

# What do I have to **PROTECT**?



## All Information and User Accounts in Accordance with Federal and State Laws and Regulations, and CSU Executive Orders, Guidelines, and Policies:

[www.calstatela.edu/its/policies](http://www.calstatela.edu/its/policies)  
[www.calstatela.edu/ferpa](http://www.calstatela.edu/ferpa)  
[www.calstatela.edu/itsecurity](http://www.calstatela.edu/itsecurity)

Be familiar with applicable laws, regulations, and Executive Orders to ensure that Cal State L.A. users treat confidential information and user accounts appropriately. Complete the FERPA tutorial to learn how to protect student records, and check the **areyouSecure** website for tips on securing and handling confidential information. The list below includes, but is not limited to, the types of information the campus community needs to protect.



**Personal Information:** Under SB 1386: The individual's first name or first initial and last name in combination with any one of the following: Social Security Number (SSN); driver's license number; California Identification Card; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.



**Confidential Information:** In addition to those listed in the Personal Information definition above: financial records; medical records; physical description; home address; home phone number; education; grades; ethnicity; gender; employment history; performance evaluations; disciplinary action plans; NCAA standings; etc. Confidential information must be interpreted in combination with all information contained on the computer or in printed format to determine whether a violation has occurred.



**Confidential Student Information:** In addition to other confidential and personal information, any personally identifiable information, such as name, parent's name, address, Social Security Number (SSN), Campus ID number (CIN), credit card numbers, and personal characteristics or other information that would make the student's identity easily traceable.



**Proprietary Information:** Information that an individual or entity possesses, owns, or holds exclusive rights to. Examples include: faculty research; copyrighted materials; white papers; research papers; business continuity and other business operating plans; e-mail messages; vitae; letters; confidential business documents; participants of an organization, class, or group; detailed building drawings; network architecture diagrams; etc. Proprietary information, if lost or stolen, could compromise, disclose, or interrupt operations or embarrass the individual or the university.



**Shadow Systems/Confidential Files:** Shadow systems and/or confidential files are any files or applications, third party or home-grown databases, systems, spreadsheets, documents, tables, etc., external to Student Administration (SA) and the Common Management System (CMS) applications and that contain personal and/or confidential information. Examples: Stand-alone payroll or financial systems; student housing systems; library systems; rosters that contain names of students, their addresses, phone numbers, and grades; attendance databases containing emergency contact information; information repositories containing passwords, employee ID numbers, drivers' license numbers, and Social Security Numbers; and rosters containing NCAA standings or commuter information.



Campus Information Security Awareness  
for Faculty & Staff

# areyouSecure?

## QUICK REFERENCE GUIDE



Information Technology Services

## INFORMATION ASSURANCE

### Director, IT Security Management and Compliance

(323) 343-2600  
ITSecurity@calstatela.edu  
LIB PW 1070

### ITS Help Desk

(323) 343-6170  
LIB PW Lobby  
helpdesk@calstatela.edu

## NEW! ONLINE SERVICE

## areyouSecure?

[www.calstatela.edu/itsecurity](http://www.calstatela.edu/itsecurity)



Always be aware of how you use and secure information. Get security tips about combating viruses, spam, hoaxes, phishing, pharming, ID theft, and more. Learn how to secure confidential information, electronic documents, offices, workspaces, computers, laptops, electronic storage devices, passwords, and more.

Securing information is the responsibility of every department and individual on campus. No one can assume that anti-virus software, firewalls, and data encryption can provide the protection needed to secure all data that resides on personal workstations, in file cabinets, or on desks, printers, and copiers. Everyone on campus needs to think about information security in a new light.

### Information Security Is Everyone's Responsibility!

Help protect confidential information and campus resources.

- Be Aware
- Be Cautious
- Be Responsible

Check the **areyouSecure** website often for updates and new postings.



## WHAT CAN I FIND OUT ABOUT INFORMATION SECURITY?

**SECURITY GUIDELINES**  
[www.calstatela.edu/policies](http://www.calstatela.edu/policies)

Find information technology guidelines; applicable federal and state laws and regulations; and CSU guidelines, policies, and Executive Orders.

**SECURITY MAILBOX**  
[ITSecurity@calstatela.edu](mailto:ITSecurity@calstatela.edu)

Submit questions, and report security violations, breaches, vulnerabilities, and issues.

**ITS ALERTS**  
[www.calstatela.edu/alerts](http://www.calstatela.edu/alerts)

Subscribe to be notified of breaking virus and scam alerts to ensure that appropriate prevention is applied.

**ITS NEWS/UPDATES**  
[www.calstatela.edu/its/news](http://www.calstatela.edu/its/news)

Check this website for announcements, bulletins, and special reports.

# WHAT FACULTY & STAFF NEED TO KNOW?

## WHY DO I HAVE TO PROTECT INFORMATION?

Cal State L.A. must adhere to the laws and regulations that govern how we handle and use confidential information and the user accounts accessing that information.

### Federal Laws

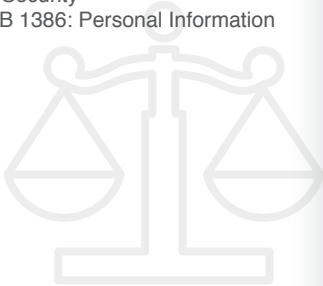
[www.calstatela.edu/its/policies](http://www.calstatela.edu/its/policies)

- Federal Privacy Act of 1974
- FERPA (Family Educational Rights and Privacy Act)
- Gramm-Leach-Bliley Act (Financial Modernization Act of 1999)
- HIPAA (Health Insurance Portability and Accountability Act of 1996)
- Patriot Act (Public Law 107-56)

### California Laws

[www.calstatela.edu/its/policies](http://www.calstatela.edu/its/policies)

- California Civil Code sections regulating personal information (1798.29, 1798.82, 1798.84, 1798.85)
- California Financial Information Privacy Act
- California Information Practices Act of 1977
- California Senate Bill (SB) 25: Personal Information Security
- California SB 1386: Personal Information Privacy



## HOW DO I PROTECT INFORMATION?

### Protect Your Passwords

[www.calstatela.edu/itssecurity](http://www.calstatela.edu/itssecurity)

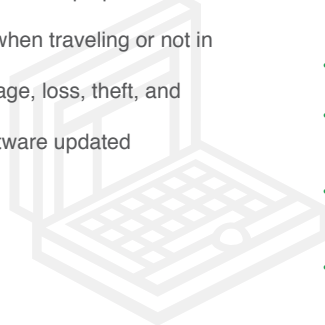
- Change the default password immediately after logging into an account for the first time.
- Use strong passwords (minimum 8 characters, mixed case, numbers, and special characters).
- Do not share passwords with anyone.
- Do not leave passwords where others can find or access them.

### Protect Your Laptop

[www.calstatela.edu/itssecurity](http://www.calstatela.edu/itssecurity)

[www.calstatela.edu/its/policies](http://www.calstatela.edu/its/policies)

- Treat your laptop like you would your wallet or purse. Keep it in your possession and don't let anyone else have access to it.
- Configure all security measures on new laptops for optimum security.
- Protect laptop data from unauthorized access, use, and/or tampering
- Secure the wireless laptop connection
- Physically safeguard the laptop from theft or damage.
- Secure the laptop when traveling or not in use
- Report laptop damage, loss, theft, and security breaches
- Keep anti-virus software updated



### Secure Your Office and Workspace

[www.calstatela.edu/its/policies](http://www.calstatela.edu/its/policies)

See complete user guidelines on website.

- Confidential information may only be handled by those authorized to do so.
- Use a confetti or pulp shredder when discarding documents containing confidential information.
- Store confidential documents in locked file cabinets or drawers.
- Do not leave confidential documents unattended at the printer, fax, or copier.
- Locate workstations containing confidential material so that others cannot see the computer screen.
- Lock your computer and office door every time you must leave your work area.
- Completely reformat the hard drive(s) of every computer being redeployed or discarded.
- Securely store electronic storage devices (CDs, DVDs, etc.) containing confidential information.
- Remove metadata (hidden data) from electronic documents and password protect them before they are published or distributed.
- Do not put confidential information in documents meant for general distribution.
- Call IT Security (3-2600) for help in encrypting documents containing confidential information.
- Do not e-mail confidential information. Move e-mail containing confidential information to a secured hard drive.
- Do not post confidential information in an Outlook Public Folder.

## WHERE CAN I FIND ONLINE SECURITY FORMS?

### Faculty/Staff SA and CMS Accounts

[www.calstatela.edu/its/forms](http://www.calstatela.edu/its/forms)

Required forms to access the Student Administration and CMS systems (the appropriate Chancellor's Office mandatory Access and Compliance form is automatically appended):

- Contributor Relations
- Human Resources
- Financials
- Student Administration

### Faculty/Staff Network/E-mail Accounts

[www.calstatela.edu/its/forms](http://www.calstatela.edu/its/forms)

Required forms to access the campus administrative network and e-mail:

- Network/E-mail Account Request

### Network Usage

[www.calstatela.edu/its/forms](http://www.calstatela.edu/its/forms)

Request ITS assistance to create secure network and/or server applications.

- Network Usage Request

### Third Party Access

[www.calstatela.edu/its/forms](http://www.calstatela.edu/its/forms)

Required form for vendors, consultants, and outside contractors to access campus and network systems:

- Third Party Access Request
- Network/E-mail Account Request

**Keep checking the ITS Forms website. New forms are posted as needed.**



## HOW DO I PROTECT STUDENT RECORDS?

[www.calstatela.edu/ferpa](http://www.calstatela.edu/ferpa)

Learn about the Family Educational Rights and Privacy Act (FERPA) and why protecting student records is important to our campus.



## HOW DO I REPORT INFORMATION THEFT?

### Report a Lost or Stolen Computer or Electronic Storage Device

[www.calstatela.edu/its/policies](http://www.calstatela.edu/its/policies)

- Notify University Police immediately (323) 343-3700
- Complete the Lost or Stolen Computer or Electronic Storage Device Report form found under Incident Response <http://www.calstatela.edu/its/forms/> and bring it to LIB PW 1070 or e-mail it to [ITSecurity@calstatela.edu](mailto:ITSecurity@calstatela.edu)

### Report Lost or Stolen Documents

- Contact University Counsel immediately (323) 343-3054
- Contact IT Security Management and Compliance (323) 343-2600

### Report a Security Breach

- Contact ITS Help Desk immediately (323) 343-6170 [ITSecurity@calstatela.edu](mailto:ITSecurity@calstatela.edu)