Security Best Practices –
System Administration
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.

1. An example of technical information that should be documented:
   a. Server name and IP address
   b. The operating system
   c. Hardware Vendor
   d. Purpose
   e. Services running
   f. Application software
   g. Data classification and security requirements

2. Utilize Security and Analysis tools or baseline 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, i.e. NexPose
   a. When new servers are deployed
   b. After a significant upgrade is performed to the operating system
   c. After a 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
10. Follow adequate procedures for user passwords
   a. Reference the 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/