



CruzID Computer Account Form

University of California, Santa Cruz

What to do with your completed form:

Mail this form *or* fax it to the IT Support Center: **Fax:** (831) 459-4171
Kerr Hall room 54, UCSC Santa Cruz, CA 95064
or send it via campus mailstop: ITS-Kerr

Questions? Call us:
Phone: (831) 459-4357

Name (First MI Last)	Can be reached phone number	Alternate Email
Campus Location (Room number and building)	Unit/Division	Hire Date
Applicant's Supervisor (Sponsor)	Supervisor's Email	Supervisor's Telephone

Create an Account Claim Code:

- Note, Sundry Account Holders cannot print in IC Labs
- **This is not your password.** You will create a new password after you claim your account.
Your claim code must:
 - be at least 8 characters in length
 - contain a mixture of upper and lower case letters, numbers, and symbols
 - be difficult to guess (e.g. don't include real words or personal information like user name, names of family members, places, pets, birthdays, addresses, hobbies, etc.)

Account Claim Code

Agreement: My signature on this application constitutes my receipt of and intention to comply with the University policies governing the use of this account. I have received a copy of these policies. I also understand that I am responsible for any service authorizations requested and I will not disclose my private claim code in any manner. **All applicants must sign below.**

Applicant Signature	Date
---------------------	------

IT Account Service Team Internal use only			
ITR Ticket Number	Date Received	Date Notified	Completed by

Policies for Use of UCSC Computing Facilities

It is the policy of the University of California to provide computer resources to students, faculty, and staff to be used in ways that are consistent with the University's mission – instruction, research, and public service – and in activities that support that mission, such as administration. These resources include computers, terminals, networks, modems, and printers.

It is the policy of the University to provide its users with access to local, national, and international sources of information, access to a rich collection of services, and open and free discussion. The University expects that its user community will respect the public trust through which these resources have been provided. The work and efforts of the user community should not be subject to unauthorized disclosure, tampering, destruction, theft, harassment, nor should there be a denial of access to resources.

All users of campus computing resources share in the responsibility to protect the rights of the entire community. All users must guard against abuses of the University's information resources and systems.

The University has determined that the following list, while not exhaustive, characterizes unacceptable behavior, which may be subject to disciplinary action:

1. Use of any University facilities in a manner that violates copyrights; patent protections, or license agreements.
2. Attempts to gain unauthorized access to any information facility, whether successful or not. This includes running programs that attempt to calculate or guess passwords, or that are designed and crafted to trick other users into disclosing their passwords. It also includes electronic eavesdropping on communications facilities.
3. Any violation of state law as described in the Penal Code. As an example, a copy of Section 502 of the California Penal Code is available separate from this policy statement.
4. Any action that invades the privacy of individuals of entities that are the creators, authors, users, or subjects of information resources.
5. Any action that disrupts the availability of a system for others, such as running programs that utilize all system resources and prevent others from making productive use of the system.
6. Any use of University computing facilities for personal gain (including advertising) or political purposes without the prior approval of the University.
7. Any use of University computing facilities to harass others.
8. Attempts to alter, damage, delete, destroy or otherwise abuse any computer or network resource.

In addition, the user should be aware of the following policies and expectations:

The University grants permission to members of its community to use computation resources by issuing individual computer accounts. As a condition of receiving such an account, the user must exercise diligence to keep his or her password as a secret and not disclose it to any other person. Users of shared computers or, networks, which connect to the campus network, should not share or transfer their account privileges to any other person.

The University expects that all those who choose to use our offcampus network connections will understand and honor the policies

of those regional and national network organizations to which the University is a party. The use policies for these networks are available separately from this policy statement.

Campus units that administer computers may also establish guidelines for the appropriate use of their equipment in addition to these campus-wide policies. These guidelines must be consistent with campus-wide policies.

When a non-University-owned computer is used on campus, the user must follow all of these campus-wide policies. In addition, if the computer is attached to the campus network it must be registered with the owner's name and contact information, machine manufacturer and model number, location of machine, and the network address of the machine. This registration can be done through divisional computer/network managers or through CATS. This includes computers with one or more unique network addresses

as well as computers that obtain network addresses on a dynamic basis.

Account usage is also governed by the University of California Electronic Communications Policy. Full text of the policy is available at this URL:

<http://www.ucop.edu/ucophome/policies/ec>

Your Temporary Password

Your CruzID account is secured by a password that is known only to you. Your CruzID account gives you access to resources, which, in the wrong hands, can be misused.

You are responsible for every use of your account and therefore you should never share your password, or make it easy to guess.

Your password should not be a real word, but rather a string of characters something like a word that you can remember.

Examples

of good passwords are: m**nshadow, Iderful A&Z\$.

Passwords must have one character that is non-numeric, and it must be at least six characters long. If you use a symbol such as &, *, ?, it can be four characters long.

How to change your password

Directions and a web form can be found at:

<http://www2.ucsc.edu/cats/sc/services/change-password.shtml>