SECURITY BEST PRACTICES – SYSTEM AMDIN.
CATS - INFORMATION TECHNOLOGY

VERSION HISTORY

Version	Date	Author Name	Reason for Revision
1.2.1	01-08-2009	Mike Natale	Initial Publication - DRAFT
1.2.2	07-02-2010	Mike Natale	Annual Review/minor revisions
1.2.2	10-4-2011	Michael Persina	Annual Review – No Changes
1.2.2	04-09-2014	Ken Nelson	Annual Review
1.2.3	06-29-2015	Mike Natale	Fixed broken links
1.2.3	09-6-2016	Mike Natale	Annual Review
1.2.3	10-24-2017	Mike Natale	Annual Review
1.2.3	02-01-2019	Mike Natale	Annual Review
1.2.4	02-20-2020	John Remley	Annual Review and Minor Revisions
1.2.4	9-21-2021	John Remley	Annual Review and Fixed Link
1.2.4	4-21-2022	Mike Natale	Annual Review

	Wright State University Information Security	

Controls	
Policy Title:	Security Best Practices – System Administration
Category:	Information Technology
Audience:	WSU Staff
Reason for Revision:	*N/A*
Created / Modified Date:	01-08-09
Location:	http://www.wright.edu/security/policy/

Responsible Parties	
Author	Mike Natale
Technical Reviewer	John Remley

TABLE OF CONTENTS

Security Best Practices – System Administration

1. Document and understand the system, application, and technical environment for which you are responsible. Without proper documentation it is not possible to properly assess security requirements.
    a. An example of technical information that should be documented
        i. Server name and IP address
        ii. The operating system
        iii. Hardware Vendor
        iv. Purpose
        v. Services running
        vi. Application software
        vii. Data classification and security requirements

2. Utilize Security and Analysis tools or base line security tools
    a. Run the Windows Security Configuration and Analysis tool using the security template for the role the server will play, i.e., Domain Controller you would use securedc.inf.
    b. In lieu of baseline analyzers, or other security tools, utilize baseline reference documents such as those provided at Center for Internet Security - www.cisecurity.org.
    c. CaTS also maintains security baselines for several supported operating system types that should be considered/applied.

3. Apply vendor-supplied fixes necessary to repair security vulnerabilities

4. Request that the *Information Security* department scan the system for security vulnerabilities using available technical tools.
    a. When new servers are deployed
    b. After a significant upgrade is performed to the operating system
    c. After significant upgrade is performed to the application

5. Repairing discovered vulnerabilities
    a. Vulnerabilities should be patched as soon as possible, i.e., the first available maintenance window.
    b. In situations where applying patches are a concern to production systems, then patches should be applied to a test environment as soon as possible to eliminate these concerns. After testing has been completed, patches should then be applied to the production environment. Serious vulnerabilities may require putting mitigating controls in place during the testing phase.

    Vulnerabilities that cannot be repaired due to compatibility issues affecting the stability of the system must have mitigating controls put in place (network access controls or system level controls for example). Such vulnerabilities and the measures taken to mitigate them should be documented.

6. Install and maintain anti-virus software when available for a given operating system
    a. Update virus definitions on a daily basis or schedule daily automatic updates

7. Remove unneeded services and software

8. Stay abreast of technology security issues affecting Operating Systems and Application software for which you have responsibility

9. Follow adequate access control methods
    a. Limit access to only authorized persons
    b. Assign accounts only to individuals – no group accounts
    c. Use different passwords for privileged accounts, such as root and administrator, on different systems being maintained by the same individual

   d. Whenever possible work as a non-privileged user. Use privileged accounts for tasks that require elevated capabilities

10. Follow adequate procedures for user passwords
    a. Reference Password Management Policy:

11. Maintain adequate system logs. Where possible:
    a. Audit successful logins, including the location from which the logins originated.
    b. Audit and Alert unsuccessful logins, including the location from which the attempts originated.
    c. Audit unsuccessful file accesses.
    d. Audit the use of administrative privileges with operating system settings or tools such as sudo.
    e. Ensure that all logs are routinely backed up.
    f. Keep logs for a minimum of 30 days, unless otherwise required by compliance standards or regulation.
    g. Consider sending logs to a central logging server. Contact CaTS for additional information.

12. Limit access to IT resources to local network addresses where possible

13. Provide technicians adequate time and resources to allow them to secure IT resources

14. Immediately report any successful or attempted security breach at the following site: http://www.wright.edu/security/incident/