CSULB COMPUTER USAGE AND SAFETY GUIDELINES

Table of Contents

Using Campus Technology Resources

Technology has become an integral support component in all areas of CSULB. The campus recognizes the importance of technology and its role in the academic mission of the campus as well as its administrative services. The campus policy on ***Acceptable Use of CSULB Electronic Communications Systems and Services*** states:

> "Electronic communications systems and services are essential to conducting University business. The continued and reliable availability of these systems and services are paramount to California State University, Long Beach's (University) ability to fulfill its mission of education, research, and public service. To this end, the University uses, supports and provides electronic communications systems and services for telecommunications, mail, education, and research.
>
> The University encourages the use of electronic communications systems and services for lawful purposes and makes them widely available to the university community. Nonetheless, the use of electronic communications resources is limited by restrictions that apply to all University property and by constraints necessary for the reliable operation of electronic communications systems and services. The University reserves the right to deny use of its electronic communications systems and services, when necessary, to satisfy these restrictions and constraints. " [1]

The campus has established ***policy governing access to and use of CSULB computing resources***[2] and supports ***information security policies, procedures and standards*** to ensure safe computing.[3] The campus Information Security Management and Compliance mission states:

> "California State University, Long Beach (CSULB) recognizes it's affirmative and continuing obligation to protect the confidentiality, maintain the integrity, and ensure the availability of information about and used by CSULB faculty, staff, students and customers and to provide administrative, technical and physical safeguards to protect university information assets. The CSULB Information Security and Privacy Program provides the framework and the Information Security Management and Compliance office provides assistance to the University for meeting its responsibilities by:
>
> - Developing University policies, standards, and procedures regarding the acquisition, transmission, processing, maintenance, safeguarding, release, and disposal of personal and confidential information and other CSULB sensitive data;
> - Developing and providing appropriate training and informational materials; and
> - Assessing and ensuring University compliance with program related laws, regulations, CSU and CSULB policies, standards and procedures."[4]

[1] http://daf.csulb.edu/offices/vp/information_security/policies/elec_comm_sys.html
[2] http://www.csulb.edu/divisions/aa/grad_undergrad/senate/documents/policy/1996/18/
[3] http://daf.csulb.edu/offices/vp/information_security/policies/index.html

University and Personal Computing Equipment

University equipment shall not be used for any purpose related to outside employment, non-university consulting, personal business, or any activity outside of university employment. Such misuse of university resources for personal gain or interest could constitute an unauthorized use of State funds or raise conflict of interest questions. Faculty and staff are not permitted to install or load personal software on university computing equipment.

Ensuring Technical Security

Computer security is the process of preventing unauthorized use of your computer or theft of confidential data as well as sensitive personal information which includes but is not limited to such data as social security number, email address, home address or employee ID.

Preventative measures help block unauthorized users (also known as "intruders") from accessing any part of your computer system and prevent personal information from being inadvertently altered or destroyed.

Computer security is necessary for all CSULB users, whether you are computing on campus, remotely from a University-owned system or connecting to the network from your own personal computer.

Why is computer security important?

The campus has a responsibility to ensure computing resources are secure and that data is protected. The campus is responsible for complying with laws surrounding security of information and computing resources, including but not limited to:

- California Information Practices Act; California Civil Code §1798-1798.78
- Employee Access to Information Pertaining to Themselves; California Education Code §89546
- California Code of Regulations, Title V, § 42396-42396.5
- Gramm-Leach-Bliley Act; FTC-15USC Subchapter I, §6801-6809 & Subchapter II, §6821-6827
- Family Educational Rights and Privacy Act (FERPA) also known as the "Buckley Amendment," Statute: 20 U.S.C. 1232g; Regulations: 34 C.F.R. Part 99
- United States Copyright Act of 1976 (17 U.S.C.), and amendments including the Digital Millennium Copyright Act (DMCA).

Users of campus technology assets must abide by guidelines to ensure the security of the University data network and all the machines that connect to it. These guidelines help minimize risk of compromised network, devices, and personal data. Devices that connect to the CSULB network, whether university purchased or personal, need to meet a minimum level of security to ensure the stability and security of university systems.

[4] http://daf.csulb.edu/offices/vp/information_security/mission.html

Safe Computing

Access to Your Workstation

Allowing anonymous or guest access to your computer is *never* recommended. User access is allowed only through a single unique username and password. Administrative access is provided to campus technical support staff and required to ensure the computer is kept secure and software is kept current. All users of campus information systems or network resources are advised to consider the open nature of information disseminated electronically and must not assume any degree of privacy or restricted access to information they create or store on campus systems.[5]

Anti-virus Protection

In order to meet campus security guidelines, university computers must have university provided Symantec Endpoint Protection (SEP) software installed. Symantec Endpoint Protection is licensed for Windows and Macintosh computers for the campus and will proactively protect these machines . In addition to detecting and removing dangerous viruses, worms, and Trojan horses, Symantec Endpoint Protection automatically blocks spyware installation and detects and removes stealth spyware.

Campus technology coordinators have the ability to install and configure university provided antivirus software onto university computers. Only university provided antivirus software shall be installed. Conflicts can occur when multiple antivirus software runs concurrently and non-university software is not allowed to be installed on university provided computers.

Computer Disposal and Sanitization

Prior to the survey and disposal or a campus computer, or transfer of a computer from one user to another, the computer's hard drive shall be wiped according to campus media sanitation procedures. The campus has a policy on electronic media sanitation. [6]

Email Safety

One of the most prevalent threats to users and university data is email phishing. Phishing is an illegal attempt to fraudulently acquire confidential information, such as usernames, passwords, or credit card details by masquerading as a trusted business or organization in an email communication.

[5] http://www.calstate.edu/icsuam/sections/8000/8025.0.shtml

[6] http://www.csulb.edu/misc/adminguidelines/pdf/Information%20Security/mediasanitization_07-mar.pdf

Only open email from senders you recognize and never open unknown attachments. If you receive such email, simply select it, delete it and empty your trash. It's important to note that university help desk staff will never ask you for your password via email.

File Sharing Software

Use of any university resource such as computers (hardware or software), network connections, servers, routers, facsimile machines, copy machines and other electronic equipment by any university constituent (faculty, student, staff or general public) to circumvent legitimate copyright protections or illegally access, copy or disseminate copyrighted material is unacceptable.[7]

Unauthorized applications such as file sharing programs run the risk of exposure to unauthorized access. This type of software may contain "malware," such as spyware or other programs that compromise security and privacy.

Locking or Logging Out

Always lock or log out when you walk away from your computer – no matter how long you will be gone. It takes only seconds for someone to view or load confidential data. The campus has a policy on clean desk and clean computer screens. [8]

Password Protection

Password protection is one of the simplest and most effective steps in practicing good computer security. Guard yourself and your computer by following some basic guidelines:

1. *Never* share your password. Write it down and keep it in a safe place not easily accessible by anyone.
2. *Never* use a single word as your password, i.e., your street or dog's name. These are very easy to guess, even when numbers are added.
3. *Always* use mixed characters like upper and lower case letters and numbers or symbols. A good example: Washth3dog!
4. *Always* use a pass*phrase* instead of a pass*word*. These are easy to remember and contain more characters making them more difficult to guess. A good example: V1vaLasV3gas!
5. *Always* change your passphrase regularly. In the event someone does obtain access to your password, access will be cut short once you reset it.

[7] Office of the Chancellor Executive Order 999, 2007

[8] http://daf.csulb.edu/offices/vp/information_security/policies/clean_desk_clean_screen.html

Strong Passwords

Campus domain and CMS password policies mandate using strong passwords that follow the criteria below.

- Must not have been used as your previous five (5) Active Directory passwords
- Must not contain your full name or Active Directory user name
- Must be at least 8 characters
- Must contain at least three (3) of the following four (4) character types:
- Uppercase letters (A through Z)
- Lowercase letters (a through z)
- Numbers (0 through 9)
- Special characters (such as: !, $, %, #)

Software Updates

As software is revised by manufacturers, improvements are made to fend off threats to its security and performance. One way to fight exposure to these threats is to keep your software current. Effective desktop security begins with ensuring the desktop system software is properly installed and contains the latest patches and anti-virus definitions.

- University deployed systems will come preloaded with current operating system software versions, proper antivirus software, and undergo ongoing updates automatically and/or by campus technical staff .
- It is essential that home users never install “freeware” software, as it often contains malware or spyware that can compromise the home deploy system and University systems.
- All University deployed home laptops must have PGP encryption software installed and users will enroll in full disk encryption.

Remote Computing and Virtual Private Network (VPN)

Software such as pcAnywhere and GoToMyPC is not allowed because the university offers a Virtual Private Network (VPN) for remote access.

To safely access campus network resources from a remote location (like your home), use the Virtual Private Network (VPN). VPN creates a secure virtual pipeline between your computer and the University. Once logged in, you have access to campus resources, just as if you were logged on physically onsite.

Please contact Information Technology Services at (562) 985-8344 or VPN Service for more information and detailed instructions on VPN services.

Pretty Good Privacy (PGP)

If your position requires you to save sensitive information to your computer, make sure it is appropriately secured using Pretty Good Privacy (PGP) encryption. In the event of a computer's physical theft, your data will be protected.

Please contact Information Technology Services at (562) 985-8344 for more information and to learn how to obtain PGP software.

Security Checklist for Desktop and Laptop Users

Use the checklists below to follow good computer security habits, as well as to ensure the general security of your device:

Operating System

- □ I am running at the latest available operating system patches and fixes.
- □ I am not running the operating system as Administrator.
- □ I chose a strong password to log in to my computer.

Automatic Updates

- □ Updates are set to automatically download and install from the operating system vendor.
- □ I understand that the major operating system vendors will never send out updates and patches, or announcements about updates and patches, via email.

Anti-Virus

- □ I have anti-virus software installed and running.
- □ My anti-virus software is made by this company: _____.
- □ My anti-virus software automatically updates itself.
- □ My anti-virus software automatically scans my computer for viruses.
- □ My anti-virus software automatically scans my IM (instant messaging) software.

Email

- □ I never open attachments unless I am expecting them.
- □ I never open attachments that are programs (files that end with .bat, .chm, .cmd, .com, .exe, .hta, .ocx, .pif, .scr, .shs, .vbe, .vbs, or .wsf).
- □ I never respond to spam, even to "unsubscribe." I understand that AOL, eBay, PayPal, my bank, and other web sites related to my money will never send out requests for passwords, PINs, or other sensitive information via email.

The Internet / Web Browser

- □ I understand that advertisements on web sites warning me that my computer can be hacked or fixed should be ignored; if I am concerned, I will ask someone with IT knowledgeable.
- □ When I buy online, I make sure that sensitive information is entered only on secure pages (https). Secure web sites usually display a small graphic image of a locked padlock at the bottom of the screen or within the url bar next to the website address.

Appendix A: Policy Governing Access To and Use of CSULB Computing Resources – Table of Contents

http://www.csulb.edu/divisions/aa/grad_undergrad/senate/documents/policy/1996/18/

Approved by CSULB Academic Senate in May 1996 and by President Maxson in August 1996
Paper copies of this document are available from the Academic Senate office.

Appendix B: Policy Governing Acceptable Use of CSULB Electronic Communications Systems and Services

References: **Executive Order 999: Illegal Electronic File Sharing and Protection of Electronic Copyrighted Material**
Issue Date: **August 2007**
Revision Date: **N/A**
Expiration Date: **N/A**

Web Links:
http://www.calstate.edu/EO/EO-999.html
http://daf.csulb.edu/offices/vp/information_security

POLICY STATEMENT

Electronic communications systems and services are essential to conducting University business. The continued and reliable availability of these systems and services are paramount to California State University, Long Beach's (University) ability to fulfill its mission of education, research, and public service. To this end, the University uses, supports and provides electronic communications systems and services for telecommunications, mail, education, and research.

The University encourages the use of electronic communications systems and services for lawful purposes and makes them widely available to the university community. Nonetheless, the use of electronic communications resources is limited by restrictions that apply to all University property and by constraints necessary for the reliable operation of electronic communications systems and services. The University reserves the right to deny use of its electronic communications systems and services, when necessary, to satisfy these restrictions and constraints.

The contents of all electronic communications systems and services shall conform to CSU and CSULB policies and standards, state law and federal law including the Copyright Act of 1976 and all subsequent amendments including, but not limited to, the Digital Millennium Copyright Act of 1998 and the Teach Act of 2002.

All electronic communications systems and services intended to accomplish the academic and administrative tasks of the University shall be accessible to users with disabilities in compliance with law and University policies. Alternate accommodations shall conform to law and University policies and standards.

GENERAL PROVISIONS

PURPOSE

The purposes of this policy are to:

Ensure that University electronic communications systems and services are used for purposes appropriate to the University's mission;

Ensure that User's privacy rights are protected;

Inform the University community about the applicability of laws and standards to electronic communications;

Ensure that electronic communications system and services are used in compliance with those laws and standards; and

Prevent disruption to and misuse of University electronic communications systems and services.

SCOPE

This policy applies to:

All electronic communications systems and services, owned or managed by the University or auxiliary organizations;

All electronic communications systems and services provided by the University or auxiliary organizations through contracts or other agreements;

All users and uses of University electronic communications system and services ; and

All University electronic communications records in the possession of University employees or of other users of electronic communications system and services provided by the University.

DEFINITIONS

Terms used in this Policy are defined below.

INCIDENTAL USE

University users may use electronic communications systems and services for incidental personal use provided that such use does not 1) interfere with the University's operation of electronic communications systems and services; 2) interfere with the user's employment or other obligations to the University; 3) burden the University with noticeable incremental costs; or 4) create a security risk to the confidential or intellectual information maintained and protected by the University. When noticeable incremental costs for personal use are incurred, users shall be responsible for reimbursement to the University.

PROHIBITED USE

Users are prohibited from utilizing University electronic communications systems and services for any unlawful, unethical or unprofessional purpose or activity. Examples of prohibited use include but are not limited to:

Transmission of threats, harassment or defamation

Download or distribution of material or programs that could be deemed harmful to University electronic communications systems or services

Violations of any state of federal laws or any applicable CSU or CSULB policy or regulation, including but not limited to, Rules of the Academic Senate, the Faculty Code, the Faculty Handbook and Administrative Guidelines

Intentional access, viewing, download or dissemination of materials containing obscene matter

Violation of software licensing agreements

Intentional damage to equipment, software or data

Commercial activities unrelated to the mission of the University. This includes soliciting, promoting, selling, marketing or advertising products or services (e.g. consulting services) or other revenue generating private business operations for personal financial gain. Disputes regarding a commercial activity's relatedness to mission of the University shall be resolved by the University President or designee.

Campus auxiliary organizations are authorized to provide services and products to students, faculty and staff, and invited guests of the University through operating and service support leases.

The University President or designee may authorize additional limited commercial uses under separate policy provisions and such uses are exceptions to the above commercial use prohibitions.

University electronic communications system and services may not be used to:

circumvent legitimate copyright protections or illegally access, copy or disseminate copyrighted material in any form including, but not limited to, print, music, video or other multimedia content, that is not permitted under the principle of Fair Use;

distribute or duplicate copyrighted software without appropriate licensing agreements or use of software in a manner inconsistent with the license; or

engage in peer-to-peer technology for non-business purposes. This includes, but is not limited to, transfer of music, movies, software, and other intellectual property.

Illegal file-sharing and other copyright violations are a violation of Title 5 of the California Code of Regulations.

PRIVACY

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications systems and services. This Policy reflects these firmly-held principles within the context of the University's legal and other obligations. The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations, while seeking to ensure that University administrative records are accessible for the conduct of the University's business.

Limitations of Privacy

It is not the intent of the University to examine or disclose electronic communication records without the holder's consent. However, under limited circumstances as described in this policy, the University may examine or disclose electronic communications records without the holder's consent.

An electronic communication holder's consent shall be obtained by the University prior to any access for the purpose of examination or disclosure of the contents of University electronic communications record in the holder's possession, except as provided below.

Access without Consent

The University shall permit the examination or disclosure of electronic communications records without the consent of the holder when (1) required by and consistent with law; (2) when there is substantial reason to believe that violations of law or of University policies have taken place; (3) when there are compelling circumstances; (4) under time-dependent, critical operational circumstances; or 5) to preserve records or information consistent with the University Litigation Hold policy.

Automated Monitoring

The right to privacy does not preclude system administrators from maintaining and monitoring system logs of user activity. Automated searches for files and transmissions that endanger privacy, confidentiality of data, system security or integrity are performed regularly to protect all users and ensure the continued availability of University electronic communications systems and services. System administrators may take appropriate actions in response to detection of such files or transmissions.

Third Party Services

University contracts with outside vendors for electronic communications services must explicitly reflect and be consistent with this Policy and other University policies related to privacy. Any third party organization providing contractors to the University shall be provided access to this policy for review prior to commencing work for the University.

SECURITY

The University makes reasonable efforts to provide secure and reliable electronic communications systems and services. The University cannot ensure security of data transmitted over the Internet. Information submitted via the Internet may not be secure and could be observed by a third party while in transit. Submission of passwords, credit card numbers or other personal information via the Internet could result in identity theft.

Additionally, University Users and Public Users accessing the Internet should be aware that the Internet permits access to non-University users who are not subject to University policies, and may contain content materials, goods and services that individual users may find personally offensive or objectionable. The University does not have the right or capability to monitor or restrict Internet content. Therefore, the University disclaims any responsibility and liability for any conduct, content, materials or goods and services available on or through the Internet.

RESPONSE TO POLICY VIOLATIONS

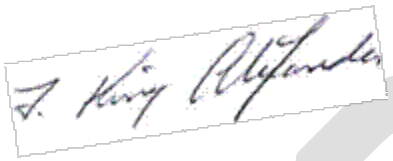
When there is reason to believe that a violation of this policy has occurred, an investigation shall be conducted. User access to electronic communications systems and services may be temporarily suspended while an investigation is being conducted.

If the investigation involves faculty or staff members and warrants University action, an explanation of the causal events shall be reported to the appropriate Vice President. In cases involving students, the Office of Judicial Affairs and the Dean of Students Office shall be notified. Investigating officials shall examine charges of violations with due respect for individual privacy, the security of other users, and the rights of due process.

Violations of University policy may result in sanctions, including but not limited to, limitation or revocation of access rights and/or reimbursement to the University for any expense related to the violation, including costs associated with the detection and investigation of the violation, as well as from the violation itself. Violation of applicable statutes may result in criminal prosecution.

Approved by President Alexander

August 2007



DEFINITIONS

Compelling Circumstances: Circumstances in which failure to act might result in significant bodily harm, significant property loss or damage, loss of significant evidence, or significant liability to the University or to members of the University community.

Electronic Communications: Any transfer of signals, writings, images, sounds, data or intelligence that is created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded displayed, viewed, read, or printed by one or several electronic communications systems. For the purpose of this policy, an electronic file that has not been transmitted is not an electronic communication.

Electronic Communications Records: The contents of electronic communications created, sent, forwarded, replied to, transmitted, distributed, broadcast, stored, held, copied, downloaded, displayed, viewed, read, or printed by one or several electronic communications systems or services. This definition of electronic communications records applies equally to attachments to such records and transactional information associated with such records.

Electronic Communication Resources: Telecommunications equipment, transmission devices, electronic video and audio equipment; encoding or decoding equipment, computers and computer time, data processing or storage systems, computer systems, servers, networks, input/output and connecting devices, and related computer records, programs, software, and documentation that supports electronic communications systems and services.

Electronic Communications Systems and Services: Any messaging, collaboration, publishing, broadcast, or distributions system that depends on electronic communications resources to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic records for the purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

Holder of an Electronic Communications Record or Electronic Communications Holder: An electronic communications user who, at a given point in time, is in possession or receipt of a particular electronic communications record, whether or not that electronic communications user is the original creator or a recipient of the content of the record.

Matter: Any book, magazine, newspaper, or other printed or written material, or any picture, drawing, photograph, motion picture, or other pictorial representation, or any statue or other figure, or any recording, transcription, or mechanical, chemical, or electrical reproduction, or any other article, equipment, machine or material.

Obscene Matter: Defined in Section 311 of the Penal Code as any matter, taken as a whole, that to the average person, applying contemporary statewide standards, appeals to the prurient interest, that, taken as a whole, depicts or describes sexual conduct in a patently offensive way, and that, take as a whole, lacks serious literary, artistic, political, or scientific value.

The prohibition regarding obscene matter does not apply to accessing, viewing, downloading, or otherwise obtaining obscene matter for use consistent with legitimate law enforcement purposes, to permit the university to conduct an administrative disciplinary investigation, or for legitimate medical, scientific, academic, or other legitimate university purposes.

Possession of Electronic Communications Record: An individual is in possession of an electronic communications record, whether the original record or a copy or modification of the original record, when that individual has effective control over the location of its storage or access to its content. Thus, an electronic communications record that resides on an electronic communications system awaiting download to an addressee is deemed, for the purposes of this Policy, to be

in the possession of that addressee. Systems administrators and other operators of University electronic communications system and services are excluded from this definition of possession with regard to electronic communication not specifically created by or addressed to them. Electronic communications users are not responsible for electronic communications records in their possession when they have no knowledge of the existence or contents of such records.

Substantial Reason: Reliable evidence indicating that violation of law or University Policy has occurred, as distinguished from rumor, gossip, or other unreliable evidence.

Time-dependent, Critical Operational Circumstances: Circumstances in which failure to act could seriously hamper the ability of the University to function administratively or to meet its teaching obligations, but excluding circumstances pertaining to personal or professional activities, or to faculty research or matters of shared governance.

University Electronic Communications Record: A Public Record in the form of an Electronic communications record, whether or not any of the electronic communications resources utilized to create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print the electronic communications record are owned by the University. This implies that the location of the record, or the location of its creation or use, does not change its nature (i) as a University electronic communications record for the purposes of this or other University policies, and (ii) as having potential for disclosure under the California Public Records Act.

Until determined otherwise or unless it is clear from the context, any electronic communications record residing on university-owned or controlled telecommunications, video, audio, and computing facilities will be deemed to be a University electronic communications record for purposes of this Policy. This includes personal electronic communications. Consistent with the principles of least perusal and least action necessary and of legal compliance, the University must make a good faith a priori effort to distinguish University electronic communications records from personal and other electronic communications in situations relevant to disclosure under the California Public Records Act and other laws, or for other applicable provisions of this Policy.

University Electronic Communications Systems and Services: Electronic communications systems and services owned or operated by the University, auxiliary organization or provided through contracts with the University or auxiliary organization.

Use of Electronic Communications systems and Services: To create, send, forward, reply to, transmit, distribute, broadcast, store, hold, copy, download, display, view, read, or print electronic communications with the aid of electronic communication systems and services. An electronic Communications user is an individual or organization who makes use of electronic communications services.

The act of receipt of electronic communications records as contrasted with actual viewing of the record by the recipient is excluded from the definition of “use” to the extent that the recipient does not have advance knowledge of the contents of the electronic communications record.

User: University students, faculty and staff, emeritus and employees of the University’s auxiliary organizations who have legitimate access University electronic communications resources. Users may also be persons or organizations who have legitimate access to University electronic communications resources under programs sponsored by the University and authorized by the University President.

Appendix C: Information Security Policy

http://daf.csulb.edu/offices/vp/information_security/policies/is.html

Issue Date: **April 2007**
Revision Date: **May 2009**
Expiration Date: **N/A**

POLICY STATEMENT

California State University, Long Beach (CSULB) recognizes its affirmative and continuing responsibility to protect the confidentiality, maintain the integrity, and ensure the availability of its information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the integrity of the mission of CSULB, violate individual privacy rights, and possible constitute a criminal act. It is the policy of California State University, Long Beach to ensure:

- confidentiality of personally identifiable information;
- integrity of data stored on or processed by CSULB information systems;
- availability of information stored or processed by CSULB information systems;
- maintenance and currency of applications installed on CSULB information systems; and
- compliance with applicable laws, regulations, and CSU/CSULB policies, standards, and procedures governing information security and privacy protection.

SCOPE

The CSULB Information Security Policy applies to:

Information assets that are acquired, transmitted, processed, transferred and/or maintained by CSU Long Beach or CSU Long Beach auxiliary organizations;

All media in which the information asset is held (e.g., paper, electronic, oral, etc.)

All data systems and equipment including departmental, divisional or other ancillary systems and equipment as well as data residing on these systems and equipment;

All faculty, staff, administrators, students, and consultants employed by CSULB or CSULB auxiliary organizations having access to CSU information assets; and

Personal electronic devices of CSULB faculty, staff, and administrators which access information technology resources.

RESPONSIBILITIES

Information security roles and responsibilities are intended to support the University's information security program. These roles and responsibilities include, but may not be limited to the following:

University Information Security Officeris an appropriate administrator designated by the President and delegated authority for implementing this policy; developing standards and procedures to support this policy; developing appropriate training and informational materials; and assessing and ensuring the University's compliance with applicable laws, regulations, and CSU and University policies, standards and procedures regarding information security.

Division Information Security Officers are management employees designated by each Vice President, the director Athletics, and each CSULB auxiliary organization who serves as a conduit between the University Information Security Officer and their respective division/area and who work closely with the University Information Security Officer to guide compliance with established CSULB information security policies, standards and procedures.

Custodians of Records are appropriate administrators designated by the Vice President, Administration and Finance who are responsible for 1)accepting and responding to subpoenas, court orders or other compulsory legal processes involving the release of University records; 2)accepting and responding to requests for records made pursuant to the California Public Records Act; or 3)ensuring compliance with the CSU records/information retention and disposition schedules.

University Administrators are mangers or supervisors included in the Management Personnel Plan or equivalent in CSULB auxiliary organizations who are responsible for ensuring compliance with established information security policies, standards and procedures within their respective college, department, administrative area or organization.

Faculty, Staff and Employees of CSULB Auxiliary Organizationswho in the course and scope of their duties and responsibilities access, collect, distribute, process, store, use, transmit or dispose of CSULB information assets are responsible for following established information security polices, standard and procedures.

POLICY COMPLIANCE

The University reserves the right to temporarily or permanently suspend, block, or restrict access to information assets when is reasonably appears necessary to do so to protect the confidentiality, integrity, availability, or functionality of those assets.

Any disciplinary action resulting from violations of this policy or program supporting policies, standards or procedures shall be administered in a manner consistent with the terms of the applicable collective bargaining agreement and/or the applicable provisions of the California Education Code. Student infractions of this policy or supporting policies, standards or procedures may be referred to the Office of Student Judicial Affairs. Third party service providers who do not comply with established information security policies, standards or procedures may be subject to appropriate actions as defined in contractual agreements.

POLICY MANAGEMENT

This policy shall be reviewed and if necessary updated annually by the University Information Security Officer.

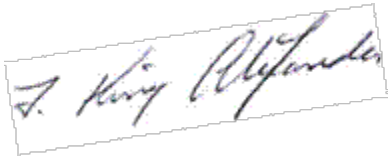
FURTHER INFORMATION

Information Security Management and Compliance

iso@csulb.edu

(562) 985-4862

Approved by President Alexander



May 2009

Appendix D: Electronic Media Sanitation

Subject:	**Electronic Media Sanitization Process**		
Department:	**Information Technology Services**	Reference No.:	
Division:	**Administration and Finance**	Issue Date:	**March 2010**
References:	• **Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley Act)** • **California Code of Regulations, Title 22, Division 4.5, Sections 66273 & 66273.6** • **CSULB Records Management Standard**	Revision Date:	**October 2010**
Web Links:	• **Information Technology Services** **http://daf.csulb.edu/offices/its/** • **Information Security Management and Compliance** http://daf.csulb.edu/offices/vp/information_security/policies/index.html	Expiration Date:	**N/A**

I. PURPOSE

The purpose of the *Electronic Media Sanitization Process* document is to guide campus staff and information technology coordinators through the use of CSULB's standardized tool and processes to securely wipe hard disks of computers that are being:

- Surveyed for public auction;
- Disposed of (e.g drive is too small, or no longer needed);
- Reassigned to other individuals on campus; or
- Transferred to another department of campus.

This is necessary to reduce possibility of inappropriate exposure of data and unauthorized use.

II. SCOPE

This Process applies to all University and Auxiliaries. Individual departments shall be fully responsible for ensuring storage media (e.g. hard drives) have been wiped or destroyed prior to asset disposition or internal reassignment.

III. BACKGROUND

To protect the confidentiality of information and the related privacy rights of CSULB students, faculty, staff, donors, patrons, vendors, and others, University and Auxiliary employees, in conjunction with their Information Technology Coordinator, must ensure that electronic data in their possession is secure at all times.

When electronic computing devices and/or electronic storage media are transferred between departments or divisions, or removed from service, all electronic data must be properly sanitized prior to release of custody. The sanitization process ensures that recovery of information is not possible. Several methods can be used to sanitize media; however, the two major types of sanitization are clearing and destroying.

Clearing – Clearing information is a level of media sanitization that protects the confidentiality of information against a robust keyboard attack. Simple deletion of items does not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities and must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. Overwriting is an acceptable method for clearing media. The security goal of overwriting is to replace written data with random data.

There are several overwriting software products to overwrite storage space on media. CSULB Information Technology Services provides software tools and instructions to securely clean the data from electronic storage media. Overwriting cannot be used for media that are damaged or not rewritable. In such cases, electronic media should be destroyed.

Destroying – When electronic media is inoperable and cannot be cleared, the electronic media must be physically destroyed.

IV. TRANSFERRING OR SURVEYING OF ELECTRONIC DEVICES AND MEDIA

When electronic computing devices or electronic storage media are to be transferred or surveyed, area Information Technology Coordinators will work with appropriate supervisors to complete the following steps:

1. All electronic computing devices or electronic storage media must be sanitized without exception. Only instances involving an inoperable internal hard drive that cannot be cleared will require its' removal from the electronic computing device in order to ensure proper destruction. Inoperable electronic computing devices and/or electronic storage media must be isolated and secured until properly destroyed. While physical destruction can be accomplished using a variety of methods, the campus has contracted with a third party vendor to ensure electronic media are destroyed in accordance with industry standards.

2. Overwrite data using university-approved and validated overwriting technologies/methods/tools;

Darik's Boot and Nuke (DBAN)	http://dban.sourceforge.net (One pass is sufficient)
Apple Disk Utility	http://support.apple.com

1. The designated Information Technology Coordinator must complete and sign a *Media Sanitization Certification* form for the item(s) to be transferred or surveyed.

2. The *Media Sanitization Certification* must be submitted with either a *Property Transfer Request Form* or *Property Survey Request Form* to Materials Management for processing.

3. Upon approval from Materials Management, the item(s) may then be transferred to the new Department or Division, or surveyed to Material Management.

V. DEFINITIONS

Electronic Computing Devices	Include, but not limited to, desktop computers, laptop computers, PDAs, tablet PCs, and smart phones.
Electronic Storage Media	Include, but not limited to, floppy disks, ZIP disks, DVDs, CDs, external/internal hard drives, and USB storage devices.
Information Technology Coordinators	University and Auxiliary employees who are responsible for maintaining electronic computing devices and/or electronic storage media for their designated areas.

FURTHER INFORMATION

Information Security Management and Compliance
iso@csulb.edu
(562) 985-4862

Or contact your area's designated Information Technology Coordinator.