OPEN COMPUTING FACILITY Group Account Application Form

1. **Pick an account name.** It must consist of between three and eight lowercase letters (no spaces, numbers, underscores, or other symbols), and it must be based on the group's name or initials.

Requested Account Name: ___ ___ ___ ___ ___ ___ ___ ___

2. **Pick a password.** The password must be at least eight characters long, and it may contain upper and lowercase letters, numbers or other symbols. However, it may not be a word in any language. Good passwords are usually a combination of upper and lowercase letters and numbers. You will type your password in when your account is approved. **Do not write your password on this form.**

3. **What is the responsible party's name?** This is the name of the person who will be responsible for the account.

Full Name: _____

4. **What is your group's name?** Write your group's name in your preferred spelling, including capitalization. If the group's name is longer than 32 letters and spaces, write the way you'd like it abbreviated. Be sure to include all the parts of the name that the account name above is based on.

Group Name: _____

5. **How is the group affiliated with the University?** Check one of the following, and provide the requested information.

☐ The group is registered with the Office of Student Life (OSL), and you are a signatory.
☐ The group is OSL registered, and you have been authorized by a signatory to be responsible for the account.
Signatory's name: _____
☐ The group is affiliated with a campus department. Department Name: _____

6. **How can we contact you?** Because of the system we are currently using, it will take a few days before your account is created. Please write your e-mail address below so the OCF can contact you when your account has been created.

E-mail Address: _____

7. **Read our disclaimer.** Please read the following, as you are responsible for knowing and following these policies.

Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Students and employees may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files as required to protect the integrity of computer systems. For example, system administrators may access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.

All existing laws (federal and state) and University regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct.

Misuse of computing, networking, or information resources may result in the loss of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable University or campus policies, procedures, or collective bargaining agreements. Illegal reproduction of software protected by U.S. Copyright Law is subject to civil damages and criminal penalties including fines and imprisonment.

Examples of misuse include, but are not limited to, the activities in the following list:

1. Using a computer account that you are not authorized to use. Obtaining a password for a computer account without the consent of the account owner, or sharing your own account.
2. Using the Campus Network to gain unauthorized access to any computer systems.
3. Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
4. Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network. This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.
5. Attempting to circumvent data protection schemes or uncover security loopholes.
6. Violating terms of applicable software licensing agreements or copyright laws.
7. Using electronic mail or communication to harass other users.
8. Posting materials on electronic bulletin boards that violate existing laws or the University's codes of conduct.
9. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.
10. Using OCF or University equipment or resources for commercial purposes unless specifically authorized.

8. **Sign this form.**

By signing below, I certify that the information that I have provided is complete and accurate. I have read, understood, and agreed to follow the above policies. In addition, I agree not to hold the University of California, the Associated Students of the University of California, or the Open Computing Facility (OCF) responsible for lost files or other misfortunes which may result from my use of the OCF's facilities.

Signature: _____ Date: _____

9. **Find a staff member.** He or she will check your ID, enter the information into a computer, and allow you to type in your password.

OCF STAFF USE ONLY: Approved By (Staff Username): Date: / /20
☐ Approval Completed (Make sure to check university ID, signature, and that username is not taken)
☐ Account Created and E-mailed Group