User Guidelines for Network Traffic Management

Document No.	ITS-1001-G	Rev:	D
Owner:	IT Security and Compliance		
Approved by:	Sheryl Okuno, Acting Director		
Issued:	5/28/08	Effective:	5/28/08
			Page 1 of 8

1 Purpose

Critical computing, networking, and other information technology systems support the University's educational mission. As the complexity of, and dependency on, this technology and the infrastructure that supports it rapidly increases, so does the opportunity for security violations, compromises, and intrusions – both externally and internally. Greater accessibility poses a greater risk to personal, proprietary, confidential, and institutional data.

Industry experts predict not only an increase in network attacks in the future, but much more sophisticated threats. "Blended" threats that use multiple modes of infection are increasing. These include hacking, computer worms, denial-of-service attacks, and Web site defacements that all can be remotely and instantly deployed. These kinds of infections and attacks can penetrate beyond e-mail and network servers to department servers, desktops, laptops, and other devices and services. Not only can these blended threats insert malicious code and wreak havoc on systems, but they can also alter or steal information. Therefore, the campus must manage its technology and infrastructure to mitigate these risks.

Protecting the security, integrity, and confidentiality of information, as well as mitigating the risks associated with unauthorized access, is a campus priority. These guidelines are intended to help users meet established network bandwidth allocations and traffic standards to ensure that all University network and technology resources are managed securely.

2 Definitions

Bandwidth – The amount of data traffic that can be transmitted over the network at any given time.

Bandwidth Allocation – Shaping or sizing the amount of bandwidth allocated to individual network users, ensuring that all network users are able to obtain their fair share of resources and preventing noticeable congestion during peak usage periods

Computer Servers – Includes Web, application, electronic mail, file, and print servers located in the University's data centers, offices, student labs, classrooms, special service areas, colleges, schools, divisions, and departments throughout the campus

Information Technology Systems – All University owned and managed computers, peripherals, and related equipment and software; voice and data communications infrastructure, peripherals, and related equipment and software; all associated tools, instruments, and facilities; classroom technologies; and computing and electronic communications devices and services – e.g., PBX, modems, phones, facsimile machines, multimedia, voice mail, electronic mail, message boards, and other related devices or technologies

Information Technology Services (ITS) Change Advisory Board – A team of ITS compliance and technical members that reports directly to the Chief Technology Officer, and that reviews and evaluates Firewall Modification Requests, recommends new network safeguards, audits security patches and fixes for compliance, monitors current security threats, and responds to intrusions

Network Protocols – Acceptable network transmission applications and services that are identified as appropriate for inbound and outbound communications, and that support the educational, research, and service mission of the University (Note: Network protocols determined to be harmful are prohibited because they may cause problems that jeopardize the integrity, functionality, and safety of information technology systems.)

Risk, Critical – Any event that requires an immediate response because: a) damage to a system or data is occurring; b) attempts to exploit - a vulnerability on that system are occurring; or c) a vulnerability is being exploited on other similar technologies within the University

Risk, High – Any event that requires a response within 24-hours because: a) a vulnerability is known to exist on a University system; or b) a vulnerability is being exploited on a University system against another system outside the University

Risk, Moderate – Any event that requires a response within 48-hours because: a) the system is susceptible to attack or intrusion due to incorrect configuration; and b) there is a potential for damage to systems or data

Risk, Low – Any event that requires a response within 72-hours because: a) the system is susceptible to attack or intrusion due to incorrect configuration; and b) damage to systems or data is possible, but not considered likely

Security Breach – Any successful unauthorized access to, or use of, a Cal State L.A. computer, system, or network

Third Party – Any vendor, consultant, or union representative who requires temporary access to Cal State L.A. systems or data to perform services outlined in a CSULA purchase requisition or contract between the third party and Cal State L.A., the California State University, or a CSU bargaining unit

3 Guidelines

3.1 Confidentiality and Privacy of Network Communications

a) The network infrastructure is the property of Cal State L.A., as are the communications that traverse it. All network communications are treated as confidential.

b) Users of campus computing resources should have no expectation of privacy with regard to electronic information that is transmitted over, uploaded to, downloaded from, or stored in University systems or facilities.

c) Requests from any individual, agency, or organization to obtain the content of Cal State L.A. network communications shall be directed to the University Counsel.

d) The University will examine or disclose network communications content only: a) when authorized by the content owner; b) when required to evaluate or adjust network traffic to ensure effective operation; or c) when directed by University Counsel or the Internal Auditor.

e) Investigations requested by the University Counsel or the Internal Auditor will be performed: a) when there is evidence or reason to believe that a violation of University computer security, FERPA, or state or federal laws, statutes, and regulations is occurring or has occurred, b) the health or safety of people or property is involved, or c) when legal obligations and responsibilities require it.

f) Students are prohibited from having access to faculty or staff computers, or faculty or staff user IDs, passwords, or authorization codes.

3.2 Acceptable Network Traffic and Usage

IMPORTANT

Exceptions to network constraints and remote access may be requested using the Firewall Modification Request to secure a private network or data, or to enable course- or business-related applications. See section 4 for more details.

a) Unauthorized access to a campus network is prohibited.

b) Authorized campus users and guests must use their assigned network accounts to connect to the campus wired or wireless networks. The level of any user's access is determined by the permissions granted to the assigned account.

c) Students, faculty, staff, third parties, and sponsored guests are expected to comply with all laws, policies, and user guidelines that govern access to and use of the University's networks, accounts, and data.

d) All communication using campus networks must be appropriate, ethical, professional, and lawful.

e) Use of a wireless or other device to form a bridge (connection) or act as a hub between the University's wired and wireless networks is prohibited.

f) Unauthorized peer-to-peer file sharing of copyrighted works, including music, pictures, movies, games, and other published copyrighted materials is prohibited. It is the user's responsibility to ensure that downloaded or uploaded files are not copyrighted works, and, if they are, to obtain permission from the copyright holder before downloading or uploading the files.

g) Unauthorized Web services from campus computers for external use are prohibited.

h) Use of computers as unauthorized servers is prohibited. Such use increases the possibility of intruders downloading illegal software onto the computer and conducting disruptive or illegal functions in the background.

i) Computers and laptops connected to the campus network while simultaneously operating with any form of modem is prohibited. Such use increases the risk of intrusion to the campus network.

j) Access from the Internet to workstation computers, laptops, servers, printers, or other network communications devices that access or store personal, confidential, or fiscal data without the necessary security precautions in place is prohibited. Contact IT Security and Compliance to ensure your device has the proper security measures implemented before making it accessible from the Internet.

k) Network bandwidth constraints will be deployed immediately in the event of excessive bandwidth utilization, and will remain in place until corrective action determined and implemented.

l) ITS is responsible for assignment and management of all Internet Protocol (IP) addresses for Cal State L.A.

m) All remote network access to the campus network must be through a CSULA wireless network connection or the campus Virtual Private Network (VPN), which provides a secure encrypted connection to the campus network, including full Outlook functionality, over the Internet.

NOTE

Network users with broadband service may download and install VPN software on their off-site computer(s) from http://www.calstatela.edu/its/techsupport/vpn. Instructions for loading and using the software are available at this site. Outlook Web Access (OWA), which provides most of the same functionality as the full Outlook client program, is available on the Internet for those users who do not want to use VPN. This secure e-mail Web site is located at: http://email.calstatela.edu.

n) All computers that access the campus network must be running up-to-date anti-virus software.

NOTE

Users with campus-issued laptops and Internet access will receive automatic anti-virus updates. Other laptop users must ensure that the most up-to-date anti-virus software is protecting their computer before logging on to the campus network.

o) ITS will establish a separate private network with no external Internet access for departments when campus services (e.g., cash registers or cash terminals) or data (e.g., medical, financial, or police records): a) do not require access from any person outside the department, b) may require enhanced security administration due to the nature of the information, or c) may represent a possible target for intruders. In special circumstances where outbound traffic is required from these private networks, the outbound traffic will be restricted to e-mail and Internet access only.

p) Non-University supported instant Messaging (IM) on a campus network is prohibited. IM increases the campus's risk for virus infections, vulnerability to hacker intrusions, and potential for legal liability.

q) Internet Relay Chat (IRC) on a campus network is prohibited. IRC increases the campus's risk for hacker intrusions and consumes extensive network bandwidth that interferes with legitimate campus business.

r) Internet games on a campus network are prohibited because they are not University-business related.

s) Academic Support should be involved in the planning and execution of new network applications for academic network users to identify special communications requirements and ensure seamless continuity of work.

t) Users must report critical or high risk security incidents within fifteen (15) minutes of discovery to IT Security and Compliance at 323-343-2600, and by e-mail to itsecurity@calstatela.edu.

4 Terms, Conditions, and Sanctions

4.1 Violations

a) Any violation of these guidelines and network protocol policies will result in the immediate loss of connectivity for the system or device in violation, and may result in a loss of connectivity for other systems or devices as well. Systems and devices include, but are not limited to, computers (workstations and laptops), servers, routers, switches, or devices connected to the network.

b) Repeat violators, who through negligence, misconduct, or willful disregard, take inappropriate or unapproved actions that jeopardize campus networks or systems, will lose their connectivity privileges for an extended period of time or permanently. In addition, instances of repeat violations will be reported to the appropriate administrator/manager, Human Resource Management, University Counsel, and the appropriate Vice President for review and possible disciplinary action as provided by statute, including, but not limited to, Education Code section 89535.

c) IT Security and Compliance will conduct periodic audits of network traffic to ensure that user conduct meets the requirements of these guidelines, and that no unauthorized or potentially dangerous traffic is passing through the campus network.

4.2 Incidents and Intrusions

a) If a system or device is disconnected from a campus network due to a compromise, intrusion, or bandwidth constraint, in most cases service will be restored once the system or device is reconfigured to adhere to network traffic protocol policies.

b) In the event of a critical or high risk incident or intrusion, affected or suspected ports immediately will be shut down, the user(s) notified, and a status message posted to the ITS Alerts Web page (http://www.calstatela.edu/its/alerts), Ports will be reopened as soon as it is safe to do so.

c) In the event of a moderate or low risk event, computer users will be contacted prior to removing affected computer(s) from the network.

d) For computers that are, or believed to be, compromised or corrupted, do the following:

If the computer:	Immediately Contact
Contains personal, confidential, or proprietary data	IT Security and Compliance (323) 343-2600 See section 5 below for more details.
Does <u>not</u> contain personal, confidential, or proprietary data	Contact your ITC

The subject computer(s) will be removed from the network immediately to avoid spread of the problem. The incident will be fully investigated, referred to the appropriate technical, administrative, and executive personnel. Depending upon classification of data stored on the computer and the nature of the compromise, the machine will be will be fully examined, backed up, cleaned, re-imaged, and reconnected to the network as quickly as possible.

4.3 Network System Administrator Access

a) System security administrators who misuse their access privileges will automatically lose them. Any misuse of system administrator accounts may result in disciplinary action or dismissal as set forth by statute, including, but not limited to, Education Code section 89535.

b) All applications for security administrator access must include a confidentiality agreement.

c) Network system administrators may not be assigned a generic user or group log-on ID (e.g., “administrator” or “sysadmin”).

d) Network system administrator IDs must be constructed in such a manner that University logs can identify an individual administrator (e.g., sysadmjdoe or JohnDoeadmin).

4.4 Third Party Network Access and Usage

a) Third party accounts that access any campus computing or network equipment must be approved by the hiring department chair or manager, dean or director (or the executive director of UAS when appropriate), the Director of IT Security and Compliance, the Director of IT Infrastructure Services, and the Vice President for ITS and CTO.

NOTE

Requests for network and network/e-mail accounts for third parties should be made using the Third Party Vendor/Consultant Network Access Request form located online at: http://www.calstatela.edu/its/forms.

b) Written contracts or agreements with third parties who request access to a campus network must address security measures, confidentiality, hold harmless statements, scope of work, and other parameters or contingencies to ensure integrity and security of University systems and data.

c) Third parties must have a current purchase requisition or contract on file in the Procurement and Contracts office prior to their network access request being approved. In the case of union representatives, a union unit contract must be on file in the Human Resources Management office.

d) Third parties must request access to a particular network system for routine maintenance, troubleshooting, or incident investigation at least 72 hours prior to the scheduled work.

NOTE

Third parties must use the most appropriate third party request form available online at http://www.calstatela.edu/its/forms to make this request.

e) Third parties must sign a confidentiality and appropriate use of access agreement prior to being approved for any type of access to any network, e-mail, or system.

f) Third parties must be supervised by an appropriate University administrator.

g) To ensure that all networked machines are maintained in accordance with University security procedures, all units built, repaired, or otherwise accessed by third parties may not be added or returned to network operation until cleared by IT Security and Compliance.

h) Third parties' access codes must be changed or locked immediately upon completion of the contracted work.

4.5 Requesting Firewall Modifications and Assistance with New Network Communication Projects

a) To ensure uninterrupted essential services (such as Web CT, PeopleSoft, CMS, etc.), better network service, and adequate bandwidth for each specific application, network users and departments must work with ITS in planning upcoming projects that require special or off-campus network communications. Submitting a Firewall Modification Request form starts this process.

b) Use the Firewall Modification Request form (available online at http://www.calstatela.edu/its/forms when any one or more of the following are required:

- A department project for off-campus network communications
- A departmental web application for off-campus access
- A server-based application within a department
- A secure private network is needed for University business reasons and to protect data

c) The ITS Change Advisory Board will review Firewall Modification Requests within five business days of receipt, and promptly will notify requestors of its determinations. If the board does not approve the request, it may provide the user with specific security vulnerabilities or lapses that could occur by allowing the requested access and usage. In these cases, ITS will work with departments to develop secure and acceptable alternatives.

d) The ITS Change Advisory Board will perform periodic audits of all network traffic to ensure there are no violations of recommended safe communications protocols.

5 Contacts and Resources

a) Report critical or high risk security incidents within fifteen (15) minutes of discovery to IT Security and Compliance at 323-343-2600, and by e-mail to itsecurity@calstatela.edu.

b) Report low or moderate risk security incidents to the ITS Help Desk, LIB PW Lobby, or (323) 343-6170.

c) Report network access problems or a loss of network service to the ITS Help Desk at (323) 343-6170.

d) Direct questions regarding these guidelines to itsecurity@calstatela.edu.

e) Locate ITC contact information at: http://www.calstatela.edu/academic/aa/ess/itc/

6 Related Documents

ID/Control #	Title
ITS-8812	**Firewall Modification Request** http://www.calstatela.edu/its/forms This form is used to request exceptions to the campus firewall policies.

ID/Control #	Title
ITS-4818	**Network Guest Account Request** http://www.calstatela.edu/its/forms Sponsors may use this form to request temporary access up to seven consecutive days to equipment (e.g., in a Technology Enhanced Classrooms (TEC)) or to the Internet for a guest auditor or guest lecturer or speaker/presenter. (See form for further details.)
ITS-8828	**Third Party Vendor/Consultant Network Access Request** http://www.calstatela.edu/its/forms This form is used by third parties to request a network or network/e-mail account.
ITS-1015-G	**User Guidelines for Wireless Access** http://www.calstatela.edu/its/policies Guidelines, terms, conditions, sanctions, and contacts regarding wireless access to the campus network.
ITS-4815	**Wireless Guest Account Request** http://www.calstatela.edu/its/forms Sponsors may use this form to request temporary wireless Internet access up to seven consecutive days for guests.