User Guidelines for Electronic Communications	Guideline No.	ITS-1000-G	Rev:	F
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Director IT Security and Compliance		
	Issued:	7-2-03	Revised:	9-2-15
				Page 1 of 17

Table of Contents

1 Purpose 2
2 Entities Affected by These Guidelines 2
3 Definitions 2
4 Guidelines 4
4.1 Proper Usage of Electronic Communications 4
4.2 Improper Usage of Electronic Communications 5
4.3 Receiving and Replying to Email Messages 5
4.4 Forwarding Email 6
4.5 Email Broadcast 6
4.6 Student Electronic Communications 7
4.7 Donor and Alumni Electronic Philanthropic Communications 7
4.8 Email and Electronic Communications Security 8
4.9 Privacy and Monitoring 8
4.10 Unauthorized Access 9
4.10.1 Phishing (or Spear Phishing) 9
4.10.2 Pharming 10
4.10.3 Spyware 10
4.10.4 Spam 10
4.10.5 Malware 11
4.10.6 Actions for Crimeware Victims 11
4.10.7 Actions for Online Fraud Victims 11
4.11 Records Retention, Management and Disposal 12
4.11.1 Records Retention 12
4.11.2 Records Management 12
4.11.3 Records Disposal 13
4.12 E-discovery and Electronic Communications 13
4.13 Email Access for Separated Employees, FERP and Emeriti 13
4.13.1 Separated Employees 13
4.13.2 Faculty Early Retirement Program (FERP) 13
4.13.3 Emeriti 13
5 Contacts and Resources 14
6 Applicable Federal and State Laws and Regulations 14
7 Related Documents 16

1 Purpose

Electronic communications allows for communication both internally within the University and externally with users, including prospective students, alumni, donors and the public. These guidelines are intended to help all users of electronic communication to manage and use the University's communication resources in a legal, ethical and professional manner.

2 Entities Affected by These Guidelines

This user guideline applies to all users who have been granted network or email privileges at Cal State LA.

3 Definitions

a) Chain Letter: A typical chain letter consists of a message that attempts to convince the recipient to make a number of copies of the letter and then pass them on to as many recipients as possible.

b) Copyright: A form of protection for literary, dramatic, musical, artistic and certain other intellectual works to authors of "original works of authorship," provided by the laws of the United States (Title 17, U.S. Code). Copyrights protect both the published and unpublished works. Copyrights protect the work's reproductions, derivations, distribution, performances and display (including recorded images or audio transmissions).

c) Electronic Communications (also called Electronic Communications Tools): Communications intended for the transmission or sharing of information through electronic means. This includes, but is not limited to, email, instant messaging (IM), text messaging (TM), chat rooms, social media (e.g., Facebook, MySpace, Twitter), *myCSULA Community*, blogs and video chat.

d) Electronic Communications Devices: Communications devices used for the transmission of information over significant distances. Examples include telephones, cell phones, smart phones, tablets and computing devices, pagers, facsimile machines and multi-function devices (MFD).

e) Electronic Communications Methods: Electronic communications methods can include telegraphs, telephones, teletypes, radio and microwave communications, fiber optics and their associated electronics, wired and wireless networks, orbiting satellites and the Internet.

f) Electronic Discovery (also called e-discovery or eDiscovery): Refers to discovery in civil litigation that deals with the exchange of information in electronic format.

g) Electronic Mail (also called email or email): Messages composed and transmitted electronically through a wireless device, computer, network or other means. Email messages can contain attachments.

h) Email Broadcast (also known as Mass Email or Mass Emailing): An email message sent campus wide from one mailbox.

i) Encrypted Connection: Data transmitted "in the air" (i.e., to and from the computer and the access point) that is scrambled such that unauthorized individuals are prevented from discerning it.

j) Instant Messaging (IM): Messages that are sent back and forth instantly, in the form of an ongoing conversation, using devices such as cell phones, smart phones, iPads or other tablets and the like.

k) Level 1 Confidential Data: Confidential data is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

l) Level 2 Internal Use Data: Internal use data is information that must be protected due to proprietary, ethical or privacy considerations. Although not specifically protected by statute, regulations or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss or deletion of information at this level could cause financial loss, damage to the CSU's reputation, violate an individual's privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

m) Multi-function Device (MFD): An office machine which incorporates the functionality of multiple devices in one and generally provides centralized document management/distribution/production. A MFD is sometimes called a multifunction printer (MFP), all-in-one (AIO) device and network printer. A MFD may act as a combination of some or all of the following devices: printer, copier, scanner, fax and email.

n) Pharming: Online fraud where the hacker's attack is aimed at redirecting a website's traffic to another bogus site for the purpose of obtaining individual's confidential information.

o) Phishing (also known as Spear Phishing): A combination of spoofing and social engineering that uses email, instant messaging or telephone calls to trick someone into divulging personal, confidential or financial information by impersonating (spoofing) a known or legitimate person, company or organization.

p) Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

q) Separated Employee: Any faculty or staff who severs employment with the University by choice, mutual agreement, end of temporary appointment, is non-retained or is dismissed for reasons under Education Code 89535.

r) Spam: The use of electronic messaging systems to send unsolicited bulk messages indiscriminately.

s) Spyware: Software that resides on a computer and sends information to its creator.

t) Text Messaging (TM) (Also known as texting): The exchange of brief text messages between phones or portable devices over a network or the Internet. Text messages can interact with automated systems, such as ordering products or services, or entering online contests, and are commonly used by product or service providers for promotions, announcements, payment deadlines and transaction notifications.

u) Transitory Communications: Messages having little or no lasting value to the organization, such as notices and reminders of meetings or events.

4 Guidelines

Electronic communication is an essential part of University communications. The University provides electronic communications tools for legitimate University-related activities to faculty, students, staff and other individuals who are responsible for all activity that occurs under their account. Cell phones, smart phones, laptop computers and tablets are now routinely used for inter-campus communications, remote access to campus resources such as email and websites, and access to social networking. Used effectively, electronic communications can be very beneficial. This guideline outlines the best practices in an effort to promote effective and secure electronic communications.

4.1 Proper Usage of Electronic Communications

The following are considered proper use of electronic communications:

a) Using electronic communication accounts for legitimate University-related purposes and conducted in an appropriate, ethical, professional and lawful manner. Examples of legitimate University-related purposes include, but are not limited to, class-related activities, academic research, access to administrative systems, sending official University communications to students and miscellaneous administrative tasks that support these efforts.
b) Respecting other people's time – sending email, text messages or instant messages only when it needs to be sent.
c) Respecting copyrighted material. Not reproducing and sending any material unless all references, quotes and sources are properly cited or with permission of the copyright holder and/or payment.
d) Taking care in achieving the proper tone when using electronic communications since body language cues and verbal intonation are absent from written messages. Sarcasm and humor can be easily misinterpreted.
e) Forwarding email or allowing folder access only to those who are authorized to view the information.

f) Marking as a high priority only those messages that have an urgent or critical time requirement.
g) Use tracking options (deliver and read receipts) only if verification is absolutely needed.
h) Keeping passwords to electronic communication accounts confidential.

4.2 Improper Usage of Electronic Communications

The following are considered improper use of electronic communications:

a) Altering the source or destination address of email.
b) Using electronic communication for commercial or private business purposes that have not been authorized by the University.
c) Using electronic communication for political advocacy in election campaigns not related to University approved on-campus student government activities.
d) Using electronic communications to threaten, harass, stalk, defame, or otherwise interfere with the legal rights of others.
e) Retrieving or reading the email, text messages or instant messages of others.
f) Concealing or posing as someone else when sending any email or instant message.
g) Sending chain letters or “spam” via email.
h) Changing someone else’s message and passing it on without clearly indicating where changes were made and by whom. Unidentified changes to another’s messages constitute misrepresentation.
i) Using electronic communications to devise or execute any scheme or artifice to defraud, deceive or extort or wrongfully control or obtain money, property or data.
j) Making copies of emails without permission.
k) Sending, posting, publishing or otherwise causing protected data to be publicly available.
l) Transmitting, receiving or viewing child pornography (a federal criminal offense).
m) Using electronic communications for more than incidental personal use.

4.3 Receiving and Replying to Email Messages

In receiving and replying to email messages, a user should:

a) Not assume the validity of a received message.
b) Read email regularly. The immediacy of email may be lost if it sits unnoticed in the mailbox for long periods.
c) Be courteous. Reply to email messages within 24 hours, even if it is to let the sender know that a lengthier response will be sent at another time.
d) Use the automatic reply feature when email messages will not be opened for a period of time. Senders should be advised of return dates, alternate contacts and any other pertinent information that may be helpful. However, use caution in preparing the automatic reply content. Do not include information that could alert criminals to an extended absence such as “traveling through Europe this summer” or “on sabbatical for one year.”
e) Use tracking options if verification that a message has been delivered or read is needed.

4.4 Forwarding Email

All users have the option of forwarding their Cal State LA email to another email service provider. However, students should understand that their primary campus email address remains the official destination for official University correspondence and Cal State LA cannot guarantee mail forwarded to another address will actually be delivered. Email routed to other sites can be lost or returned ("bounced") for many reasons, including a full mailbox at the destination site, mail filters that mistakenly reject Cal State LA email and technical problems at the destination site.

4.5 Email Broadcast

All email broadcasts must have an impact on the campus community at large, cannot be communicated as efficiently by any other means and must relate to at least one of the following:

- Official University business,
- Emergency notifications (e.g., building or street closures, power outages, evacuations),
- Medical, health or safety issues or
- Mandatory training

Email broadcasts must be approved by the vice president or appointed delegate(s) of the division that originates the broadcast and comply with this user guideline, *ITS-1031-G User Guidelines for Official Electronic Communications to Students*, the Family Educational Records Privacy Act (FERPA) and the Americans with Disabilities Act (ADA).

The following are considered proper procedures for email broadcasts:

a) Before sending campus wide broadcasts, consider whether every person on campus needs to view the message.
b) Consider using other appropriate means of sharing this information.
c) If possible, create targeted distribution lists for smaller groups of interested recipients (e.g., department offices, faculty, MPPs, activity members, etc.).
d) For campus wide messages, create segmented distribution lists that allow the message to be sent gradually throughout the day. The message will thereby have reduced impact on instructional programs and network traffic.
e) Do not hold email broadcasts for the close of business or late night delivery. Doing so creates a surge on the network that may impact instructional programs and network traffic when the campus reopens in the morning and many users are attempting to simultaneously access the message.
f) The contents of attached documents in an email broadcast should be protected from erasure or alteration prior to distribution by using the protection tools provided by the application or by creating a .pdf file.
g) Delivery or read receipts should never be used.
h) The distribution list should always be inserted into the blind copy (BCC) field.
i) The message should contain a prominent notice stating: "This is a campus wide message. Please do not reply all."
j) Public Affairs should review the message before it is sent.

4.6 Student Electronic Communications

Cal State LA uses email as one official means of communicating business and academic information to students. Messages sent to students' email accounts from administrative offices, colleges and faculty is considered official University communications. As some messages may be time-critical, it is strongly recommended that students check their campus issued email account on a regular basis or implement email forwarding to automatically forward their messages to a personal email account.

4.7 Donor and Alumni Electronic Philanthropic Communications

One significant change to the philanthropic landscape is the increased use of technology to facilitate charitable giving, including annual fund solicitations or the acceptance of online contributions from donors.

The division of University Development serves as the coordinating entity for the University's philanthropic efforts, and maintains the Cal State LA donor and alumni database. The division also serves a critical function by ensuring that the collection and processing of electronic donations are compliant with federal regulations, and for verifying and issuing tax receipts for charitable contributions.

University employees responsible for corresponding with donors and University alumni and its associated auxiliaries must:

- Ensure that all online transactions and contributions occur through a safe, private and secure system that protects donor's personal information.
- Understand that all correspondence through any form of electronic communications is not secure, private or confidential.
- Encrypt all email messages and attachments containing confidential information.
- Comply with the encryption standards outlined in *ITS-1027-G User Guidelines for Encryption Security*.
- When possible, use the sender's auxiliary title to sign emails or other electronic communications that are auxiliary correspondence, particularly donor-related correspondence. Electronic communications to donors must clearly indicate whether the correspondence is a University record or an auxiliary record.
- Adhere to the principles outlined in the American Association of Fund Raising Professional's (AFP) E-donor Bill of Rights.
- Maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS) when processing electronic contributions.
- Maintain compliance with the University's policy on Coordination of Appeals.
- Have the content and standards for such communications approved in advance by the Office of Public Affairs.

4.8 Email and Electronic Communications Security

It should be assumed that all communications on the Internet are not secure, private or confidential. Email, text messages and instant messages are exposed to the possibility of unauthorized access at a number of points:

- When it is being delivered across a network,
- When it is stored on a mail relay,
- When it is in the sender's or receiver's message store, or
- When it is accessed across a network from the sender's or receiver's message store (e.g., when message store is on an IMAP server).

Electronic communications devices are generally small, transportable and can be easily lost or stolen. If not password protected and set to automatically lock after a short period of inactivity, anyone finding a lost device will have access to all messages and information contained on the device. Information on securing these devices is available in *ITS-1020-G User Guidelines for Mobile Computing*.

All protected data at rest and in transit should use encryption measures strong enough to mitigate the risk of unauthorized access. More detailed information on encryption is available in *ITS-1027-G User Guidelines for Encryption Security*. The campus Virtual Private Network (VPN) provides a secure encrypted connection to the campus network and should be used for the transmission of protected data.

4.9 Privacy and Monitoring

Electronic communications, including email messages, are not private and users should have no expectation of privacy. Once a message has been sent, the message can be forwarded to others or printed and given to others. Postings on social network sites and chat rooms have unlimited exposure, including the ability to permanently harm reputations. Electronic communications should be viewed as correspondence that leaves a permanent record once sent and cannot be recalled.

The University does not routinely monitor the content of electronic communications. However, the University reserves the right to inspect, copy, store or disclose the contents of electronic communications to do the following:

a) Prevent or correct improper use of University communications resources.
b) Ensure compliance with California State University Executive Orders, CSU policies, University administrative procedures, standards and guidelines, and federal and state laws and regulations.
c) Ensure the stability, performance and integrity of University communications resource operations.
d) Monitor or investigate email accounts or other communications resources where there is rational basis to believe that a law or CSU or University policy is being violated.
e) Comply with a legal obligation, such as a court order, subpoena, Public Records Act request or other legal civil and criminal discovery request.
f) Obtain vital information in the event of an emergency.

4.10 Unauthorized Access

Cyber criminals use email as a way to collect personal information (spear phishing, pharming), download malicious software (spyware) and overload inboxes with unwanted mail (spam). Preventing these threats can help keep University resources safe.

Anti-virus services are applied to all campus email accounts. All student accounts are permanently subscribed to the campus anti-virus/anti-spam services and opting out is not available to students. Faculty and staff may voluntarily subscribe their accounts to the anti-spam service. While no virus or spam blocker offers total protection, the many layers of protection deployed on campus provides a strong defense against most virus and spam attacks.

As a precaution, it is recommended that everyone back up his or her computer data files to a secure, encrypted electronic storage media in the event an unauthorized access incident damages, destroys or prevents access to the computer or its content.

4.10.1 Phishing (or Spear Phishing)

Phishing is an attempt to use electronic communications, generally email or instant messaging, for the purpose of acquiring confidential information such as names, user names, passwords, account numbers or credit card information by pretending to be a trustworthy entity. Messages are sent directly to individuals and often contain lures such as click here to “verify your account” or “confirm billing information.” Successful phishing is reliant on the message recipient responding to the “bait” by clicking on a link in the fake message.

The following actions can be taken to avoid becoming the victim of spear phishing:

a) Trust no one. If you are unsure whether an email request is legitimate, try to verify it by directly contacting the sender.
b) Pay attention to the URL of a website. Malicious websites may use a variation in spelling or a different domain of a legitimate site.
c) Never email unencrypted protected data.
d) Do not click on links in unknown or unsolicited email messages.
e) Do not open any attachments in a suspicious email.
f) Consider using an anti-phishing tool on your browser that can warn of known or suspicious websites.
g) Install and maintain anti-virus software, firewalls and email filters to reduce some of this traffic.

4.10.2 Pharming

Considered a relative to phishing, pharming works on a much larger scale by redirecting traffic from a legitimate website to a bogus website. Cybercriminals attack Internet Domain Name Systems (DNS) where meaningful web names (www.mybank.com) are converted into numeric addresses (123.345.7.8). By changing the legitimate site's numeric address to a bogus website address, all traffic destined to the legitimate site is then redirected to the cybercriminal's site.

The following actions can be taken to avoid becoming the victim of pharming:

a) Do not respond to any messages including those that may appear from a legitimate source.
b) Keep your computer current with the latest patches and updates.
c) Choose strong passwords and never share them with others.
d) Protect your computer with security software.
e) Protect University protected data and your personal information at all times by encrypting computer files containing this information.
f) Do not respond to online offers that look too good to be true.
g) Review bank and credit card statements regularly.

4.10.3 Spyware

Spyware can damage or destroy your computer data but is also capable of monitoring your computer to capture protected data. The following actions can be taken to guard against spyware:

a) Keep software patches up-to-date.
b) Install and maintain up-to-date anti-virus software.
c) Don't download shareware from unknown sources.
d) Don't click on any pop-up or advertisement for free anti-spyware software.
e) Set the browser and operating system security level to at least the medium setting (or higher) for best results.
f) Install a firewall and use a separate router rather than sharing the Internet connection through one computer.
g) Avoid questionable websites.
h) If a virus alert appears on the screen of a website, don't click on it, even to close it.
i) Never open an email attachment if you are uncertain of its source.

4.10.4 Spam

If an email account does not have email filters, it will become overloaded with junk. This junk mail may contain dangerous viruses and scams. To reduce the amount of spam deposited into an email inbox, the following actions can be taken:

a) Enable a junk email (or "spam") filter. Some junk mail filters have multiple settings with the highest setting being the most restrictive.
b) Block all email from specific addresses.
c) Unsubscribe from legitimate vendors that you don't wish to do business with.

4.10.5 Malware

Malware, which is short for malicious software, consists of programming (code, scripts, active content, etc.) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources and other abusive behavior (Wikipedia). It may be difficult to detect because some threats hide themselves in the computer, while others display messages or pictures that may indicate their presence. The following steps can be taken to lessen the probability of malware infection:

a) Install anti-virus and anti-spyware programs from a trusted source.
b) Update the software regularly.
c) Use strong passwords and keep them secret.
d) Never turn off firewall protection software.
e) Use flash drives cautiously.
f) Don't be tricked into downing loading malware by clicking on links or attachments in emails from unknown sources.

4.10.6 Actions for Crimeware Victims

Cybercrimes can occur on-campus, when traveling or from personal home computers. The following steps are recommended by Norton/Symantec for users who believe they have been a victim of crimeware (Trojans, bots, etc.). For on-campus incidents, an immediate call to the ITS Help Desk, 3-6170, will initiate all the appropriate remediation steps. If you are off-campus:

a) Disconnect immediately. Unplug the network cable, phone or cable line from your machine. This can prevent data leak back to the attacker.
b) If you are at work or on business travel, contact the ITS Help Desk immediately.
c) If you are at home, consider getting assistance from a trusted source as well as contacting your Internet Service Provider (ISP).
d) Scan your computer with an up-to-date anti-virus program.
e) Back up critical information. Sensitive data can be leaked during the crime and lost or destroyed during clean-up. All critical University files, documents, databases and other important work should be backed up frequently, preferably daily, on approved electronic storage media. For more information on electronic storage media, view *ITS-1005-G User Guidelines for Portable Electronic Storage Media*.
f) Consider going back to ground-zero by reinstalling the computer's operating systems. Some crimeware is sophisticated enough to burrow deep within the computer in an attempt to hide from security software. Sometimes the best course of action is to return to a pre-infection state.

4.10.7 Actions for Online Fraud Victims

The following actions are recommended for anyone who suspects their confidential or personal information has been acquired by identity thieves.

a) Close any affected accounts immediately. To err on the side of safety, consider freezing or changing all accounts for credit cards, banks or other online service accounts.
b) Set up a fraud alert with the three national consumer reporting agencies – Equifax, Experian and TransUnion.

c) File a police report in the area where the crime took place. A copy of the police report or the report number can serve as evidence with creditors in case they require proof of the crime.
d) Contact government agencies.
   - If a driver's license number is stolen, contact the Department of Motor vehicles.
   - If a social security number is stolen, contact the Social Security Administration.
   - Report the identity theft to the Federal Trade Commission, which maintains an identity theft database used by law enforcement agencies for investigations.
e) Watch credit reports closely. Ensure information from all three credit reporting agencies is the same. Some agencies offer alerting services for a fee. Remember that it may take some time before fraudulent activity occurs or appears on credit reports so don't stop checking reports prematurely.
f) Watch for signs of identity theft. Be on the lookout for unusual items in the mail, such as unsolicited credit cards or bills that are suddenly missing. Contact by vendors regarding unfamiliar accounts or debt collectors regarding unknown purchases are also signs of lingering identity theft problems.

4.11 Records Retention, Management and Disposal

University data must be retained, secured and destroyed in compliance with all legal and regulatory requirements while implementing appropriate best practices. This includes email messages and attachments. Refer to *Administrative Procedure 707 Records Retention, Management and Disposition Program* for more detailed information.

4.11.1 Records Retention

Cal State LA creates backups of the campus email system for disaster recovery purposes only, not for retrieving deleted messages. Backups are retained for up to 30 days and should not be considered part of a records retention function. Email is a communication tool, not a replacement for filing cabinets, media storage or document retention systems.

Data stewards, division, college, department and unit management, as appropriate, are responsible for:

- Complying with legal, CSU or University document retention periods and for securely retaining those email messages and attachments that apply such as e-discovery, litigation holds and subpoenas.
- Ensuring that email messages and attachments that need to be retained are removed from the email server, stored elsewhere (either printed or saved to a local drive or other location) and backed up for the required retention period.

4.11.2 Records Management

The size of an Inbox and subfolders should be managed by doing the following:

- Save needed attachments to a local or network drive or secure electronic storage device.
- An immediate supervisor should be contacted about the messages, documents and attachments that are required to be retained.
- For a series of retained messages, keep only the last message in the series that contains the entire discussion thread. Discard the other messages since they are redundant.
- Preserve important email attachments before deleting a message.

4.11.3 Records Disposal

Permanently delete unwanted, outdated and transitory communications in all folders, including your Sent folder and the Deleted Items folder. Delete or reconcile email on all smart phones, tablets or other electronic media used to access University email.

4.12 E-discovery and Electronic Communications

Electronic discovery, often called e-discovery or eDiscovery, refers to discovery in civil litigation that deals with the exchange of information in electronic format. Examples of the types of data included in e-discovery are emails, instant messaging chats, documents, accounting databases, CAD/CAM files, websites and any other electronically stored information that could be relevant evidence in a lawsuit.

Electronic communications are different from paper communications because of their intangible form, volume, transience and persistence. Electronic communications are usually accompanied by metadata that is not found in paper documents and that can play an important part as evidence. For example, the date and time a document was written could be useful in a copyright infringement case.

4.13 Email Access for Separated Employees, FERP and Emeriti

4.13.1 Separated Employees

Once separation occurs, a former employee may not use his or her email account to conduct University business. Information Technology Services (ITS) locks user accounts upon receipt of separation notification through the Human Resources Management (HRM) online separation form. ITS is not authorized to reinstate or provide access for another individual to any separated employee's network/email access without written approval from HRM or University Auxiliary Services-Human Resources, Academic Affairs or the President's Office, depending upon the type of access required.

Separated employees' email accounts remain hidden from access for 60 days and, at the end of that time, are permanently deleted.

4.13.2 Faculty Early Retirement Program (FERP)

Email accounts for FERP faculty remain available during the entire period that the faculty is employed.

4.13.3 Emeriti

Emeriti retain the right and privilege to continued use of an email account upon approval of emeritus status from the college dean, the provost and vice president for Academic Affairs and the president.

5 Contacts and Resources

a) Address questions regarding these guidelines to: ITSecurity@calstatela.edu.

b) Address questions regarding email access for separated employees to: Human Resources Management, ADM 606, 323-343-3662.

c) The list of currently approved encryption tools is available at: http://www.calstatela.edu/its/services/software/encryptiontools.php

d) Information about encryption best practices is available in *ITS-1027-G User Guidelines for Encryption Security*: http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-1027-g_encryptionsecurity.pdf

6 Applicable Federal and State Laws and Regulations

Federal	Title
Family Educational Rights and Privacy Act (FERPA)	**Family Educational Rights and Privacy Act (FERPA)** http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html This is a federal law that protects the privacy of student education records.
Gramm-Leach-Bliley Act 15 USC, Subchapter I, Sec. 6801-6809	**Gramm-Leach-Bliley Act** http://www.ftc.gov/privacy/glbact/glbsub1.htm This is a federal law on the disclosure of nonpublic personal information.
The Donor Bill of Rights	**The Donor Bill of Rights** http://www.afpnet.org/Ethics/EnforcementDetail.cfm?ItemNumber=3359 The Donor Bill of Rights was created to ensure that philanthropy merits the respect and trust of the general public and that donors and prospective donors can have full confidence in the nonprofit organizations and causes they are asked to support.
Health Insurance Portability & Accountability Act (HIPAA), 45 C.F.R. parts 160 & 164	**Standards for Privacy of Individually Identifiable Health Information** http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/prdecember2000all8parts.pdf This is a federal law that protects the privacy of health records.

Federal	Title
U.S. Copyright Office	**United States Digital Millennium Copyright Act** For a comprehensive summary, visit: http://www.copyright.gov/legislation/dmca.pdf The legislation implements two 1996 World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty. The CMDA also addresses a number of other significant copyright-related issues.
PCI DSS	**Payment Card Industry Data Security Standards** https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf These procedures are designed to conduct reviews to validate compliance with Payment Card Industry (PCI) Data Security Standard (DSS) requirements, a set of comprehensive requirements for enhancing payment card data security.
CAN-SPAM Act of 2003 (15 U.S.C. 7701, et seq., Public Law No. 108-187	**Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003** http://business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business The CAN-SPAM Act sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them and spells out tough penalties for violations. Messages must contain a visible and operable unsubscribe mechanism and consumer opt-out requests must be honored within 10 days.
State	**Title**
California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85	**California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85** http://www.leginfo.ca.gov/.html/civ_table_of_contents.html This is a state law that provides information on safeguarding personal information.
California Government Code Section 8314	**California Government Code 8314** http://codes.lp.findlaw.com/cacode/GOV/1/2/d1/5/s8314 This is a state law that prohibits the illegal use of state-owned computing equipment for personal use, gain or downloading obscene content.
California Penal Code Sections 502 and 502.1	**California Penal Code, Section 502 and 502.1** http://codes.lp.findlaw.com/cacode/PEN/3/1/13/5/s502 This is a state law that prohibits the illegal use of telecommunications equipment.

7 Related Documents

Campus	Title
ITS-2524	**Cal State LA Information Security Program** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/campus_information_security_plan_2012.pdf This document establishes the University's Information Security Program in support of the obligation to protect the technology resources and information assets entrusted to it.
ITS-1009-G	**User Guidelines for Separated Employees' Network/Email Access** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-1009-g_separatedemployeesemailaccessguidelines.pdf These guidelines provide information on network and email access for separated employees.
ITS-1016-G	**User Guidelines for Protecting Electronic Copyrighted Material** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-1016-g_guidelines-protectcopyrightedmaterials.pdf These guidelines outline the requirements for software licensing compliance.
ITS-1027-G	**User Guidelines for Encryption Security** http://www.calstatela.edu/sites/default/files/groups/Information%20Technology%20Services/security/its-1027-g_encryptionsecurity.pdf These guidelines provide information on approved encryption algorithms, recommended encryption products specific encryption tools and practices.
Administrative Procedure 707	**Records Retention, Management and Disposition Program** http://www.calstatela.edu/sites/default/files/groups/Administration%20and%20Finance/Procedure/ap707.pdf This procedure establishes policy for the secure management of University records and the transfer of University records to the State Records Center, the retrieval of stored records and the destruction of obsolete records.

Chancellor's Office	Title
CSU Information Security Policy	**The California State University Information Security Policy** http://www.calstate.edu/icsuam/sections/8000/8000.0.shtml This document provides policies governing CSU information assets.
CSU Executive Order 999	**Illegal Electronic File Sharing and Protection of Electronic Copyrighted Material** http://www.calstate.edu/EO/EO-999.html This Executive Order specifies that resources of the California State University, including computer hardware and software and intro/inter-campus network connections, must not be used for the purpose of illegal downloading, copying or use of copyrighted materials, including, but not limited to, music, videos, motion pictures and Internet accessible content.
CSU Executive Order 1031	**System-wide Records/Information Retention and Disposition Schedules Implementation** http://www.calstate.edu/EO/EO-1031.html http://www.calstate.edu/recordsretention This Executive Order provides for the implementation of the California State University (CSU) Systemwide Records/Information Retention Schedules.