

University of Southern California Network Infrastructure Use Policy

Date Issued: May 16, 2005

Authority: Lloyd Armstrong, Jr.,
Provost and Senior Vice President for Academic Affairs

Dennis F. Dougherty
Senior Vice President for Administration

1.0 **Purpose**

The University of Southern California (USC) provides its faculty, staff and students with a network infrastructure to facilitate the missions of the university, including instruction, research, service and administration. The purpose of this policy is to confirm the ownership of the USC Network Infrastructure, defined below, and establish the responsibilities of USC faculty, staff, students and other employees in protecting and securing the USC Network Infrastructure.

2.0 **Scope**

This policy applies to all university faculty members (including part time and visiting faculty), staff and other employees, (such as postdoctoral scholars) and students (including postdoctoral fellows and graduate students) as well as any other users of the Network Infrastructure.

3.0 **Policy**

3.1 **Ownership of Network Infrastructure**

The USC Network Infrastructure is owned by and the property of USC. The Information Service Division (ISD) is primarily responsible for overseeing the operations of the Network Infrastructure. There is not an expectation of a right to privacy when using the USC Network Infrastructure. The USC Network Infrastructure includes, but is not limited to the following:

- USC network connections (wired and wireless) and other network equipment including jacks, wiring, switches, panels, hubs and routers);
- USC network-based communication services, such as e-mail and instant messaging;
- Computers and electronic devices (such as desktops, laptops, servers, PDAs and other handheld or mobile equipment, wireless technologies, copiers,

faxes, pagers, IP phones) that are purchased or leased using university funds;
and

- USC purchased, licensed or developed software.

3.2 User Responsibilities

“User” is defined as any faculty, staff, student, other USC employee or any other person who has access to or is otherwise connected to the USC Network Infrastructure (see Section 3.2.2 of the USC Information Security Policy at www.usc.edu/policies for additional information about “Users ”).

Users are expected to comply with USC information security policies and procedures to ensure the security of the USC Network Infrastructure, which includes ensuring that the devices they use that are connected to the USC Network Infrastructure are in compliance with this policy. A complete list of USC’s information security policies is available at www.usc.edu/policies.

Users are responsible for utilizing reasonable measures to protect the security of those components of the USC Network Infrastructure that they access and/or use, including appropriate passwords, virus protection and current patch management software, as described below.

3.3 System Administrator Responsibilities

“System Administrator” is defined as any faculty, staff, or other USC employee who has been designated by the USC Information Steward or Owner, as defined in USC’s Information Security policy, as the individual responsible for maintaining the security of the USC Network Infrastructure for that particular school, unit, division or department. In many cases, the System Administrator may be that department or unit’s Information Security Liaison.

The System Administrator is responsible for overseeing the security of the Network Infrastructure for his or her school, unit, division or department, which includes reasonable monitoring and oversight of User compliance with this policy.

3.4 Acceptable Use of Network Infrastructure

3.4.1 Password Protection

Users and System Administrators must utilize passwords, as appropriate, to secure access to all applicable components of the USC Network Infrastructure that they oversee, use or access, including documents, applications and other information systems that may require additional

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: May 16, 2005

protections. USC's Information Security Policy identifies those types of information that require enhanced protections.

Passwords must be kept confidential and must not be shared. Passwords should be unique and not obvious in order to reduce the likelihood that they will be stolen. It is advisable to change passwords regularly. Refer to Appendix A for further information about how to create and maintain appropriate passwords.

3.4.2 Virus Protection

Users and System Administrators are responsible for maintaining active and current anti-virus protection capabilities on all applicable components of the USC Network Infrastructure that they oversee, use or access. Refer to Appendix B for further information about how to obtain and maintain current virus protection capabilities.

3.4.3. Patch Management

Users and System Administrators are responsible for installing and maintaining appropriate security patches and service packs on all applicable components of the USC Network Infrastructure that they oversee, use or access. Refer to Appendix C for further information about how to obtain and maintain current patch updates.

3.4.4. Private Networks (a.k.a. Local Area Networks, Sub-Nets, Non-Standard and Specialized Networks")

Private networks, henceforth to be referred to as "non-standard or specialized" networks, consist of any network segment or subnet behind a router, firewall, or NAT device, behind which, ISD does not have administrative control of the switches or routers that the end-systems (PCs, servers) connect to.

- Private networks are not permitted except as approved in writing by the Information Services Division (ISD) Chief Information Officer (CIO).
- All private networks must have a System Administrator assigned to oversee and maintain the security of the private network who will be the liaison with ISD and the Information Security Office (ISO).
- Approved private networks must comply with all USC Information Security Policies.
- The System Administrators of the private network must either:
 - provide ISD and ISO with access to the private network as necessary to verify compliance with this and other applicable USC policies and procedures; or

Issued by: Lloyd Armstrong, Jr.
Provost and Senior Vice President, Academic Affairs
Dennis F. Dougherty
Senior Vice President for Administration

Date issued: May 16, 2005

- conduct their own testing and monitoring as directed by ISD and ISO to confirm compliance with USC policies and procedures and report the results in writing to the ISD CIO and the ISO Information Security Officer within the timelines prescribed by ISD and ISO.
- Private networks must comply with Appendix D of this Policy. Appendix D defines vulnerability testing and reporting requirements.

3.5 Unauthorized Access to Network Infrastructure. Unauthorized access to, or tampering and interference with, the USC Network Infrastructure is prohibited. The responsibility to implement access control mechanisms to prevent unauthorized access, or use of the Network Infrastructure, is shared between ISD and Private Network System Administrators.

3.6 System Monitoring and Auditing
 The Information Services Division (ISD) is authorized to monitor the Network Infrastructure and take proactive measures, including scanning, to maintain the operation and security of the Network Infrastructure. The Office of Information Security (ISO) is authorized to conduct monitoring and auditing of ISD, Users, and System Administrators to ensure compliance with this and other USC information security policies, in coordination with Audit Services, as appropriate. The university reserves the right to access any computer or electronic device connecting to the USC Network Infrastructure in order to verify compliance with this and other applicable USC information security policies.

4.0 Enforcement

Compliance with the university's information security policies and procedures shall be monitored regularly in conjunction with the university's monitoring of its information security program. Audit Services will conduct periodic internal audits to ensure compliance with federal and state laws and regulations as well as university policy.

Individuals who do not comply with these policies shall be subject to remedial action in accordance with the Faculty Handbook, the Staff Employment Policies and Procedures and SCampus, as appropriate.

Any disciplinary action under this policy shall take into account the severity of the offense and the individual's intent. Disciplinary action can include revocation of privileges to use or access any or all components of the USC Network Infrastructure, and may include other discipline up to and including termination or dismissal from USC. ISD and ISO reserve the right to revoke privileges to use or

Issued by: Lloyd Armstrong, Jr.
 Provost and Senior Vice President, Academic Affairs
 Dennis F. Dougherty
 Senior Vice President for Administration

Date issued: May 16, 2005

access any or all components of the USC Network Infrastructure for non-compliance with this and other applicable information security policies.

5.0. **Resources**

Questions regarding interpretation and implementation of this policy should be directed to the University's Information Security Officer at (213) 743-4900.

Appendix A

University of Southern California Computer Password Procedure

Date Issued: May 16, 2005

1.0 Purpose

This procedure identifies how USC faculty, staff, and other employees can protect the university's information by establishing guidelines (or best practices) for creating and maintaining acceptable passwords.

2.0 User Responsibilities

- Passwords should consist of a minimum of 8 alphanumeric characters.
- Passwords should contain a mix of characters and numbers.
- Passwords should be selected with the intention of not allowing other people to guess them easily.
- Passwords must never be the same as or resemble the Logon-ID. Passwords such as "password", "administrator", "user", "guest", etc. should be avoided.
- Passwords should not be displayed. It is not acceptable to write Passwords down and post them on a monitor, under your keyboard, in a desk drawer, etc. If it is necessary to write down a password, it must be kept in a secure place, such as your purse or wallet.
- Passwords should not be shared with, or given to anyone, without management approval, either in person or over the phone, even someone who claims to be a system administrator. If there is a requirement to share an account, users should get approval from their manager, and the system administrator must be made aware of it, so that, where possible better auditing of the ID activity may be recorded.
- Logon-ID/Passwords are the responsibility of the owner, (the person the Logon/ID was assigned to). The password owner is responsible for ensuring that their password complies with all USC password procedures and guidelines.

3.0 System Administrator Responsibilities

- Where possible, passwords should be set to expire within 120 days.
 - Most systems allow configuration of this parameter and the configuration for "grace logins" when the password expires.
- Systems should be configured to disallow re-use of passwords for 3 generations.
- Systems should be configured to "lock-out the account" after 5 incorrect password attempts.
- Locked-out accounts should remain locked-out for a minimum of 15 minutes.

Appendix B

University of Southern California Computer Antivirus Procedure

Date Issued: May 16, 2005

1.0 Purpose

This procedure identifies how USC faculty, staff, and other employees can protect the university's information by establishing Guidelines for Computer Antivirus Procedures.

2.0 User Responsibilities

- Ensure that current anti-virus software is installed and updated on end-user's PC, (see <http://www.usc.edu/isd/software/> for specific instructions on installing and configuring the ISD approved, desktop anti-virus software)
- Once the anti-virus software is installed on a workstation, end users should not modify the software or its configuration in any manner, unless directed by IT departmental personnel or the ISD Help Desk.
- Report virus incidents to departmental IT staff or the ISD Help Desk.

3.0 System Administrator Responsibilities

- Ensure that all departmental file and print servers and all workstations have current, and updated, anti-virus software installed on them.
- Ensure that once installed, anti-virus software is not modified or disabled on servers or workstations.
- Notify the ISD Help Desk of any virus incidents.

4.0 ISD Responsibilities

- Define an enterprise anti-virus solution for desktop PCs and negotiate a volume purchase for the university as a whole.
- Provide guidelines on installing and maintaining the anti-virus software and pattern file updates on desktop PCs.

Appendix C

University of Southern California Computer Patch Management Procedure

Date Issued: May 16, 2005

1.0 **Purpose**

This procedure identifies how USC faculty, staff, and other employees can protect the university's information by establishing Guidelines for Computer Patch Management.

2.0 **Individual User Responsibilities**

- Ensure that automated patch management is operational on the end-user's PC, (see <http://www.usc.edu/infosec> for specific instructions on configuring automated patch management on Windows 2000 and Windows XP desktop PCs).
- Once the automated patch management is configured on the desktop PC, users should not modify the software or its configuration in any manner, unless directed by IT departmental personnel or the ISD Help Desk.
- If automated patch management software is not available for a particular PC or operating system, users will periodically check for, and download, the software updates and patches from the software vendor's web site.

3.0 **System Administrator Responsibilities**

- Provide ISD with necessary access to verify compliance with this procedure, or conduct the verification tests determined by ISD to confirm compliance and report the results, in writing, to ISD within the timelines prescribed by ISD.
- Ensure that all departmental servers either have automated patch management software or are updated by regularly scheduled update procedures.

Appendix D

University of Southern California Private Networks – Administrator Responsibilities

Date Issued: May 16, 2005

1.0 **Purpose**

This procedure defines the vulnerability testing and reporting responsibilities of USC “Private Network” (aka. specialized or non-standard network) administrators.

2.0 **Vulnerability Testing and Reporting requirements for Administrators of Private, Specialized and Non-Standard Networks**

- 2.1 The University of Southern California (USC) operates a Class B Network license that covers the IP address space 128.125.xxx.xxx. Within that IP range, USC has assigned the USC Information Services Division (ISD) as the university-wide network infrastructure system administrator. ISD has authorized certain departments to share network administration responsibilities within their own departments. By sharing in the responsibilities of network administration, private network administrators must also assume the same compliance testing and reporting methodologies that ISD adopts for system-wide vulnerability testing. The System Administrators of the private network must either: (i) provide ISD and ISO with access to the private network as necessary to verify compliance with this and other applicable USC policies and procedures; or (ii) conduct their own testing and monitoring as directed by ISD and ISO to confirm compliance with USC policies and procedures and report the results in writing to the ISD CIO and the ISO Information Security Officer within the timelines prescribed by ISD and ISO.
- 2.2 Testing will consist of periodic technical evaluations, to be scheduled by ISD and the Information Security Office (ISO), that must render the following results:
- Host name
 - Patching status
 - Anti Virus Definition status
 - Vulnerability Scan status
 - This can be a dated report from any vulnerability scanner that is equivalent to Nessus or the Microsoft Baseline analyzer in its testing results.
- 2.3 Reporting will be based on the schedule established by ISD and the ISO. Reports must include the following information:
- Host Name
 - Test Date
 - Status

- Problems
- Remediation Plan
- Total Number of Hosts out of Compliance
- Total Hosts in Compliance