

Network Security & Usage Policy

DRAFT June 10, 2003

Note: This is a draft policy of Salem State College, as of May 2, 2003, pending final revisions/approvals. Revisions of this draft have occurred on 4/22/03, 5/02/03 and 6/10/03.

Salem State College Network Use Policy

A. Introduction

The network (SalemNet) of Salem State College (SSC) exists to facilitate the educational mission of the College. Both Academic and Administrative users are granted access to the network for the purpose of supporting this mission. The network provides services that allow SSC students, faculty and staff, as well as affiliated groups access to information, share data, collaborate and communicate. Responsibility for managing SalemNet and ensuring its secure and effective operation falls to the Networking Services (Networking) group of the Information Technology (IT) department. Networking is responsible for the maintenance, planning and implementation of network growth and to coordinate these efforts with the Offices, Schools and Departments (hereby defined by the term "units") that make up the College. Salem State College is subject to security audit by State and Federal auditors for compliance to standard practices. This document is designed to place Salem State College within such practices.

On October 16, 2001 the Executive Order on Critical Infrastructure Protection was signed. It specifically points out that institutions of Higher Education are targets of hackers and cyber terrorists. These groups find the open nature of such institutions to be easy targets. The information contained on College systems can lead to financial and, increasingly, identity theft. Further, College systems are targeted as "launching points" for attacks on other, more lucrative targets.

Federal legislation, such as the Family Education Rights and Privacy Act (FERPA), the Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), the USA Patriot Act, the Gramm-Leach-Bliley Act (GLBA) and the TEACH Act all place some liability on institutions that collect financial and personally identifiable information in the event that information is stolen or misused.

B. Scope

This policy is applicable to all individuals using College-owned or controlled computer and computer communication facilities or equipment. It is applicable to all College information resources that are connected to the College's network. This specifically includes, but is not limited to, all hardware connected to the network.

Individual units within the College may define "conditions of use" for information resources under their control. These statements must be consistent with this overall Acceptable Use Policy and Network Use Policy of the College but may provide additional detail, guidelines and/or restrictions. Such policies may not relax or subtract from, these College-wide policies. Where such "conditions of use" exist, enforcement mechanisms defined therein shall apply. These individual units are responsible to furnish the Office of the Chief Information Officer (CIO) with a copy of the approved document. Units must also publicize both the regulations they establish and their policies concerning the authorized and appropriate use of the equipment for which they are responsible.

C. SSC Network Components

The network consists of the following:

1. **Access-Level Physical-Layer Network Infrastructure** - network wiring and electronics (network switches and/or hubs) connecting computers and other devices within SSC buildings.
2. **Backbone-Level Physical-Layer Network Infrastructure** - Core network switches/routers in each building that interconnect SSC buildings and campuses.
3. **Wide Area Network Connections** - Wide Area Network (WAN) that connects distributed portions of the SSC network. These include Fixed and Dynamic-speed leased lines, fiber optic cable and wireless devices.
4. **Wireless Network Access "Air Space"** - radio spectrum used for wireless network access at SSC. Currently these ranges are 2.4GHz, 2.8GHz, 5GHz and 23GHz.
5. **Internet Connections** – services connecting the college network to the Internet. The College currently maintains two connections to the Internet. Faculty and Administrators are provided service through the Commonwealth's Information Technology Services (ITS) group. Resident's Halls, Classrooms and Labs access the Internet through expedient Networks.
6. **Core Network Services** – including but not limited to DNS, firewalling, e-mail, DHCP, Directory Services and the servers these processes reside.
7. **Application and File Servers** – Networking Services provides maintenance, service and support for both College-wide and departmental applications and the servers where these applications and other shared files reside. Included in these applications are the PeopleSoft Administrative System, Blackboard, Raiser's Edge, Web Services, email services and Touch-tone Registration.

D. General Provisions

1. **SalemNet as a Principal Institutional System**
The network is a critical campus principal institutional system, available to all faculty, staff, students or affiliates, at all campus locations. It provides end-to-end "wall plate to wall plate" service from any computer on campus to any other, as well as to off-campus computers and resources.
2. **Subordinate Departmental Network** – A departmental network is considered an independent system and **shall not be directly interfaced with SalemNet without the expressed written consent of the CIO**. While not required, it is strongly encouraged that these networks be maintained in a manner consistent with the policies defined in this document.
3. **Departmental Equipment Attached to SalemNet** -- Networking Services will be provided with an Administrative/root/superuser account on any system (server, network device, printer, etc) that is connected to the College Network. This **does NOT** mean that Networking Services is to be supplied access to any data residing on such equipment **unless** Networking is to be the administrator of such data.
4. **Acquisition of Data Equipment** – Any system that IT, Networking Services, MIS or Telecommunications will be expected to maintain, unless otherwise agreed upon, must reside in the Information Technology Data Center at Central Campus. Similarly, prior to the acquisition of any equipment expected to be connected to the campus network and/or managed by Networking Services, approval must be granted by the Office of the CIO.

5. **Wireless Network** - Wireless services are subject to the same rules and policies that govern other Information Technology at SSC (ie Acceptable Use Policy).
 - Wireless equipment and users must follow general wireless communication protocols.
 - Standard wireless encryption and security is to be used on all devices as appropriate.
 - All wireless needs should be directed to Networking Services for review. Only Networking Services has the authority to install wireless access points on SalemNet.
6. **Extension of the Backbone into New Buildings** - The extension of the network into new buildings on campus(s) and building renovations should be included and funded as part of building construction projects. Buildings should not be erected and renovations should not be done without the capability to communicate with the SalemNet. Installation of any communications wiring and/or facilities shall be performed in accordance to industry standards and requirements set forth by Networking Services' Standard's Document.
7. **SSC's Network Protocols** - To facilitate interoperability among SSC systems, the network backbone currently supports only TCP/UDP/IP and IPX/SPX. Other protocols, e.g. Appletalk, may traverse the backbone through target-specific VLANS.
8. **Involuntary Disconnection**

To assure the integrity of the network, it may be necessary for Networking Services to disconnect a host, a group of hosts, or a network that is unsecured or disrupting network service to others. This includes hosts involved in network security problems, such as those used by unauthorized parties to attack other systems on the SSC Network or on the Internet. Under any non-emergency situation, Networking Services will make every attempt possible to contact the owner of the host or hosts involved or a unit liaison. If those individuals are not available, the disconnection may proceed. In the event of an emergency, systems may be electronically disconnected without prior notification. With regard to security issues, a disconnection might be a "partial" one that isolates the host from attacking hosts, or from off-campus access in general. A host that has been compromised by unauthorized parties may need to stay disconnected until the host's operating system can be updated and all changes made by the attacker reversed. In any situation where it is necessary to disconnect a system from the network, Use Support and/or Networking Services will work with the owner of this system to return it to a secure state.
9. **Physical Access to Wiring Closets**

Only Networking Services and Telecommunications personnel are authorized to place equipment or cabling in wiring closets, equipment rooms, etc., unless special arrangements are made with Networking Services and/or Telecommunications. Departments maintaining their own networks must use other space for their equipment and cable. At no time shall any wiring not belonging to Networking Services or Telecommunications be located within a SalemNet wiring closet without expressed written approval from the Office of the CIO.
10. **Prerequisites for Connectivity of Network Devices**

No network device will be connected to SalemNet until it has been patched to the latest release of security patches, operational code and/or firmware. Further, default passwords and SNMP Community Strings must be changed. Unless such a device is not available, only devices that support Simple Network Management Protocol are permitted to connect to SalemNet. Under no circumstances may anyone other than Networking Services install routers, DHCP Servers, SMTP Servers, Wireless Access Points or any other device that operates above "Layer 3" without prior consent from the Office of the CIO. TCP/IP is the only protocol allowed to traverse SalemNet unless prior approval has been granted. All other default protocols must be disabled.

11. Exceptions to Network Policy Requirements and Guidelines -

Requests for an exception to a requirement or guideline of this policy should be directed to Networking Services, Telecommunications and/or the Office of the CIO for coordination and approval.

12. Acceptance

By connecting to or using devices connected to SalemNet, the user acknowledges the policies set in this document and agrees to them.

E. Networking Services Responsibilities

1. Network Maintenance

Networking Services maintains building and campus network wiring and fiber, local switches, building routers/switches, backbone routers/switches, and other network devices that comprise the SalemNet network. This includes troubleshooting problems, identifying their cause, and replacing or repairing defective equipment and wiring.

2. Network Documentation

Networking Services is responsible for creating and maintaining the detailed documentation of the network required for proper network maintenance, operation, and planning.

3. Administration of SalemNet Connections to Other Networks

Networking Services maintains relationships and agreements with ITS, e-xpedient Networks and other service providers to keep SalemNet well connected to the commercial Internet and academic networks. Networking Services administers all interfaces between networks and connections between the SalemNet and other networks.

4. Administration of SalemNet Name and Address Space

Networking Services manages the SalemNet name space and the assignment of names and network addresses (IP numbers) for security and identity of users.

5. Creation/Removal of User Accounts

Depending on the type of account(s) requested, individuals within Networking Services, MIS and Telecommunications may be involved. Every effort will be made to create accounts in a timely fashion. Because of the number of accounts usually involved, new employee account requests must be submitted no less than one week prior to the start date of that employee. Accounts will be removed at the request of an employee's supervisor or through Human Resources.

6. Administration of SalemNet Wireless Networking

Networking Services manages the radio spectrums for use of wireless networking at Salem State College to ensure compatible access to all SalemNet users.

7. Network Devices

The Network is a mission critical, strategic College resource. In order to protect the Network, devices other than computers, servers, printers, and workstations must be approved as an exception to the policy by Networking Services before being plugged into any network port. These devices may be incorrectly configured or incompatible with the SalemNet Network causing outages, reliability problems and/or security breaches to all or part of the network. Devices not approved for use on Salem State College's Data Communication Network (SalemNet) will be disabled to ensure the stability and availability of the network.

8. Traffic Monitoring

Networking Services monitors traffic flow to optimize network usage, detect network problems, and ensure equitable access and other properly authorized investigations.

9. Security Monitoring

Networking Services has the right and the obligation to monitor access to, and use of, the SalemNet Network to ensure compliance with College policy as well as local, state and federal laws. To the extent possible, Networking Services monitors network traffic to detect the "signatures" of known network intrusion scenarios, viruses, or the like. **Networking Services may periodically scan the SSC network hosts to assess the vulnerability to attack.** It should be noted that there is no guarantee that Networking Services will be able to detect all potential system vulnerabilities.

10. Campus-wide Network Security Coordination

Networking Services promotes campus-wide network security and coordinates campus-wide response to unauthorized access. This also includes working with local supporters, computer users, ITS and e-xpedient Networks to protect the campus from network intrusions, denial of service attacks, and other unauthorized and/or inappropriate activities that impair network access and use.

11. Planning for Network Growth

Networking Services interacts with campus departments to ensure current and future communication needs are addressed.

12. Upgrades to Current Infrastructure

Networking Services performs upgrades to the current infrastructure to ensure current and future needs are addressed.

13. Campus-Wide Applications

Networking Services is responsible for the installation, maintenance, security, upgrading and administration of the hardware and operating systems of the following services unless otherwise agreed upon:

- a. PeopleSoft
- b. E-mail
- c. File Servers (NetWare, NT, Linux, Unix)
- d. Blackboard
- e. Web and FTP

F. Systems Security Officer

1. The Network Security Officer will work in conjunction with the Office of the CIO and shall be the primary contact to work with appropriate College officials for the interpretation, enforcement and monitoring of this policy and the resolution of problems concerning it. The Director of Networking Service is designated as the College's Network Security Officer and will manage the daily operations of this policy. Any issues concerning law shall be referred to Salem State Legal Counsel and/or Campus Police for advice and action as applicable.
2. In situations that are an immediate threat to the security or operation of a computer or network, immediate intervention may take place. In such an emergency, Networking Services will notify, as soon as possible, the appropriate College administrators and users affected by the situation.
3. When necessary, the Security Office will work with Law Enforcement in the investigation of activities whose severity is beyond the judicial scope of Salem State College. It is expected that administrators of departmental networks cooperate fully with the Security Officer as well as Law Enforcement.
4. The Network Security Officer and the members of Networking Services are the only individuals granted permission to use Network Sniffing devices. Any individual using such devices will immediately and permanently forfeit any privileges pertaining to the use of network services at Salem State College.

G. User Responsibilities

The primary users of computers connected to the SalemNet Network are responsible for the following:

1. **Abiding by Salem State College's Acceptable Use Policy**
Users should efficiently use network resources and follow Salem State's [Computer] Acceptable Use Policy and the Network Security Policy. Users are personally responsible for all activities on their User ID or computer system including security of their own passwords and may be subjected loss of privileges for misuse of computers or computing systems under their control. Such action can be enforced even if the person controlling the computer or system does not personally engage in the offense.
2. **Remote Access**
Remote Access to desktop systems and Administrative Applications will be granted by permission from the Office of the CIO with a written request from the appropriate Dean or Vice President. The mechanism for remote access will be instituted by Information Technology and may not be modified. All reasonable security safeguards and precautions will be implemented and maintained.
3. **Reporting Problems**
Users should promptly report network problems to the IT HelpDesk , and cooperate with support staff in correcting malfunctions.
4. **Taking Proper Security Precautions**
Users should select secure passwords and change them regularly. Security-minded network access techniques should be used whenever practical.
5. **Keeping the Operating System Secure**
Users should make sure their computer's operating system is kept up-to-date with current security patches. This may be accomplished by the owner, local support staff, or central staff.
6. **Sharing of Accounts and Passwords**
Only under approved situations will the sharing of accounts and passwords be allowed. This applies to the accounts of individuals as well as generic (e.g. guest) accounts. Such exceptions may only be granted through the Office of the CIO as requested by Department Heads, Directors or higher. Passwords on systems "owned" by Networking Services will be changed on a regular basis as defined by such systems. ("owned" differentiates between departmental systems managed by Networking Services and the systems that are fully under the control and responsibility of Networking Services).
7. **Do NOT install File Sharing Applications**
Applications such as Kazaa and iMesh create a security issue in that they allow others access to information on local PC's. By default, "sharing" is enabled on these products allowing anyone running the program to download information. Even in the event that sharing is disabled, these file sharing programs install products such as Gator and SaveNow, which are referred to as "SpyWare." These "hidden" applications collect information from a local system and send it to a designated host without the owner of the information's knowledge. Under no circumstances should File Sharing applications be installed on College-owned systems.
8. **Virus Infection**
If the user suspects a computer virus infection, the following steps must be followed:
 - Stop using the computer. Do not shutdown the system, or run any commands or applications.
 - Disconnect the computer from the network, if possible
 - Do not attempt to remove the virus. Contact Help Desk and inform them of the situation immediately. Inform the Help Desk of any software or hardware changes prior to the problem.

9. Termination of Employment

Upon termination of employment from Salem State College, access to all computer services provided by SalemNet will be suspended. In the interest of data maintenance, accounts will be disabled but not deleted for a period of 60 days. In cases where agreed up, access to e-mail will be maintained for a period of 14 days.

10. Network Sniffing Devices

Under no circumstances are network "sniffing" devices to be used by any individual other than the Network Security Officer and members of Network Services. Individuals employing such technologies will be banned from any further use of SalemNet resources.

H. Special Notifications

The College's computing and network systems are a College-owned resource and business tool only to be used by authorized individuals for business and academic purposes. Users should never distribute mailing lists owned by the College. The College owns everything stored in its systems unless it has agreed otherwise. The College has the right of access to the contents of stored computing information at any time for any purpose for which it has a legitimate "need to know." The College will make reasonable efforts to maintain the confidentiality of computing information storage contents and to safeguard the contents from loss, but is not liable for the inadvertent or unavoidable loss or disclosure of the contents.

I. Notification

References to this policy will be on the Salem State Networking Services web page.

Acknowledgements

This policy was based on the Interim Network Policy of Oklahoma State University (01/02). It has been modified to better fit the specific needs of Salem State College. The Salem State Policy also incorporates ideas and suggestions from the following documents:

University of Canberra, Australia Policies and Procedures – Network Access and Use Responsibilities and Obligations

Columbia University LAN Security Guidelines

EDUCAUSE Task Force Presentation on Cybersecurity & Universities

SANS (SysAdmin, Audit, Network, Security) Institute Security Policy for Higher Educational Institutions, 12/15/00

References

Digital Millennium Copyright Act

Federal Computer Intrusion Laws

Federal Electronic Communication and Privacy Act of 1986