Auburn Montgomery

Title: Registration and Security Policy for AUM Servers

Responsible Office: Information Technology Services

I. PURPOSE

To outline the steps required to register and maintain departmental servers within the AUM data network.

II. POLICY

All servers must be registered and secured by the designated server administrator prior to making the server network accessible thus ensuring network availability, data integrity, and safe transaction processing.

III. EFFECTIVE DATE

February 2007

REVISED DATE

June 7, 2007

IV. APPLICABILITY

All server administrators responsible for providing services to AUM users.

V. RESPONSIBILITY

The Chief Information Officer, Information Technology Services (ITS), implements and administers server policies/procedures.

VI. DEFINITIONS

A Server is a computer system that provides service to other computer systems (clients) over a computer network.
A Network Server is a computer or device on a network that manages network resources and network traffic.
A file server is a computer and storage device dedicated to storing files.
A Printer Server is a computer that manages one or more printers.
A Database Server is a computer system that processes database queries.

VII. PROCEDURES

1. All AUM servers should be registered with Information Technology Services. Registration information may be obtained in room 105, Clement Hall, Information Technology Services.
2. All server administrators must notify Information Technology Services of servers in their department. Departments who have servers located in Information Technology Services facilities and maintained by the department should work closely with Information Technology Services to ensure their servers are secure in every way.
3. Registration will require the names and phone number of people to call in emergency situations, including contact information during semester breaks.
4. If and when security related issues arise and this information is not available, Information Technology Services will disconnect a server without notice.
5. Information Technology Services must be notified upon discovery of any system breach or suspected system breach.
6. Information Technology Services reserves the right to disconnect any server which poses a threat to the AUM network.
7. Any server not following procedures will be considered unsafe, and a threat to the campus network.
8. Registration of a server on the AUM data network must be accompanied by departmental approval.
9. Administrators will be provided information on Family Educational Rights and Privacy Act of 1974 (FERPA) and maintenance of student record privacy.
10. Servers should be located in areas secured by locks and be accessible only to authorized personnel.
11. Administrators should only run those services on servers that are needed to complete its designated task.
12. Services prohibited include DNS Server, TFTP server, RPC services and SMTP (Mail Server), peer to peer server, and game servers.
13. All servers should be up to date on all operating patches. The server administrator should have a frequent schedule of checking for patches to ensure the system does not become exploited by a known vulnerability. System patches should be checked immediately if a threat has been reported. If patches are not applied in a timely manner, a server could be disconnected from the network until vulnerabilities have been addressed.
14. Server administrators should limit log-on retries and disable accounts after a designated number of failed log-on attempts.
15. Accounts must be regularly reviewed for inactivity, and any dormant accounts disabled or deleted. Old accounts should be terminated

reasonably as people leave AUM. Administrators should have a clear deadline for account termination.

16. Special care should be taken with privileged accounts (including but not limited to "root" for UNIX and "administrator" for Microsoft). Passwords for privileged accounts should be given only to people with a need for privileged access. For Microsoft servers, the "administrators" account should be renamed.
17. All account passwords should be a minimal length of 7 characters and include combinations of number and special characters.
18. Wherever, feasible, a log-on banner should only give the name of the software system. A system banner will never contain a phrase that includes the server's actual name. Log-on restrictions by time of day or network address should be implemented if possible. All operating system, version/release numbers, and vendor information provided in log-on/sign-on banners should be limited or disabled.
19. Server administrators should have a regular schedule to backup the system. Archives should be held in reserve for an appropriate period of time to recreate a system image as needed. (For example, daily backups kept in a 45 day rotation, weekly backups kept in a 12 week rotation). Backups are also important to restore a server to its configuration before the intrusion, virus, etc. occurred.
20. Logs of user activity must be retained for a period of at least six months. Logs should include (where feasible) the time and date of activities, the user ID, commands (and command arguments) executed, ID of either the local terminal or remote computer initiating the connection, associated system job or process number, and error conditions (failed/rejected attempts, failures in consistency checks, etc.) Logs should be checked regularly on a daily or weekly basis for signs of malicious activity. Knowledge that logs are kept, acts as a deterrent to abuse. Logs are also essential in investigating incidents after the fact.
21. AUM assumes that any server on campus dealing with students contains sensitive data. This includes but is not limited to student numbers, credit card numbers, grades and other personal data. A FERPA form (obtained from Information Technology Services) must be signed and submitted by the Administrator and all user accounts having access to this information. FERPA training is available from the Office of Enrollment Services.
22. A vendor or consultant may gain secure access to a server from off campus for a designated period of time. The system administrator arranges access. The system administrator is responsible for enabling/disabling the vendor's access. It is recommended that the vendor or consultant access be limited to business hours only and only for the duration needed to address the scope of work. It is also recommended that vendor access be restricted by source IP address and service port. The vendor or consultant may be required to sign a non-disclosure agreement before gaining access to a

server. The system administrator should terminate vendor access/accounts at the end of the scope of work.

23. A server administrator must respond to any incidents immediately. Information Technology Services and the server administrator will analyze the server and logs to attempt to determine the method by which the server was compromised. The server's system volume will be reformatted if it has been determined that the server was compromised. The operating system will be reinstalled with the latest security patches and must pass a security scan before being reconnected to the AUM data network. Information regarding security incidents will be kept confidential by all parties involved. Only authorized personnel may disclose such information.

Add university server request form.

VIII. EXCLUSIONS

IX. INTERPRETATION

The CIO of Information Technology Services will interpret policies as needed.

APPROVAL TO PROCEED: _____ DATE:_____

Auburn Montgomery

ACCEPTANCE OF RESPONSIBILY

Registration and Security Policy for AUM Services

I,_____, understand that by my acceptance of the Registration and Security Policy for AUM Servers that I assume responsibility for complying with this policy fully. I have read the policy and procedures and understand their contents. By my signature below, I understand and agree to register and preserve the security of the server for which I have responsibility in accordance with the policy and procedures.

I also agree to perform routine back-ups of the server, apply system patches, and scan the server the AUM supported virus protection software.

I understand that Information Technology Services reserves the right to disconnect any server which poses a threat to the AUM network.

_____ Date_____

Signature of AUM Employee

_____ _____

Department Phone

Date:_____

Auburn Montgomery
Registration of University Server

What is this server's purpose?_____
What is the server's name?_____

Name of server administrator_____

Server administrator's Email address_____
Server administrator's telephone number_____

Emergency contact number_____
Contact information during semester breaks_____

Building and room where server is located_____

Currently installed Operating System:
❑ Windows ❑ Apple OS X ❑ Linux/Unix ❑ Other:_____
Version of operating system installed_____
Server is currently running the latest Operating System update or patch:
❑ Yes ❑ No

Services currently enabled (check all that apply)

❑ IIS Web	❑ FTP	❑ SNMP	❑ DNS	❑ DHCP
❑ File Sharing	❑ Print Sharing	❑ SMTP (Mail)	❑ POP3 (Mail)	❑ IMAP (Mail)
❑ Telnet	❑ Send mail	❑ Finger	❑ Other:_____	

Server currently running University anti-virus (McAfee agent)
❑ Yes ❑ No

Applications currently running on the server (check all that apply):
❑ SQL Server ❑ Exchange ❑ Cold Fusion ❑ Other_____

Server is physically secured (i.e. behind a locked door):
❑ Yes ❑ No

Server is protected with an Uninterruptible Power Supply (UPS):
❑ Yes ❑ No

Server is currently under a maintenance contract for support and parts:
❑ Yes ❑ No

Information Technology Services Use Only	
Hostname:	Switch Location/Port #
IP Address:	MAC Address:
Notes:	