SECURITY STANDARDS FOR INFORMATION SYSTEMS

I. Purpose
As established by the USG IT Handbook section 5.6, the level of security controls implemented on a system should be relative and proportionate to the level of risk associated with that system. This level of risk may be attributed to factors such as network topology, services and resources offered, type of information managed, and government mandated privacy protection policies including, but not limited to, HIPAA, PCI-DSS, and FERPA.

II. Policy Statement
This policy applies to all university systems and provides functional guidelines for the configuration and use of those systems.

III. Definitions
System - a combination of the hardware, operating system, network service, application software, and network connection.

University system - a system connected to the campus network.

IV. Exclusions
Exceptions to the above standards may be granted on an as needed basis with written approval from the Office of Information Security.

V. Procedures
A. System Standards
A system can include, but is not restricted to the following:
- A client-server architecture;
- The ability to manage files, services and other networked resources;
- Providing to authorized clients access to files, services and other networked resources;
• The ability to process multiple connections and requests using hardware or software-based virtualization technology.

This standard applies to all University systems as defined above, including those residing on personally owned hardware.

B. Risk Categories
The campus has established a three-tier server classification system (Confidential, Sensitive and Unrestricted) to assist system owners and technical staff in implementing the level of protection.

The levels of protected information are defined in the “Data Stewardship and Classification Standard” document.

The campus has identified specific controls that are appropriate for each system risk category. The controls entail configuration and procedural practices aimed at protecting the systems and minimizing the risk of unauthorized information exposure or modification and maximizing the availability of the resources.

These controls are the minimum required for the given risk level; system owners and technical staff are encouraged to supplement these as appropriate. Any exceptions to the implementation of these controls must be approved by the CISO.

Class III – Systems Holding Unrestricted Data
The following list details the minimum set of requirements and controls for low risk category systems:
• Servers must be registered in the inventory list with appropriate personnel assigned for system administrator and system owner roles.
• The system must run a legally licensed and supported version of an operating system.
• Servers must be scanned every 90 days and vulnerabilities mitigated.
• Access logs for the systems must be logged and maintained for a minimum of 90 days.
• Servers must use a static IP address assigned by Network Services.
• Systems should only have border firewall exceptions for ports that are required for the core functions of that system.
• Servers and applications should offer only essential network and operating system services.
• Server operating system and application software must be kept up to date.
• Administrative access to systems must be restricted and documented as established in IT Policies.
• Permissions must ensure that users can access only the services and information for which they are authorized.
• System passwords must meet or exceed the University password standards.
• Inactive accounts with administrative access must be disabled within 3 business days.
• Servers should not reboot automatically in case of a failure.
• Servers must be physically or logically located in an access-controlled environment to prevent unauthorized access.
• Servers must have anti-malware protection software installed and maintained.
• Linux servers must have a file integrity checker.
• All devices must run host-based firewalls where available.
• Firewall/TCP wrapper rule sets must allow access to only those ports which are necessary. All rule sets must be set to default deny configuration.
• Systems requiring remote access for vendor support should allow for access to the system via campus VPN.
• Multi-factor authentication must be used.

Class II – Systems Holding Sensitive Data
In addition to the requirements for Class III data, the following are required:
• Systems must be protected by appropriate physical, logical and environmental controls to prevent unauthorized changes.
• Systems must have a documented log review process.
• Systems must have a documented plan for regular data backup.
• Systems should have a current, documented disaster recovery plan.
• Data backups should be physically separated from production data.
• Systems must have a documented change management plan.

Class I – Systems Holding Confidential Data
In addition to Class II, the following are required:
• Systems should employ redundant resources.
• Systems should have a documented incident response plan.
• Systems must have documented access controls.
• Systems must use current secure protocols.
• Must use encryption for all data except where mitigation controls are approved.

Related Documents
Information Technology Appropriate Use Policy
Data Stewardship and Classification Standard