Salem | STATE UNIVERSITY

Network Security Policy

I. PURPOSE

Attacks and security incidents constitute a risk to the University's academic mission. The loss or corruption of data or unauthorized disclosure of information on campus computers could greatly hinder the legitimate activities of University staff, faculty, students and associated users. The University also has a legal responsibility to secure its computers and networks from misuse. Failure to exercise due diligence in managing these resources may lead to financial liability by persons accessing the network from or through the University.

The purpose of this policy is to establish appropriate security requirements and restrictions on accessing and using University computers, computer systems and networks and safeguarding University information. The goals of this policy reflect these considerations and are as follows:

- Safeguard the integrity and availability of the campus networks for shared use by the Salem State University community;
- Minimize vulnerability from known threats to the integrity and availability of workstations and server systems connected to the network; Preserve the privacy of network users to the greatest extent possible;
- Block by default, commonly known mechanisms through which computing systems on a campus network are frequently attacked by other individuals or organizations; attacks leading to ethical or legal liability and injury to the University's reputation;
- Provide processes to respond to queries and complaints about actual and perceived abuses, whether internal or external, and to take action to resolve the incident and to minimize the likelihood of recurrence;
- Promote an efficient, standards-based approach to providing and managing network based services, servers, and user systems.
- Enable efficient mechanisms to detect outside attacks and to recover from damage done by such attacks, protecting the majority of network users from any campus systems which become infected with malicious code.

II. SCOPE

This policy covers all Salem State University owned and maintained computers, computer systems, computer networks and electronic communications facilities, the users of all such systems and networks, all computers connected to these networks, and to all University computing facilities, data centers and processing centers.

III. POLICY

The following policies apply to all equipment connected to the campus networks:

General

- All software used on University networks must be properly licensed. Licensing information must be readily available for audit. Licensing audits will be performed yearly, and on an as needed basis.
- University networks may be accessed only by individuals authorized by the University. Issuance of an account and access to any network must be approved by an authorized University official. Questions regarding authorization and permitted uses must be referred to the Chief Information Officer (CIO).
- Individual accounts may not be transferred to or used by an individual other than the authorized individual account holder. Sharing accounts or passwords is prohibited.
- Generic accounts, intended to be used by more than one user, shall not be allowed on any computer, computer system or network without prior written authorization from the CIO.
- All University computers and computer systems attached to University networks will be compliant with all laws, including, without limitation, laws relating to computer security.

Addressing and Domain Services

- Individuals and academic or administrative users may not create or support an Internet domain hosted from the University's network without prior approval of Information Technology and Services (IT).
- IT administers the Salem State University IP address and the *salemstate.edu* domain. IT also manages any additional domains that support the mission of the University.
- Technological changes and other factors may require a reconfiguration of the network resulting in a change to the network addresses assigned to University computers. IT will give prior notice to affected users before making any changes.

Network Connections

- No Salem State University departments, faculty, staff, or students may connect, or contract with an outside vendor to connect, any device or system to the University's networks without the prior review and approval of the CIO.
- Universitys or departments that wish to provide Internet or other network access to individuals or networks not directly affiliated with the University must obtain prior approval from the CIO.
- All devices placed on the University's network must be registered with IT. All authorized University network users (faculty, staff, or students) must be assigned a physical network port and network address by IT. Network connections at public access ports are restricted to authorized members of the University community.
- Physical access to University networking equipment (routers, switches, hubs, etc.) is not permitted without the prior approval of IT.
- IT will provide a general method for network authentication to University systems.

External Services and Requests

- IT will take action to prevent source network address forgery (spoofing) of internal network addresses from the Internet. IT will also take action to protect external Internet sites from source address forgery from the University's network.
- The University's external Internet firewall policy is to deny all external Internet traffic to the University's network unless explicitly permitted. Access and service restrictions may be enforced by IP address and/or port number. Proxy services may be used in conjunction with the firewall to restrict usage to authenticated individuals.

This policy is designed to protect University network users from attacks launched from the Internet.

- The University will identify the systems that will offer Internet services. To facilitate this, academic universitys/departments and other administrative departments must register with IT, systems that require access from the Internet. These systems must also be protected by access control software (e.g., TCP Wrappers).
- The University's internal Internet firewall policy is to deny all internal IP traffic out-bound to the Internet unless explicitly permitted. This policy is designed to protect others on the Internet from attacks launched from the University's network.
- Some network services through standard ports are supported. However, services may be restricted to a limited number of subnets or hosts. For example, electronic mail may be sent and received only by authorized mail servers on campus. User access to the mail accounts on these servers will be permitted from off campus through the firewall.
- Most network services through non-standard ports are not supported. Services through non-standard ports may be restricted to a limited number of subnets or hosts. For example, WWW access via the standard HTTP port will be permitted, but via some other arbitrary port number may not be permitted.
- Limited encrypted tunnels for passing through the firewall to internal resources, such as X-Windows, is permitted with the prior approval of IT. The recommended method is to use Secure Shell (SSH). IP Multicast tunneling is not permitted.
- All modem connections that allow someone from outside the University network to access the University's network must be registered with IT. The University reserves the right to block any modem connections, or disconnect any computer system that allows unauthorized access to the network.

Network Security

- In collaboration with academic and administrative departments, IT shall identify the appropriate network security level for University systems. These levels are, from highest to lowest: Mission-critical, Important, Normal and Low. Efforts shall be made to protect University computer systems and reviews will be conducted periodically.
- Wireless communications or other broadcast technologies must not be used for data transmission containing "confidential" or "restricted" data unless the connection is encrypted and has an acceptable level of user authentication.
- Computers configured with the intent of accepting connections from other computers are considered to be servers, and must be physically secured in a location that meets the University's standards and guidelines for servers.
- Third-party vendors must **not** be given dial-up privileges to University computers and/or networks unless the involved system administrator determines that they have a bone fide need. These privileges must be enabled only for the time period required to accomplish the approved tasks (such as remote maintenance).
- Confidential or restricted data in unencrypted format is prohibited on University mobile computing and storage devices. Please see the State policy on mobile computing and storage devices for additional guidance and requirements.
- In coordination with administrative departments and law enforcement, IT will investigate, or cause to be investigated; any unauthorized access to University computer systems.
- Systems on the network must have adequate security installed and maintained. All systems connecting to the University network must be configured and maintained in such a manner as to prohibit unauthorized access or misuse. For example, a guest account must have a secure password.

- Only an authorized system administrator may alter a computer's network settings, parameters and user access controls lists.
- Adequate virus protection software must be installed and frequently updated on all equipment attached to the networks, and patches must be routinely applied to computer operating systems and applications.
- It is the responsibility of all Salem State University network users to report security problems to IT for investigation, on a timely basis.
- Network usage judged appropriate by the University is permitted. Some activities deemed inappropriate include, but are not limited to:
    - Establishing unauthorized network devices, including a router, gateway, or remote dial-in access server; or a computer set up to act like such a device.
    - Engaging in network packet sniffing or snooping.
    - Operating network servers of any sort in violation of IT guidelines.
    - Setting up a system to appear like another authorized system on the network.
    - Other unauthorized uses prohibited by the Salem State University Acceptable Use Policy, or other related policies.

Monitoring and Auditing

- IT maintains traffic logs of the firewall and network backbones for security auditing purposes.
- To safeguard the integrity of the University's computing and electronic communication resources, and to minimize the risks to both those resources and the end users of those resources, IT will monitor data traffic to detect anomalous network activity and will access, retrieve, read and if required, disclose data communications when there is reasonable cause to suspect a violation of applicable University policy or criminal law, or when monitoring is otherwise required by law.
- IT will coordinate investigations into all alleged computer or network security compromises, incidents, and/or problems. To ensure that this coordination is effective, ITS requests that security compromises be reported to ITS (e-mail: IThelp-desk@salemstate.edu) at the time they are first detected.
- If scans or network monitoring identifies security vulnerabilities, the cooperation of the system owners and system managers for the systems and the networks will be solicited. If the appropriate contact cannot be determined, the department's management will be notified. When a security problem (or potential security problem) is identified IT will take steps to disable network access to those systems and/or devices until the problems have been rectified. IT will disable network access at the closest network port to which IT has administrative control.

IV. REPORTING SECURITY INCIDENTS

Reporting incidents is an ethical responsibility of all members of the Salem State University community. A critical component of security is to address security breaches promptly and with the appropriate level of action. The University's Incident Management Policy outlines the responsibilities of departments and individuals for reporting, as well as defines procedures for handling security incidents. No one should take it upon themselves to investigate the matter without authorization from the Chief Information Officer or General Counsel.

V. VIOLATION OF POLICY

Violation of this policy may subject a user to disciplinary action under appropriate University disciplinary procedures. The University may take such action as necessary, in its discretion, to address any violation(s) under this policy. In addition:

- Any device found to be in violation of this Policy, or found to be causing problems that may impair or disable the network in any way is subject to immediate disconnection from the University's network. IT may require specific security improvements where potential security problems are identified.
- Attempting to circumvent security or administrative access controls for information resources is a violation of this Policy. Assisting someone else or requesting someone else to circumvent security or administrative access controls is also a violation of this Policy.

VI. AUTHORITY

This policy will be approved by the President, CFO and CIO

VII. DISCLAIMER

The University shall not be liable for, and the user assumes the risk of loss or destruction of data or interference with files resulting from the University's efforts to maintain privacy, integrity and security of the University's networks.

The University reserves the right to change this policy at any time without notifying the audience affected by the policy.

VIII. SUPPLEMENTAL REGULATIONS AND STANDARDS

Acceptable Use Policy: Salem State University policy for acceptable use of University services and equipment.

Incident Management Policy: Salem State University policy for incident management and reporting.

Information Security Policy: Salem State University policy for information security.

Enterprise Wireless Security Standards: Commonwealth standard for wireless communications and data encryption on those devices.