PURPOSE

The purpose of the UW-Madison IT Security Baseline for Research and Academic Computing is to accommodate research organizations that have unique computing requirements that do not fit into the campus standard IT security baseline requirements.

The UW-Madison IT Security Baseline for Research and Academic Computing is intended to inform research organizations of the necessary actions required to ensure that organizations have an IT security plan that reduces the risk of unauthorized access to IT resources and sensitive data. These requirements are intended to create a minimally acceptable security standard for research heavy centers and organizations on campus. UW-Madison IT Security will work with information technology units to implement a common set of IT practices that report results through centrally monitored mechanisms and accomplish the following goals.

- Implement a common set of tools, processes, and procedures to reduce the risk of unauthorized access to information systems.
- Implement a common set of procedures so that intrusions are quickly detected and appropriate personnel are alerted in a timely manner.
- Monitor and verify security metrics to ensure units are operating at the minimally acceptable security baseline.

This baseline will not ensure compliance with any particular federal or industry security standard (e.g., PCI-DSS, HIPAA, FERPA, FISMA) and may not meet the expectations of any particular grant requirements.

A. POLICY AND AWARENESS

1. Each organization should assign a departmental security contact within AANTS to:
   a. Be responsible for departmental IT security
   b. Act as point of contact with UW-Madison IT Security
   c. Monitor and review log information in the UW-Madison IT Security SEM.

2. The UW-Madison Information Incident Reporting and Response policy (http://www.cio.wisc.edu/IReportPolicy.pdf) and procedure must be followed to ensure timely and effective handling of all breach situations.

3. The UW-Madison Electronic Devices policy (http://www.cio.wisc.edu/devices.pdf) must be adhered to at all times.

4. Media or devices that may contain sensitive information must be adequately obfuscated, erased, destroyed or otherwise rendered unusable before disposal or reuse for another purpose per the UW-Madison Media and Device Disposal and Reuse Policy (http://www.cio.wisc.edu/IDisposePolicy.pdf).

5. The UW-Madison Responsible Use of Information Technology Policy (http://www.cio.wisc.edu/policies-responsibleuse.aspx) must be adhered to at all times.

6. All server and workstation images should be audited using a formal security or hardening guide.
   a. UW-Madison IT Security recommends using the Center for Internet Security compliance assessment tool. The Center for Internet Security templates can be used as a baseline for comparing the department’s operating system security settings to a set of federal security standards and provide a report. http://www.cisecurity.org/

B. DATA CLASSIFICATION AND PROTECTION

1. Systems that handle restricted data must be designated as such and protected at a higher level than defined by the IT Security Baseline. Please consult with UW-Madison IT Security for implementing increased security controls.

2. Organizations should understand the types of data being stored, processed, and transmitted on their systems.
a. UW-Madison IT Security recommends using Identity Finder to discover unknown data types and take action with the data.
   i. Identity Finder should be installed and run on servers and workstations that store, process, or transmit with University data.
   ii. Servers and workstations should be scanned every 30-calendar days for restricted data.
   iii. Identity Finder should be configured to check for updates daily.
   iv. Identity Finder should be configured to report centrally.
   b. The departmental security contact should review identity finder results and follow-up on exceptions.

3. Draft a departmental Terms of Service for using computing resources that state specifically what types of data may be stored, processed, or transmitted by the system.
   a. Explicitly state what data types may not be stored, processed, or transmitted by the system.
   b. Users should agree to the Terms of Service prior to access being granted to computing resources.
   c. The Terms of Service should be reviewed and approved by organizational leadership annually.

C. NETWORK SECURITY
1. Protect networked devices with firewall(s) where possible
   a. It is recommended administrators who manage campus firewalls successfully complete the DoIT firewall training class or equivalent. (http://www.doit.wisc.edu/training/pte/class.aspx?class=7260)
   b. Firewalls must restrict inbound connections to systems of interest.
   c. Firewalls send logs to the UW-Madison IT Security, security event management (SEM) system.
   d. Firewall rule changes must be documented and tracked.
2. Networks which are unable to utilize network firewalls should apply the following compensating controls
   a. Apply a 24 hour patch cycle on all exposed systems
   b. Apply switch and/or router level Access Control Lists
   c. Increased network monitoring utilizing network flows, intrusion detection, and Bro IDS
   d. Implement Instrumented SSHD used to monitor user sessions for unauthorized access based on keywords entered into the session
   e. Implement private networking space for compute cluster nodes

3. The departmental security contact is responsible for ensuring firewall rules are audited annually.
4. The departmental security contact is responsible for ensuring external vulnerability scans against network resources are performed every six months.
   a. Results must be reviewed by the departmental security contact.
   b. Vulnerabilities should be remediated within 30 calendar days.
5. The departmental security contact is responsible for ensuring internal vulnerability scans against network resources are performed every six months.
   a. Results must be reviewed by the departmental security contact.
   b. Vulnerabilities should be remediated within 30 calendar days.
6. The departmental security contact must monitor and respond to alerts received from the UW-Madison IT Security Event Monitoring system or the UW-Madison IT Security border Intrusion Detection Systems.

D. PROTECTING SERVERS AND WORKSTATIONS
1. Servers and workstations should be managed using an endpoint management suite (e.g., Microsoft SCCM, Altiris, Puppet or TEM).
2. Servers and workstations should run a community or vendor supported operating system.
3. Operating systems should have critical and security patches applied within 30 calendar days of release.
4. Critical and security patches for all applications should be installed within 30 calendar days of release.
a. UW-Madison IT Security recommends Secunia: Corporate Software Inspector is installed on supported servers, and report results centrally.

b. Production applications should be either vendor or community supported, and end-of-life applications with known vulnerabilities should be removed.

c. The departmental security contact should monitor and review security patching processes and results.

5. All servers and workstations should run an antivirus protection tool (e.g., Symantec Endpoint Protection, Microsoft Forefront managed by SCCM, ClamAV), the tool should be capable of:
   a. Performing daily lightweight scans
   b. Performing full weekly scans
   c. Reporting results to a central console
   d. Notifying IT staff if malware is found.
   e. The departmental security contact should review alerts and ensure remediation of malicious content within three business days.

6. Servers or workstations that cannot run an antivirus protection tool should
   a. Run an antivirus protection tool only on exposed services, such as submit nodes or public disk storage
   b. Utilize a central syslog to collect antivirus activity and report the logs to a SEM system
   c. Implement private networking space for compute nodes which cannot run antivirus

7. Disable all unnecessary services before a server goes online.

8. Servers hosting email services must not provide open relay services.

9. Host-based firewalls should be installed on all servers.
   a. Host-based firewalls should restrict inbound connections to ports of interest.
   b. Host-based firewalls should send logs to the UW-Madison IT Security SEM.
   c. The departmental security contact must review rules and exceptions annually.

10. Configure access logs, security logs, DHCP logs, DNS logs, and firewall logs to report to the UW-Madison IT Security SEM.
    a. Set up a central syslog service onsite
    b. Send appropriate logs to a SEM

E. APPLICATION DEVELOPMENT SECURITY

1. An inventory of all custom developed applications in production should be maintained
2. An Inventory of all databases in production should be maintained
3. Web logs, access logs, and security logs should be reported to the UW-Madison IT Security SEM.
4. Require SSL for all sensitive pages. Non-SSL request to these pages should be redirected to the SSL page.
5. Ensure your certificate is valid, not expired, not revoked, and matches all domains used by the site.
6. An inventory of active certificates should be maintained.
7. A code repository is recommended for tracking changes and keeping backups.
8. IBM AppScan can be used to scan custom applications using the Open Web Application Security Project Top 10 as a template.  https://www.owasp.org/index.php/Main_Page
9. Vulnerability scans of applications in development should take place prior to an application moving to production.
10. Vulnerability scans of applications in production should take place every six months.
11. Vulnerabilities identified as OWASP Top Ten should be remediated as soon as possible.
12. Production Databases should be scanned every six months using the MacAfee Vulnerability Manager for Databases
13. Scans of database services in development should take place prior to an application moving to production.
F. ACCESS CONTROL
1. All passwords must conform to the campus minimum password standards. (see: http://www.cio.wisc.edu/policies-password.aspx)
2. Verify user’s identities before performing password resets or implement a reliable self-service password reset option.
3. A process must be in place to deactivate user accounts under emergency circumstances such as termination, compromise, or infection.
4. Inactive user accounts are disabled after a reasonable amount of time determined by the organization.
5. User ID’s are locked out for X minutes after X invalid authentication attempts, UW-Madison IT Security recommends 15 minutes after 6 invalid authentication attempts.
6. Users should not have local administrative privileges unless an exception is made by the department head, documented and reviewed annually.
7. Administrative account passwords (e.g., root or enterprise domain admin accounts) should be stored in a secure repository.
8. All desktop workstations should initiate a screen lock after X minutes of inactivity; it is recommended servers initiate a screen lock after X minutes of inactivity where possible, UW-Madison IT Security recommends 15 minutes.
9. Privileged access to administrative systems should be documented and reviewed annually.
10. Access to computing, printing, or datacenter resources by vendors should be approved and monitored.
11. Service accounts should be used for internal application and database operations.
12. Secure administrative interfaces for applications and devices.
   a. Default passwords must be changed upon first usage.
   b. Deny access to administrative interfaces from the public Internet unless encrypted.
13. System Administrators should not use Administrative accounts for general purpose computing.
14. First-time passwords are set to a unique value for each user, and must be immediately changed upon first use if assigned by a person.
15. Reset passwords should be set to a unique value for each user, and immediately changed upon first use if assigned by a person.

G. PHYSICAL SECURITY
1. System backup media should be stored in a secure location or encrypted.
2. Access to network jacks in public areas should require authentication.
3. Servers should be kept in a locked room.

H. SUPPORTING PROCESS DOCUMENTATION
1. Identify a departmental security contact.
2. Document and maintain an inventory process for tracking additions and removal of IT assets including servers, workstations, printers, firewalls, and other network devices.
3. Document and maintain a change management process for tracking changes to IT assets.
5. Document and maintain patch management strategies for custom applications where applicable.
6. Document and maintain a backup media storage and disposal processes.
8. Document and maintain processes for maintaining and updating continuity of operations plans.