

California State University, Fullerton Division of Information Technology

Security Practices and Standards for All University Networks and Network-attached Systems

September 2, 2003

I. Statement of Purpose

The computer communications network is a resource critical to the mission of our university. Faculty, staff and students depend on a reliable and secure network to protect the efficiency, integrity and confidentiality of information. As required by CSU Policy, the CSUF Division of Information Technology (IT) is implementing security responsibilities and security practices and standards to protect the integrity and confidentiality of the university's computer networks and network-attached systems (computer workstations, computer servers, printers, wireless systems, and other network-attached items/systems) and to diminish the impact when a network or network-attached system is compromised by computer intrusions, worms, viruses, and/or other malicious misuses.

II. Applicability

The international security problems with hackers and with viruses, worms, and other hostile software are well known. A robust and secure network is essential to the functioning of modern universities. Without standardized and up-to-date security processes, the Titan Network cannot exist. As such, being connected to the Titan Network is a privilege permitted only to those who accept responsibility for and adhere to *Cal State Fullerton IT Division: Minimum Required Security Practices and Standards* (see Appendix A). All of these practices and standards must be adhered to in order for computer networks and network-attached systems to become and remain connected to the university's networks. The security practices and standards will be reviewed and updated as needed and at least annually. The security practices and standards apply to all persons (students, faculty, staff, vendors, contractors, guests, visitors, and volunteers) including end-users and those who maintain the computer networks and/or network-attached systems on any and all of the university's networks (regardless of their location or custodial status). That is, state-owned, auxiliary-owned, contractor-owned, contractor/vendor-operated, leased, donated, or otherwise acquired systems are covered by these security practices and standards if the computers, servers, or other network devices that utilize the university's networks or university's systems.

III. Requirement for IT's Security Team to Have Administrative Access and Controls on Networks and Network-attached Systems Connecting to Any of the University's Networks

For any system to become connected and remain connected to the university's networks, the Division of Information Technology's Security Team requires *administrative access and controls* to the systems attached to all Titan networks in order to perform security audits and apply corrective measures. In order to reduce computer vulnerabilities, any systems which do not allow administrative access and controls may be immediately disconnected without notice. In addition, IT has the authority to disconnect systems that are considered a threat to others.

It cannot be said strongly enough that the purpose of this requirement is only to perform critical security audits and corrective measures to protect confidential information and assure correct security controls are in place.

Any exceptions to this requirement must be approved by the Chief Information/ Technology Officer on a fiscal year basis.

Note: The Division of Information Technology's Security Team staff is subject to all campus, state and federal requirements to ensure the security and protection of confidential data. Staff must undergo fingerprinting and background checks to establish and maintain a position on the Security Team.

IV. Computer Technical Support Staff Responsibilities

All computer technical staff who design, manage and operate campus electronic information resources must comply with this document and the detailed security standards and practices as provided in Appendix A. The campus technical support community must meet the following conditions:

- The "Rollout" workstations are to be administered *only* by the IT Help Desk staff.
- Any and all systems attached to the university's networks require prior notification to the help desk and must name specific technical and administrative contacts for the equipment. 24-hour contact information must be made available to the help desk and kept current. The technical and administrative contacts must be permanent, full-time, 12-month employees who can be contacted 24-hours a day, 7 days a week, when problems are encountered with those specific resources. These named contacts must themselves register with IT's Security Team and provide current contact information. It is the responsibility of the contacts to update IT's records *within 3 days* when contact information or staff changes occur. This includes "non-centralized resources" that are not serviced by the division of Information Technology. Examples -- College- or department-specific computing labs, faculty-maintained servers, laptops not provided by IT, etc. (We realize that students, part-time staff and contractors provide a valuable service to the campus community with respect to our Web presence and information technology capabilities, however, *we cannot expect them to assume responsibility for safeguarding those resources*. As such, each division/college/department or other unit must provide the name(s) of a responsible person(s) and must also provide a means by which that individual can be contacted at any time during the day or night when problems arise.)
- Maintain current anti-virus software on all network-attached systems.
- Become knowledgeable and implement Appendix A requirements
- Analyze potential threats and the feasibility of various security measures
- Implement security measures that mitigate threats.
- Provide this document to vendors/contractors and coordinate the vendors'/ contractors' conformance with the document.
- Assure that activities outsourced to off-campus entities comply with this document and any updates to the standards and practices.
- Establish procedures to ensure that privileged accounts are kept to a minimum and that privileged users comply with privileged access agreements.
- Be available for contact by IT when a security issue arises.

- Computers must have the most recently available and required software security patches. Exceptions must be approved by the Chief Information/ Technology Officer on a fiscal year basis.
- University-approved authentication and authorization functions must be implemented on all systems attached to the university networks.
- All installations must be configured to minimize security risks/ potential intrusions.
- Appropriate controls must be employed to protect physical access to resources (e.g., doors and locks).

V. End-User Responsibilities

End-users have a personal responsibility to maintain reasonable security on computers they use. End-users should avoid installing software that can compromise the security of the computer systems they use. End-user systems considered a threat to others may be disconnected without notice.

Those authorized to obtain confidential data must ensure that it is protected in accordance with applicable laws and policies. Systems not in compliance and considered a threat to confidentiality of information may be disconnected without notice.

VI. At-Home and remote Users Responsibilities / Internet Connectivity

Users who simply access email via <http://email.fullerton.edu> (Outlook Web Access), the portal at <http://mycsuf.fullerton.edu>, or business services through <http://uam.fullerton.edu> should make it a regular practice to check for anti-virus updates and critical updates, specifically, for Microsoft Windows systems, weekly updates from <http://windowsupdate.microsoft.com> are highly advisable to protect your own system and data.

Information Technology will provide a virtual private network (VPN) solution for remote access to university networks and network-attached systems so that higher speed users (cable and DSL users) will have a means to access the university.

All users who connect to the university networks for any other applications (Host Explorer--SIS+, remote file sharing, Outlook email (*not Outlook Express*), remote control software, and other database applications) must use VPN software that IT Helpdesk will provide to connect to the campus. Before connecting the at-home users must ensure the following has occurred:

- Make weekly updates to anti-virus software
- Ensure that home computer operating system is patched at current vendor software patch levels. Specifically, for Microsoft Windows systems, weekly updates from <http://windowsupdate.microsoft.com>.

=====

APPENDIX A -- Security Practices and Standards

Network-attached systems will be required to comply with the following detailed Security Practices and Standards as specified below. These security practices and standards will be reviewed and updated on at least an annual basis.

Immediately as of September 9, 2003, the following standards and practices are required:

- All Microsoft-based network domain settings must enforce password complexity.
- Password expiration must occur on all accounts except those used in automated processes. Automated Processes accounts must change passwords every year on a fiscal year basis.
- Campus-licensed Anti-virus software and current definitions must be running and updated weekly using campus-licensed McAfee EPO (Electronic Policy Orchestrator).
- Campus-licensed St. Bernard Update Expert will be run against all Microsoft domains.
- Department run domains will be required to run Update Expert against locally administered computers on a monthly basis.
- Microsoft-based computers not in the centrally administered domain must:
 - Run Microsoft Baseline Security Analyzer and repair "critical" problems
 - Install vendor recommended "critical" security patches
 - Make vendor recommended "critical" security settings
- Other settings limiting anonymous access will be required to be on all computers.

The following standards and practices are scheduled for compliance by all areas beginning July 16, 2004 (by the midpoint of summer 2004 session). The campus technical community must complete migration to the Active Directory domain before this date.

- No Microsoft Windows domain shall exist outside of the university Active Directory domains (AD or ACAD) unless authorized by the Chief Information Officer on an annual basis. The campus technical community must complete migration to the Active Directory domain before July 17, 2004.
- Minimum Hardware and Minimum Software Requirements will be forthcoming which will limit what may remain connected to the university's networks. For example, some workstations may be determined to be too antiquated to be connected to the campus network and left OFFLINE to use as stand-alone systems.

REFERENCES

- CSU Security Policy, effective 9/20/2002.
http://its.calstate.edu/systemwide_it_advisory/ITAC_keydocuments/IT_Security_Policy_092002.doc
- Article 1, Section 1, of the Constitution of the State of California, defines pursuing and obtaining privacy as an inalienable right.
- The Comprehensive Computer Data Access and Fraud Act (Calif. Penal Code Section 502) affords protection to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer information systems. It allows for civil action against any person convicted of violating the criminal provisions for compensatory damages.
- The Information Practices Act of 1977 (Calif. Civil Code Section 1798, et seq.) places specific requirements on State agencies in the collection, use, maintenance and dissemination of information relating to individuals.
- The California Public Records Act (Calif. Government Code Sections 6250-6265) provides for the inspection of public records.
- Title V Section 42396.2(d) of the California Code of Regulations confirms the right to privacy in California and states an intent to implement it within the CSU.
- The Family Educational Rights and Privacy Act (20 U.S.C. Section 1232g) (commonly referred to as FERPA or the Buckley Amendment) is a federal statute applicable to every institution which receives federal funds. It protects students (and former students) from the release of personal information about them. It provides for the right of a student to inspect and review his or her own education record, the right to request the records be amended, and the right to some control over the disclosure of personally identifiable data from such records.