

☐ New User ☐ Modify User ☐ Re-approval

This form is used to request SSU system access for non-employees who require system access to fulfill their responsibilities to the university. For questions regarding use of this form, contact hr@sonoma.edu. The individual requiring access must review the attached Confidentiality Training and complete the Access and Compliance Form.

Due to the confidential information on this form, please submit in hard copy, via fax, AdobeSign or other secure method.

Step 1. Individual requiring system access completes "Personal Information" section.

1. Personal Information	
Name (First M. Last): _____	SSN or SSU ID #: _____
Address: _____	Date of Birth (day/mo/yr): ____/____/____
City, State, Zip: _____	Telephone #: _____
<input type="checkbox"/> I have reviewed the Confidentiality Training and completed the "Access and Compliance Form" attached to this request.	
Signature: _____	Date: _____

Step 2. Department completes "Department Information" section and returns to Human Resources for processing.

2. Department Information	
Check one: <input type="checkbox"/> Independent Contractor <input type="checkbox"/> Intern <input type="checkbox"/> Other (Please describe): _____	
Specify the type of access needed below:	
<input type="checkbox"/> Email/calendar	<input type="checkbox"/> Canvas
<input type="checkbox"/> Web pages (www)	<input type="checkbox"/> Computer/drive access (Solar)
<input type="checkbox"/> One Card <input type="checkbox"/> Other: _____	
Reason for Access: _____	
Effective Date: _____	Department Name: _____
Expiration Date*: _____	Department #: _____
Requested by (AA): _____	Title: _____ Extension: _____
<p>My signature below certifies that the above named individual requires system access and/or access to data in a computer-based information system because such access is necessary in the ordinary course of fulfilling responsibilities to the university. I understand my obligation to ensure training is provided to this so that they understands the state and federal laws and University policies that govern access to and use of information contained in employee, applicant, and student records including data accessible through computer-based information systems.</p>	
Signature: _____	Date: _____

* Expiration Date must be in relation to services provided and cannot exceed one year. A new form will need to be submitted to extend services beyond this date.

FOR EMPLOYMENT SERVICES USE ONLY	
The individual identified above is approved and certified to receive access.	
_____ (print name)	Signature: _____ Date: _____
VP Approval Needed: <input type="checkbox"/> Yes <input type="checkbox"/> No	Signature: _____ Date: _____
Person of Interest Type: _____	Empl ID #: _____ Processed by: _____ Date: _____

Access and Compliance Form

University Information Systems

EMPLOYEE

I certify that I have received training regarding state and federal laws and University policies that govern access to and use of information contained in employee, applicant, and student records, including data that is accessible through University Information Systems (e.g. PeopleSoft).

I understand that I am being granted access to this information and data based on my agreement to comply with the following terms and conditions:

- I will comply with state and federal laws and University policies that govern access to and use of information accessible through a University information system. While a current summary of state and federal laws are described below, these laws may be revised that may necessitate additional training and requirements.

The California State University (CSU) has responsibility to protect sensitive personal data and maintain confidentiality of that data under the Information Practices Act (IPA) and Title 5.

The Information Practices Act, California Civil Code §1798, et seq., requires the Chancellor's Office and campuses to collect, use, maintain, and disseminate information relating to individuals in accordance with its provisions (<https://www.calhfa.ca.gov/privacy/ipa.pdf>). The CSU is obligated under IPA to disclose any breach of system security to California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. General Counsel's Records Access Manual located at http://www.calstate.edu/gc/Docs/Records_Access_Manual.doc addresses the IPA disclosure requirements.

Additionally, §42396 through §42396.5 of Title 5 of the California Code of Regulations (<http://ccr.oal.ca.gov/>) address privacy and the principles of personnel information management.

Additional documents on protecting confidential data are available at Human Resources' Policy Web site at <http://www.calstate.edu/HRAdm/policies.shtml> (under Confidentiality/Protection of Personal Data).

- My right to access information and/or data is strictly limited to the specific information and data that is relevant and necessary for me to perform my job-related duties.
- I will maintain the privacy and confidentiality of information or data that I obtain, including storing and disposing of the information so it remains confidential.
- I will secure access to confidential/sensitive data by taking appropriate actions, which may include, but are not limited to, locking the data in cabinets or my office, signing off the system when not actively using it, not leaving data open on the computer screen or my desk, etc.
- Before sharing information or data with others, electronically or otherwise, I will make reasonable efforts to ensure that the recipient is authorized to receive that information or data.
- I will sign off the University Information System(s) prior to leaving the terminal/PC.
- I will keep my password(s) to myself, and will not disclose them to others unless my immediate supervisor authorizes such disclosure in writing.

I understand that if I intentionally misuse personal information or data that I obtain through my employment, I may be subject to corrective (counseling and reprimands) or disciplinary (i.e., suspension, discharge, or downgrade) action pursuant to the applicable California Education Code provisions and collective bargaining agreements.

I certify that I have read this Access and Compliance Form, I understand it, and I agree to comply with its terms and conditions.

Name (please print)

Signature

Date

Title

Email

Overview: Here are some key requirements to keep in mind, and some critical resources to check, when making decisions or taking actions that could impact information security for the campus.

[Section 8000 of the Integrated CSU Administrative Manual](#) states that it is the collective responsibility of all users to ensure:

- Confidentiality of information that the CSU must protect from unauthorized access;
- Integrity and availability of information stored on or processed by CSU information systems;
- Compliance with applicable laws, regulations, and CSU/campus policies governing information security and privacy protection.
<https://it.sonoma.edu/kb/security/information-security-policies-and-standards>

Electronic Communications Responsible Use -
<https://calstate.policystat.com/policy/6607908/latest/>

Family Educational Rights and Privacy Act (FERPA) -
<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
Protects the privacy of students enrolled in an institution of higher education. Federal regulations prohibit the disclosure of a student's information to anyone other than the student without the student's written permission except for the parent of a dependent student. Students must be allowed access to their student records.

Information Practices Act of 1977, California Civil Code -
<https://www.calhfa.ca.gov/privacy/ipa.pdf>
“...the right to privacy is a personal and fundamental right...” The Information Practices Act, Section 1798 of the California Civil Code, places specific requirements on state agencies in relation to the collection, use, maintenance and dissemination of information relating to individuals. **Careless, accidental or intentional disclosure** of information to unauthorized persons can have far-reaching effects, which may result in disciplinary action against those involved (Section 1798.55) and civil action against the CSU.


Title 5, California Code of Regulations - <http://ccr.oal.ca.gov/>
Personal information should not be transferred out of the CSU unless such transfer is compatible with the disclosed purpose for which it was collected.

The Corporation for Education Network Initiatives in California (CENIC) and Digital California Project (DCP) - Acceptable Use Policy - <http://www.cenic.org/calren/aup.html>
Requires educational institutions to handle and protect confidential information. Users must not use Level 1 and Level 2 data for profit making activities, partisan politics, or stalking. If policies are not followed or information is used for these activities and not caught, then it is possible the University could lose access to the Internet entirely.

CSU Data Classification Standard - (Defines Level 1 and Level 2 data)
https://it.sonoma.edu/sites/it/files/files/8065_final_draft_data_classification_cw_v4.pdf

State Administrative Manual - <http://sam.dgs.ca.gov/TOC/4800/default.htm>

Quick Reminders:

Keyboard Shortcut:  + ‘L’
‘Windows’ key and ‘L’ will lock your workstation instantly. Should not replace logging off or shutting down your workstation.

Screen-Saver Password
Macs and PCs alike allow the user to require passwords to be used when exiting a screen-saver.

Work Purposes Only
Only use the information that you have access to for work related activities.

Do Not Share Passwords
Do not tape passwords in plain sight or under a keyboard. Keep them unique from personal ones. Do not let others log into any of your account(s).

Clear Desk
Keep your desk clear of confidential documents. Flip over or cover up any documents when guests enter your workspace.

Use Common Sense
Treat all information, even if you are unsure if it contains Level 1 or Level 2 data, as if it were your own.

Secure Handling of Level 1 data
Never communicate Level 1 data over unsecured channels (applies to electronic mail). Email is not approved for Level 1 data. SSNs, credit card information, or other highly sensitive information should never be transmitted or stored in an unsecure manner (see [CSU Information Security Policy and Data Classification Standard](#) for more detailed information).

Ask
If you ever have any doubt about how to handle confidential data or have questions about any of the policies, ask your appropriate administrator or the [Information Security Office](#).