



OIT 62.403: IT System Hardening

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy:
Approved-On Date: 4/19/2011
Effective Date: 7/1/2011
Revision Date: 4/11/2011

I. Policy Statement

IT System Hardening defines the steps necessary to provide adequate and effective protection for University systems.

II. Purpose

The IT System Hardening policy delineates technical security controls to protect IT systems against security vulnerabilities.

III. Scope

This policy applies to all Commonwealth of Virginia (COV) systems and to the University IT network infrastructure.

IV. Requirements

NSU shall or shall require that its service provider:

1. Identify, document, and apply appropriate baseline security configurations to all agency IT systems, regardless of their sensitivity.
2. Identify, document, and apply more restrictive security configurations for sensitive agency IT systems, as necessary.

Note: The University may develop University-specific baseline security configuration standards or may elect to use baseline security configuration standards that are publicly available, such as those developed by the Center for Internet Security (www.cisecurity.org).

3. Maintain records that document the application of baseline security configurations.
4. Monitor systems for security baselines and policy compliance.

5. Review and revise all security configuration standards annually, or more frequently, as needed.

Note: The University should establish a process to review applicable security notifications issued by equipment manufacturers, bulletin boards, security-related web sites, and other security venues, and establish a process to update security baseline configuration standards based on those notifications.

6. Reapply all security configurations to agency IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.
7. Require periodic operating system level vulnerability scanning of sensitive IT systems in a frequency commensurate with sensitivity and risk, to assess whether security configurations are in place and if they are functioning effectively.
8. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.
9. Apply all software publisher security updates to the associated software products.
10. All security updates must be applied as soon as possible after appropriate testing, not to exceed 90 days for implementation.
11. Prohibit the use of software products that the software publisher has designated as End-of-Life (i.e., software publisher no longer provides security patches for the software product).

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.

