Server Policy and Procedures Guide

I. Introduction

This policy concerning server systems and the users of those systems is intended to maintain consistency, assure availability, facilitate disaster-recovery, coordinate technical operations and apply sound security and management practices consistently.

II. Roles

A. SAWS – Systems Administration and Web Services. The department within Information Resources that is responsible for SUNY Cortland's servers.
B. Departmental Technical Contact – the person within a department that is responsible for the operational management of the server and the applications residing on the server. This person must have had experience managing servers and the applications on the departmental server, or attend an appropriate level of server training (at the expense of the user department).
C. SAWS Technical Support Contact – the SAWS staff person that is responsible for the technical support of a specific server.

III. Server Purpose

A. The purpose of a server must be documented by the designated departmental technical contact and SAWS technical support contact and kept current by the departmental technical contact to reflect any changes.
B. The server shall only be used for the documented purpose, and changes in purpose need to be agreed to by both parties, the SAWS director and the department head.
C. The purpose(s) of the server must integrate with the overall campus network and server design. SAWS will coordinate with Networking and Telecommunication to assign appropriate Internet Addresses, and allow appropriate access through firewalls.

IV. Server Documentation and Service Level Agreement

A. Server documentation should include the name of the department head, the departmental technical contact, backup procedure, root-privileged users, life-cycle replacement plan, disaster recovery plan and purpose(s) of the server.
B. SAWS will provide a formal, written Service Level Agreement (SLA) which will detail the specific responsibilities of the departmental technical contact and also the SAWS technical support contact. Sign-off by the dean or associate vice president, the associate provost for information resources, the department head and the SAWS director will be required to complete the SLA prior to installation of the departmental server.

V. Server Location and Hardware Standards

A. All servers must be housed in the Information Resources data center.
B. In most circumstances, servers shall be installed in Information Resources' virtual environment.
C. If dedicated hardware is required, the departmental technical contact must consult with the SAWS director, or designee, prior to the department's procurement. Information Resources has standardized on certain hardware to maximize stability and control, and hardware installed into the data center must comply with these standards.
D. Departments utilizing dedicated hardware will be responsible for funding the dedicated hardware's life cycle replacement, and continuation of warranty service.
E. SAWS will provide basic hardware support, including working with the vendor on hardware issues.
F. SAWS will coordinate physical access to the server if needed.

VI. Server Administration

A. Each server must have a designated departmental technical contact. Students will not be allowed to administer a server without permission from the Director of SAWS.
B. SAWS will designate an Information Resources technical support contact for each server.

C. SAWS will provide only the most basic support for departmental servers, SAWS will facilitate joining the server to the domain, provide an Operating System if in the virtual environment, provide power and network connectivity, and provide antivirus.

D. It is the responsibility of the departmental technical contact to maintain all aspects of the application and administration of this server.

E. Departmental servers shall not run prohibited services, such as: IMAP, POP3, SMTP, DNS, WINS, DHCP, or any service which Networking or SAWS deems detrimental to the server or network infrastructure.

F. Proposed changes to the server configuration or purpose should be coordinated with SAWS through the departmental technical contact and SAWS technical support contact. Such changes must be communicated and coordinated with SAWS in advance of additions or changes to the configuration.

G. Each server will have a backup and disaster recovery plan (as well as a life-cycle replacement plan if using dedicated hardware) developed by the departmental technical contact and SAWS technical support contact. This plan must be completed at implementation time and is a part of the overall server documentation.

H. "Root" access to servers must be established for SAWS support staff use. This may be in the form of a single, shared user account. All servers will be part of the Active Directory Domain, and all Domain Administrators will have access to the server, via remote services and physical console access.

I. To provide a consistent mailing address to the public, e-mail should be obtained and distributed from the campus' central mail node(s). This involves using the following address format when advertising mail addresses or configuring POP mail clients "reply to" address: *username@cortland.edu*

J. Public WWW visibility necessitates stability of HTTP servers. Creating publicly accessible URLs on a very stable top level server provides better information to the public while minimizing demands on departmental servers. Information Resources also serves to provide the public with a more complete view of the College when "surfing" the Cortland web site. It is recognized that users who frequent information on departmental servers will establish the necessary bookmarks to expedite access.

VII. User Accounts

A. User accounts on servers should be the same name from server to server and equate to the user name within Active Directory. Usernames are of the general form *firstname.lastname.* Accounts not named in this fashion must be documented in the overall server documentation so as to identify the person responsible for the account and its intended use. No anonymous accounts are permitted.

B. All guest accounts will have an assigned faculty or staff sponsor. Guest accounts are to be documented and made available to SAWS. This documentation should indicate the name and contact information of the user in addition to the faculty/staff sponsor. The documentation should also indicate the purpose, privileges, and duration of planned use.

C. It is the intent of SAWS to develop a common account creation tool for the creation of user accounts. This common tool would maintain a central database of users accounts, names, purpose of the account and expiration date among other data items.

D. User accounts on departmental servers shall be subject to the same College "appropriate use" policies as the central systems.

VIII. Security

All servers must adhere to all Information Resources security policies and SAWS security best practices including but not limited to:

A. Windows Servers Best Practices

1. Working antivirus software with up to date definitions
2. A member of the SUNY Cortland Domain
3. Receiving windows updates, from SUNY Cortland's WSUS
4. Utilizes strong password for local accounts
5. File servers that are not directly administered by Information Resources should not contain any personal information.
6. Unnecessary Services are disabled
7. Wireless devices disabled
8. Windows firewall enabled with only necessary ports/services

B. Web Server Best Practices

1. No webserver shall house any personal information
2. All web servers must adhere to the server best practices
3. If running SSL all web servers will utilize SUNY Cortland certificates from our selected vendor
4. Web servers will be routinely scanned
5. Any forward facing web server, those available to the public, will be routinely scanned and any scripts such as php, asp, asp.net or perl will be reviewed periodically for code compliance

C. Linux Servers and Appliances

1. When possible automatic updates shall be enabled
2. Only necessary services should be enabled

All servers will be routinely scanned for necessary configurations. Routine scans are also conducted to search for sensitive data; reports are reviewed by the information security officer, and the deputy security officers.

IX. Sanctions

Violations of this policy and/or other Information Resources policies may result in the server being removed from service.

3/2011