Security Standards for Information Systems

Area: Information Technology Services	Number: IT-3610-00
Subject: Information Systems Management	Issued: 8/1/2012
Applies To: University	Revised: 4/1/2015
Sources:	Updated: 4/1/2015
	Reviewed: 4/1/2015
Responsible Party: Vice President for Information Technology	Page(s): Page **1** of 5

I. Purpose

The CIO, as established by the Board of Regents Policy 11 and USG IT Handbook section 5.6.3, directs that 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 multiple 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

1) System Definition
   For the purpose of the following System Security Baseline Standards, the definition of a System is a combination of the hardware, operating system, network service, application software, and network connection. A system is a University System when it is connected to the campus network by any means and associate server uses an approved Georgia Southern University IP address.

   A system can include, but is not necessarily restricted to the following:

   i. A client-server architecture;
   ii. has the ability to manage files, services and other networked resources;
   iii. Provides authorized clients with access to files, services and other networked resources;
   iv. is operationally bound to the applications it hosts;
   v. has the ability to handle multiple connections and requests;
   vi. May use hardware or software based virtualization technology.

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

2) Risk Categories

The campus has devised a three tier server classification system (high, medium and low risk categories) to assist system owners and technical staff in implementing the level of protection required for their systems. The characteristics of systems belonging to each tier are given in the following table:

Server Risk Category	High	Medium	Low
Description of System Characteristics	1.Contains Protected Class I Information and/or 2.Provides enterprise wide services and/or 3. Has high availability requirements.	1.Contain Protected Class II Information and/or 2.Provides administrative services and/or 3. Has medium or varied availability requirements.	1.Contains no Protected Level Information and/or 2.Has low availability requirements

The levels of protected information are defined in the "Data Classification Standards" 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 CIO.

3) Low Risk Category Systems

The following list details the minimum set of requirements and controls for low risk category systems:

i. Servers must be registered in the server registry site with appropriate personnel assigned for system administrator and system owner roles. This site is maintained by the CISO;
ii. The system must run a legally licensed version of an operating system that supports appropriate Internet communication protocols;
iii. Servers must be scanned every 90 days and vulnerabilities mitigated (see IT System Scanning Procedure);
iv. Servers must use a static IP address assigned by Network Services;
v. Systems should only have border firewall exceptions for ports that are required for the core functions of that system;
vi. Servers and applications should offer only essential network and operating system services;

vii. Server operating system and application software must be kept up to date;
viii. Administrative access to systems must be restricted and documented;
ix. Permissions must ensure that authorized users can access only the services and information for which they are authorized;
x. System passwords must meet or exceed the University password standards;
xi. Inactive accounts with administrative access must be disabled immediately;
xii. Servers are to be configured to not reboot automatically in the case of a failure;
xiii. Systems on which vulnerabilities have been exploited and are a risk to the campus (and beyond) may be physically removed by the Information Security Office for purposes of conducting forensic analysis;
xiv. Servers must be physically located in an access-controlled environment to prevent unauthorized access to equipment.
xv. Physical access must only be granted to authorized individuals and accompanied service personnel.
xvi. Servers must have virus protection software installed and maintained current and an active scanning schedule. Linux servers must have some form of file integrity checker.
xvii. All server operating systems for which there are commercial or publicly available host based firewalls (e.g. ipfilters, iptables, Windows Advanced Firewall, etc.) must run these firewalls or appropriate TCP wrappers.
xviii. Firewall/TCP wrapper rule sets must allow access to only those ports which are necessary to provide service and to maintain the servers. All rule sets must be in 'default deny' configuration.
xix. Systems that require remote access for vendor support or administration must allow for a vendor account and access to the server through the campus VPN (see Remote Access Standards document).

4) Medium Risk Category Systems

i. The following list details the minimum set of controls and requirements for medium risk category systems. All controls listed for low risk category servers apply to medium risk category servers, in addition the following:
ii. Servers must be protected by appropriate physical and environmental controls that prevent unauthorized physical access to the system, unauthorized manipulation of hardware controls, unauthorized server configuration, or unauthorized server state changes
iii. Inactive accounts with non-administrative access should be disabled within three days
iv. Physical access to the environment should be logged and maintained for at least 30 days.
v. External connections to any non-public IT resource must use an encrypted protocol such as Virtual Private Networking (VPN), Secure Shell (SSH), Secure FTP (SFTP), secure web services (SSL or HTTPS), etc.
vi. Systems must have a current, documented log review process, and must be logging appropriate server activities for purposes of detecting intrusions and attempted intrusions, and have a process of reviewing and responding to the logs appropriately.

vii. Servers should use uninterruptible power supplies to protect against electrical power variations that can cause outage or equipment damage.
viii. Support contracts with authorized service providers should be maintained to ensure expedient support in case of failure.
ix. Systems must have a documented plan for regular data backup to prevent loss or downtime due to unavailability of data.
x. Systems must have a current, documented plan for data restoration and testing.
xi. Backed up data should be physically separated from original production data.
xii. Two factor authentication must be used for any remote administrative functions

5) High Risk Category Systems

i. The following list details the minimum set of controls that should be implemented for high risk category systems. All controls listed for low and medium risk category systems apply to high risk category systems in addition to the following.
ii. Servers must use host based intrusion detection technology and have a documented response process.
iii. Systems should employ redundant hardware and resource connections to minimize risk of failure.
iv. Systems should use redundant storage systems (such as RAID) to minimize data loss and single points of failure.
v. Systems must use approved file integrity checking tools and have a documented response process.
vi. Systems must have documented secure authentication practices.
vii. Systems must use secure protocols as default (technically infeasible exceptions need to be documented by an appropriate administrator).
viii. Systems storing any Class I information must use encryption for both the live production information, and for backups of that information.
ix. The system may not function as a relay for SMTP or other means of relaying non- University related email.
x. Systems must have a current, documented plan for installing, configuring and managing the operating system.
xi. Systems must have a current, documented plan for installing, configuring and managing application(s).
xii. Systems must have a current, documented plan for installing, configuring and managing the system hardware.
xiii. Systems must have a current, documented change and configuration management plan.
xiv. Systems must have a current, documented incident response and continuity plan.
xv. Systems must have a current, documented plan for regular maintenance.
xvi. Two factor authentication must be used for administrative functions

III. Responsibilities

By USG Board of Regents Policy 11, the CIO is responsible for ensuring the implementation of security requirements which pertain to these Server Security Standards. Employees who violate this standard will be subject to disciplinary action up to and including termination of employment.

IV. Related Documents

University Acceptable Use Policy
Data Stewardship and Classification Standards
Remote Access Policy
Remote Access Standards
IT Systems Scanning Procedure

Modifications:

4/1/2015

Changed Title from Server Security Standards to Security Standards for Information Systems
Added addition of IT handbook section 5.6.3 to Purpose section
Removed Purpose from 2 and re-named it as Risk Categories
Replace “server” with “system” in various places
Add requirement of two factor authentication at sections 4, xii and 5, xvi.
Section 3i, changed from “server owner” to “system owner”