Infrastructure Management Policy

I. PURPOSE

II. POLICY

The secure and persistent availability of technical services to all members of the Salem State University campus community is of paramount importance to the Information and Technology Services group on campus. Intermittent outages of online services, no matter how rare, are clearly disruptive to the members of the campus academic and administrative communities. The Information and Technology Services department takes great pride in the delivery of a quality and consistent service structure to the University, following the guidelines outlined in this policy.

The purpose of this policy is to establish appropriate operational guidelines for administering University computers, computer systems, applications and networks supporting the University technical service offerings. The goals of this policy reflect these considerations and are as follows:

- Safeguard the integrity and availability of the campus services used throughout the campus community;
- Provide an operationally effective working platform for those services;
- Provide a service environment that keeps pace with the business needs of the University;
- Provide a working environment that is free of unplanned disruptions and technical surprises;
- Provide an environment that respond quickly to unforeseeable incidents that may affect the operational integrity of the service platforms;
- Provide an operational environment that grows smoothly with changes, and forecasts predictable expectations.

III. SCOPE

This policy covers all Salem State University owned and maintained computers, computer systems, computer networks, application services and electronic communications facilities, and all members of the support team administering these services.

IV. POLICY

The following policies apply to the administrative activities used by the Information and Technology Services department to support the infrastructure management needs of the University:
Visitors Access to the Data Center:

- Visitors must be granted access by an authorized member of the ITS staff.
- They must sign-in to the Visitor’s Log before entering the data center.
- They must wear a Data Center Visitor’s Pass at all times during their visit.
- They must sign-out when completing their visit to the data center.
- They must return their Data Center Visitor’s pass to an authorized ITS staff member.

External Connections to Application Software Environments:

- Vendors wishing to debug or upgrade a software component will contact either the business office or the Application Services group directly. The request will be forwarded to the Infrastructure Services group to enable remote access to the machine to which the third party vendor has requested access. If Infrastructure Services is contacted first, they will then notify Application Services to verify that the connection is required prior to taking any action.
- This connection will be setup with an estimated completion time established between the Vendor and Application Services. When the timeframe has elapsed, the remote access is disabled on the machine.

Network and Portal Access:

- User IDs are managed via the issuance of the campus Clipper Cards; all persons that are issued a Clipper Card (because they have business on campus) are given minimal service access to the campus network.
- The Clipper Card Office requires a photo ID to verify the person’s identity. They then verify that the person is either a student or an employee via the campus Employee Management System. If the person is a student or an employee, they issue the card with the correct category printed on the front (Student, Faculty/Staff).
- Additional application services access are administered by departmental security manager request and manually entered into the appropriate application system by the ITS Security Administrator.
- All entries on the campus Employee Management System are Human Resources or Registrar authorized.
- Access to facilities is granted by the University Facilities office after receipt of a valid request from the appropriate Faculty/Staff person.
- Each card has a serial number printed on the back is bar code, and characters, and electronically recorded on the magnetic stripe on the back of the card.

Portal Authentication:
• Portal authentication uses Username/Password combinations. The PeopleSoft Portal prompts for Username and Password. It first determines if the account is disabled in PeopleSoft. If it is, the authentication fails and the login process terminates unsuccessfully.

• If the account is not disabled in the Portal, it then determines if it should use data stored internal to the Portal, or use the LDAP server.

• If it should use the internal data, it compares the encrypted password with the password stored within the Portal. If there is a match, the authentication completes successfully and the Portal proceeds to authorization.

• If the encrypted passwords do not match, or if it should use the LDAP server, the Portal contacts the LDAP server to authenticate the user. The LDAP server determines if the account is disabled in LDAP. If it is, it returns a failure status to the Portal.

• If the account is not disabled in LDAP, LDAP then compares the encrypted passwords (the one provided by the Portal and the one stored in LDAP). If they match, LDAP returns success to the Portal. If they do not, LDAP returns a failure status to the Portal.

• If the Portal receives a success status from LDAP, the authentication succeeds and the login proceeds to authorization. If the Portal receives a failure status from LDAP, the authentication and the login complete with failure.

• If the user changes the password in the Portal, whether by the user's choice or because the Portal requires the password to be changed, the encrypted new password is communicated to the LDAP server, and the Portal data changed to indicate that future authentications should use the LDAP server.

• If an administrator changes the password within the Portal, the Portal will indicate that future authentication attempts should use the Portal data. SSU policy requires that the administrator also set the password expired indicator, which will result in the user having to change their password on the next successful authentication.

• When a user attempts to use with SA or FS, the Portal communicates to the application that the user is authenticated and what user ID should be used. The user can access the application only if a menu item to do so is presented to the user. The authorization phase of login determines whether these items should be displayed.

**Password Rules:**

• Access to network, portal or application servers are synchronized, and use a consistent set of password rules, as follows: (Active Directory does not allow us to set the same password-formation rules. We are looking at ways to do this, but right now the first bullet item applies to PS, not AD)

• Password length: 8 character minimum (one alpha and one number required)
• Password changes for student and faculty are required at least every 127 days.

• Password changes for administrative accounts are required at least every 90 days.

• Password changes for faculty and student accounts are required at least every 127 days to accommodate summer recess and leaves of absence.

• Passwords are blocked after six missed attempts.

• Blocked passwords can be reset if the user knows the answer to the secret question they set up on original entry. (I think the auditor mentioned that the account only needs to be blocked for an hour)

• Blocked passwords can also be reset by ITS user support after the user successfully authenticates themselves to ITS user support personnel.

• Passwords cannot be reused for a sequence of ten versions.

• If a terminal session has been idled for more than 15 minutes, the user must login to resume access to the terminal.

**Network Devices:**

• “Network devices” are defined as infrastructure systems through which data passes. This does not include end-devices such as servers and workstations.

• Most Networking personnel have access to all Network system components, and Application Services database administrators have access to the servers which support their applications.

• Default security configurations must be modified/removed where they are not necessary or do not conform to Salem State University configuration requirements. The following is a list of parameters to which special attention is given:

  • SNMP Communities: By default, most systems use the value “public” as the default for the Read and Write community strings. These should be changed to something more secure or disabled altogether; dictionary words are not.

  • Default accounts/passwords: Where possible, default accounts are removed completely. Some systems do not permit this. In that instance, they should be disabled. If that is not available, the passwords should be changed to a very long, random string.

  • Admin/root accounts are to have their passwords reset immediately. NO SYSTEM WILL GO ON THE NETWORK WITHOUT A STRONG PASSWORD.

  • Default IP addresses: All network equipment, including servers, shall have static IP addresses. Default addresses will be changed to an address within the appropriate subnet for the device.
• Default listening ports: For all network components supporting remote access (Telnet, SNMP, FTP, SSH, Web/SSL, etc.), where possible, unnecessary ports will be disabled. In the event that a non-standard port is necessary, a Network Security inspection should be performed and relative rules placed on firewalls. Where possible, Telnet will be disabled in favor of SSH and HTTP in favor of HTTPS. Similarly, non-secure protocols will be disabled wherever possible.

• Default rules: Default rules on firewalls, routers and switches need to be reviewed for relevance to our environment and configuration standards. Rules that are not necessary or do not otherwise comply are removed or disabled. By default, a “deny” rule is put in place. Subsequent “allow” rules should then provide the necessary access. Changes to such systems are logged in the University's Change Management System.

• Authorized sites for automatic downloads: Many systems have the ability to automatically download patches and updates. The default patch sites are reviewed and modified as necessary to ensure trusted zones.

• Time servers: University systems point to the University time server at monsoon.salemstate.edu.

• DNS: While all network components are listed in the University’s DNS systems, only those that require access from the outside participate in zone transfers. That is to say, those that do not require access from the outside will be hidden from off-campus queries.

• Backups: Servers and other systems that contain dynamic data are backed up as a part of the daily routine. However, all network components that contain configurable parameters are to have their configurations backed up. In the event that the system does not provide a mechanism for back up, the configuration will be documented in hard copy. All changes to configurations will be logged in the University’s Change Management System.

• Restrict who can connect/from where: With the exception of external-facing servers (e.g., Web servers) and appliances (e.g., VPN), access to University systems will be restricted to on-campus personnel. Where necessary, off-campus access will be provided via a VPN connection.

• IP Address standards: Configuration of devices that require an IP address will conform to the IP Standards of the University. IP addresses shall be documented with Network Services.

• Addition/modification of firewall rules: Addition of firewall and router rules shall be reviewed by Network Services and, where necessary Application Services, prior to implementation. Changes to rules shall also be reviewed prior to implementation. Some rules, e.g., blocks based on network scans, can be modified to add offending addresses/ranges. All changes will be logged to the University’s Change Management System.

• Consoles: Consoles are to be set to auto-lock or logout after 15 minutes of inactivity.
Access to PCI Information:

- The policy is that the only PCI information retained in any University system is the credit card number itself (in encrypted format), the pin block, CVS code and authorization codes are not retained.

- No screen in either PeopleSoft Student Administration or PeopleSoft Enterprise Portal display the entire card number; only the last four characters.

- Access to even this information is limited. In PeopleSoft Student Administration there is only one screen within the Admissions module and three screens within the Student Financials Module which display the truncated credit card number.

- In the portal there is one screen available to ClipperCard administrators and it only shows the trailing four digits of the card number.

- This card visibility information also applies to all transaction logs generated in portal applications.

Credit Card Information Encryption:

- The capture and transmission of credit card information by campus services is classified as confidential information and is therefore treated in the following exceptional manner. For all credit card numbers stored in the system, we are using DES3 encryption technology. This technology makes the information unusable to anyone trying to access the information by unapproved means.

- This same encryption process ensures that the information is unavailable even on an inquiry basis to all members of the Information and Technology Services support team.

Testing of Security Systems and Processes:

- Logs are checked daily for inconsistencies and suspicious traffic. ITS conducts independent, random penetration testing annually.

Security Patch Installation

- Network system patches are applied once a month (unless circumstances require an interim installation) on the Thursday following the 2nd Tuesday of each month.

- To ensure system and application stability for these patches, they are tested by Application Service personnel in the development environment before being applied to production machines.

- Once they have cleared this testing process, they are immediately applied to the production operating systems.

Implementation, Use and Updating of Anti-Virus Software:
• All Windows servers use self-updating McAfee antivirus. Sun and Linux systems are not running antivirus software.

Encryption Keys:

• Access to data encryption keys protecting the University’s data resources are protected by a dual encryption process ensuring that only authorized members of the IT support staff have access to these keys.

• The primary key is protected by a DES3 encryption algorithm supplied by the application vendor.

• This key is encrypted again, using a second key supplied by authorized data center personnel to ensure that the key stored on the hard drive cannot be unencrypted by conventional means.

• These secondary keys are stored in an offsite, secure location, accessible to only a few key members of the data center staff.

Firewall/Router Configuration Review and Testing:

• Firewall and router configurations are reviewed for consistency and compliance on an as needed basis (when significant infrastructure changes are made) or every six months at a minimum.

• To ensure that hardware configuration process have not been compromised, the Network Services personnel conduct quarterly reviews of all firewall and router rule sets.

Tape Management:

• Tape backups are stored securely in the data center until the scheduled pickup by Iron Mountain. On the day of the pickup the tapes are transferred into a locked safe in the reception area of Information and Technology Services. At time of pickup, University personnel open the safe and transfer the media to the Iron Mountain courier.

• Iron Mountain tape vault documentation attached and more available at: http://www.ironmountain.com/resources/services/tape.asp

• ITS currently uses two different software packages to backup our systems; Veritas (Symantec) NetBackup and BakBone NetVault. The University does not encrypt the data on these tape prior to offsite storage because PCI data is already encrypted at the field level ensuring privacy.

• The data retention policy for the University specifies that all copies of confidential data are destroyed once their preservation cycles have elapsed.

• All tapes sent to our media disposal vendor and are certified as destroyed by that third party service.

Synchronization of all Critical System Clocks:
• The clocks on all network system components are connected to an NTP server clock to ensure precise timing synchronization between all network hardware.

V. 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.

VI. 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.

VII. AUTHORITY

This policy will be approved by the President, Executive Vice President and CIO.

VIII. 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.

IX. 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.

Network Security Policy: Salem State University policy on network security.