PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity
NIST Special Publication 800-53 Revision 5

1. This policy is applicable to all departments and users of IT resources and assets.
    a. Identify, report, and correct information system flaws.
    b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
    c. Install security-relevant software and firmware updates within 3 days of the release of the updates.
    d. Incorporate flaw remediation into the configuration management process.
    e. Employ automated mechanisms weekly to determine the state of information system components about flaw remediation.

Violations: Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.

Attachments: None

Related Policies:

This project was funded by a National Centers of Academic Excellence in Cybersecurity grant (H98230-21-1-0318), which is part of the National Security Agency.