 2, and requirements 03.14.01, 03.14.02, 03.14.03 and 03.14.06 of Revision 3. It also supports the matching controls in other frameworks.

Scope

This policy applies to all Your Organization information systems, including servers, workstations, network devices, cloud services, and applications, with particular attention to systems that store, process, or transmit Controlled Unclassified Information (CUI) or other sensitive data, and to the people who administer them.

Roles and responsibilities

- **IT and system administrators** apply patches, run protection tools, and respond to alerts.
- **The security team** owns the standards, subscribes to advisories, reviews monitoring output, and reports on compliance.
- **System owners** accept the schedule and any exception for their systems.

Requirements

1. Flaw identification and remediation (3.14.1)

- All systems are scanned for missing patches and known vulnerabilities at least monthly, and after significant changes.
- Fixes are tested and applied on a risk basis, within the remediation windows set in the Risk Assessment and Vulnerability Management Policy, and sooner for flaws that are actively exploited. Vendors' end-of-life software is replaced or isolated.
- Flaws that cannot be fixed within the target are recorded with compensating controls and an owner in the plan of action and milestones or the risk register.

2. Malicious code protection (3.14.2, 3.14.4, 3.14.5)

- Endpoint protection (antivirus or endpoint detection and response) is installed on all workstations and servers where the platform supports it, and cannot be disabled by users.
- Protection tools update their signatures and engines automatically, at least daily, and updates are verified through console reporting.

- Systems are scanned on a schedule, and files from external sources (downloads, email attachments, removable media) are scanned as they are opened, downloaded, or executed.
- Email and web gateways filter known malicious content.
- Detections are triaged and handled under the Incident Response Plan.

3. Security alerts and advisories (3.14.3)

- The security team subscribes to advisories relevant to the Your Organization technology stack, including vendor bulletins and national alert sources.
- Advisories are assessed for applicability within one business day of receipt for critical items. Actions taken are recorded.
- Relevant advisories are shared with the people who run the affected systems.

4. System monitoring (3.14.6, 3.14.7)

- Inbound and outbound communications are monitored at the network boundary and at key internal points using firewalls, intrusion detection or prevention, or equivalent cloud controls.
- Logs from servers, endpoints, identity systems, and network devices are collected centrally under the Audit and Accountability Policy, and alert rules identify attacks, indicators of compromise, and unusual access or data movement.
- Monitoring identifies unauthorized use of systems, such as logins from unexpected locations, use of disabled accounts, privilege escalation, and unapproved software or devices.
- Alerts are reviewed on a defined schedule, and high-severity alerts are triaged within the time stated in the Incident Response Plan.

5. Reporting and metrics

The security team reports patch compliance, protection coverage, advisory handling, and alert handling to management at least quarterly, and raises exceptions for overdue items.

Exceptions

Exceptions are requested in writing with the system, the reason, the compensating controls, and an expiry date, and are approved by the security team and the system owner.

Enforcement

Staff who disable protections or ignore required updates may face disciplinary action in line with the Acceptable Use Policy.

Evidence

Evidence of operation includes vulnerability scan reports, patch management records, endpoint protection console reports, advisory tracking records, monitoring configuration and alert logs, and the plan of action and milestones.

Review cadence

This policy is reviewed annually by the security team, or sooner after a significant incident or a change in the applicable requirements.

Effective date: [the date this policy takes effect]