SCCCD Technology Authorization Form

Colleague ❖ **Exchange Email** ❖ **Network Account** ❖ **Phone/Voice Mail**

STEP 1 - THIS SECTION TO BE COMPLETED BY HUMAN RESOURCES OR COLLEGE BUSINESS OFFICE

Last Name: _____ First Name: _____ Preferred First Name: _____

District Office ☐ _____ Clovis Community College ☐ _____ Effective Date: _____

Fresno City College ☐ _____ Reedley College ☐ _____ Notes: _____

Department/Division: _____ Colleague Employee ID# _____

Classified: _____ Academic: _____ Other: _____ Title:

Step 1 - ***email*** Dept Manager or Higher

Next section must be approved by Department Manager or Higher

STEP 2 - COMPUTER ACCOUNT REQUEST - SECTION TO BE COMPLETED BY DEPARTMENT MANAGER

New Colleague Account: ☐ **Change Colleague Account:** ☐ **Email Account Only:** ☐ **Phone:** ☐ **Voice Mail:** ☐ **Ext:** _____

Colleague access required (or Security Group): ** _____

(** Best Described as… "Same as another Employee in the same department" OR "List Specific mnemonics being requested" **)

Approved By (Type First/Last Name): _____ Job Title: _____

Print Computer Use Policy: ☐ eSignature: _____ Date: _____

Step 2 - ***email*** District / College Technology Dept.

Next section must be approved by District/College Technology Department

STEP 3 - THIS SECTION TO BE COMPLETED BY _____ DEPARTMENT

System Manager: _____ Date _____

AD Account Name _____ Tel. Ext. _____ Mail Store: ▼ Other: _____

Script: _____

Division/User Notification: _____ **New email account:** ☐ **Change email account:** ☐

Primary Address _____ _____ _____ AD Group Membership(s)

Alias Address _____ _____ _____

Alias Address _____ _____ _____

Global Distribution List – ▼ **Mailall :** _____

Step 3 - ***email*** DO - IS

Next section must be approved by District Office Technology Department

STEP 4 - THIS SECTION TO BE COMPLETED BY DISTRICT INFORMATION SYSTEMS DEPARTMENT

Colleague Account Manager: _____ Date: _____ Division/User Notification: _____

Colleague Account Name: _____ Notes / Comments: _____

Colleague: _____ SVM: _____ GLUD: _____ CSHS: _____ AD Grp: _____

Step 4 - ***email*** Submit to All

Completed form must be sent to Employee, HR, Manager and Technology Lead

Back to Authorization Form

Print Computer Use Policy (Pages 2-5 Only)

SCCCD – Computer Use Policy

1. INTRODUCTION

State Center Community College District ("SCCCD") owns and operates a variety of computer systems for use by its faculty, students, and staff. SCCCD encourages the use of its computer systems for education, academic development, public service, and other educational related purposes. When using SCCCD computer systems, all users are required to abide by the rules of this Policy and use the system in an ethical and lawful manner.

2. POLICY REQUISITE

All users of SCCCD computing systems must read, understand, and comply with the terms outlined in this Policy, as well as any additional guidelines established by the administrator of the system. BY USING ANY OF THESE SYSTEMS, USERS AGREE THAT THEY WILL COMPLY WITH THESE POLICIES. Users understand and agree that SCCCD role in managing these systems is only as an information carrier, and that they will never consider transmission through these systems as an endorsement of contents of such transmission by SCCCD.

3. RIGHTS

These computer systems, facilities, and accounts are owned and operated by SCCCD. SCCCD reserves all rights, including disruption of service without notice, to the computing resources which it owns and operates. These procedures shall not be construed as a waiver of any rights of SCCCD, nor shall they conflict with applicable law.

4. AUTHORIZED USE

Access and privileges on SCCCD computing systems are assigned and managed by the administrator of the specific system. Eligible individuals may become authorized users of the system and be granted appropriate access and privileges by following the approval steps prescribed for that system.

An authorized SCCCD agent must approve all access to SCCCD computer resources, including issuing of passwords. Users may not, under any circumstances, transfer or confer these privileges to other individuals. Others shall not use any account assigned to an individual without written permission from the system's administrator. The authorized user is responsible for the proper use of the system, including any password protection.

5. PERMISSIBLE USE

Electronic communications facilities (such as e-mail **and voice mail**) are mainly for district-related activities. **While at times conducting personal business from SCCCD facilities may be unavoidable, such uses shall be kept to a minimum.** Further, users are responsible for maintaining the following:

An environment in which access to all of SCCCD computing resources is equitably shared between users. The administrator or area manager will set minimum guidelines within which users must conduct their activities.

An environment conducive to learning: Many of the SCCCD computing systems provide access to outside networks, both public and private, which furnish electronic mail, information services, bulletin boards, conferences, etc. Users are advised that they may encounter material that may be considered offensive or objectionable in nature or content. Users are further advised that SCCCD does not assume responsibility for the contents of any of these outside networks.

The user agrees to comply with the acceptable use guidelines for whichever outside networks or services they may access through SCCCD systems. The user agrees to follow proper etiquette on outside networks. Documents regarding etiquette are available through specific individual networks. The user agrees that, in the unlikely event that someone does transmit, or cause to be transmitted, a message that is inconsistent with an environment conducive to learning or with a misleading origin, the person who performed the transmission will be solely accountable for the message, not SCCCD, which is acting solely as the information carrier.

Any user who finds a possible security lapse on any system is obligated to report it to the system administrator. **Before gaining access to the internet from SCCCD facilities, users will have to agree to SCCCD computer use policies as stated herein.**

Within the guidelines stated above, confidentiality among students, faculty, and staff will be strictly maintained.

6. PROHIBITED USES

Use of any and all of SCCCD computer systems for any of the following purposes is strictly prohibited. Liability for violations of prohibited uses shall remain solely and exclusively with the user. By using SCCCD computer systems, the user further agrees to indemnify SCCCD for any liability incurred by SCCCD for misuse by the user.

An individual's computer use privileges may be suspended immediately upon the discovery of a possible violation of these privileges. Such suspected violations will be confidentially reported to the appropriate system administrator or area manager.

Violations of these policies will be considered violations of District policies dealing with misuse or abuse of District property, and may result in disciplinary action. In such event, the full range of disciplinary sanctions is available.

COPYRIGHT INFRINGEMENT

Computer software protected by copyright cannot be copied from, into, or by using campus computing facilities, except as permitted by law or by the contract with the owner of the copyright. This means that such computer and microcomputer software may only be copied in order to make back-up copies, if permitted by the copyright owner. The number of copies and distribution of copies may not be done in such a way that the number of simultaneous users in a department exceeds the number of original copies purchased by that department.

DEFAMATION - LIBEL/SLANDER

Creation or transmission of any false statement which tends to cause injury to one's reputation is strictly prohibited. Any user creating or transmitting defamatory statements shall have sole liability for any damages resulting from such defamatory statement. Users will also be subject to SCCCD disciplinary procedures set forth in the Governing Board Policy. The user agrees never to attempt to transmit, or cause

to be transmitted, any message in which the origination is deliberately misleading (except for those outside services which may conceal identities as part of the service).

OBSCENE MATERIAL

Creating, transmitting, uploading, or downloading obscene materials is a strictly prohibited use of SCCCD computer systems unless the materials are parts of approved courses of SCCCD Curriculum. "Obscene matter" means matter taken as a whole, the predominant appeal of which to the average person, applying contemporary statewide standards, is to prurient interest, meaning a shameful or morbid interest in nudity, sex, or excretion; and is matter which taken as a whole goes substantially beyond customary limits of candor in description or representation of such matters; and is matter which taken as a whole lacks significant literary, artistic, political, educational, or scientific value. Any user violating this provision may be subject to applicable criminal and civil penalties. Civil liability shall be solely and exclusively with the user.

COMMERCIAL USE

Commercial use of SCCCD computer systems is prohibited **except for company sponsorships approved by the chancellor or chancellor's designee.**

DOWNLOADING PROGRAMS

Downloading of executable files to SCCCD computer systems is not encouraged and is done solely at the user's risk. SCCCD computer personnel will not support downloaded files and any problems caused by such a download are solely the user's responsibility.

Violations of some of the above policies may constitute criminal offenses.

The user agrees never to use the system to perform an illegal or malicious act as set forth in this section. Any attempt to increase the level of access to which the user is authorized, or any attempt to deprive other authorized users of resources or access to any SCCCD computer system shall be regarded as malicious, and may be treated as an illegal act.

7. ACCOUNTS

Others must not use an account assigned to an individual without written permission of the system administrator. The individual is responsible for the proper use of the account, including password protection.

8. CONFIDENTIALITY

Programs and files are confidential unless they have been made available, with written permission, to other authorized individuals. **SCCCD reserves the right to access all information stored in SCCCD computers**. File owners will be notified of file access and/or maintenance, in advance, if such notice is practical. When performing maintenance, every effort is made to ensure the privacy of the user's files. However, if policy violations are discovered, they will be reported immediately to the appropriate system administrator.

The system has the ability to read your mail: your own account, and the system administrator account. All reasonable attempts have been made to ensure the privacy of your accounts and your electronic mail; this is no guarantee that your accounts or your electronic mail is private.

9. SYSTEM PERFORMANCE

No one should deliberately attempt to degrade the performance of the computer system or to deprive authorized personnel of resources or access to any college computer system.

10. UNAUTHORIZED ACCESS

Loopholes in computer security systems or knowledge of a special password shall not be used to damage the computer system, obtain extra resources, take resources from another user, gain access to systems or use systems for which proper authorization has not been given.

11. ADDITIONAL GUIDELINES

SCCCD retains the right to revoke, amend, or change the provisions of this Policy. The system administrator or area manager will establish more detailed guidelines, as needed, for specific computer systems and networks. These guidelines will cover such issues as allowing connect time and disc space, handling of irretrievable mail, responsibility for account approval and other items related to administering the system. **All changes to this regulation are subject to the regular approval process that applies to all administrative regulations. In addition, there will be a notification period before such changes result in disciplinary action.**

Employee Name: _____ Title: _____

Signature: _____ Date: _____