STANISLAUS COUNTY COMMUNITY SERVICES AGENCY	Developed by/Date: Per Old DSS Manual Prior to 2002, Information Systems 5/14/08, Rev 2/11	Page: 1 of 3	Number: 4.1
			Category: Information Technology
	Reviewed by/Reviewed Date: CSA Exec Team 11/08, Rev 2/11	Replaces:	Distribution: All Staff

Title: **Information Technology Security Policy**

Approved: 2/7/11

Policy [√] **Procedure** [ ] **Guideline** [ ]

Purpose

The purpose of this policy is to state the rules established by this agency to safeguard CSA IT resources, equipment, and information. This policy applies to all users of CSA/County-owned or leased IT resources. For purposes of this policy, the term user refers to any employee (permanent or temporary), contractor, consultant, vendor, volunteer, student, or other person who uses, maintains, manages or is otherwise given access privileges to CSA/County IT systems. Additionally, the phrases "IT system" and "IT resources" include all computer hardware (including peripherals), software applications and data (including electronic communications), networks, and network connections (including to the Internet).

Workplace Privacy

All forms of messages/documents/information, including but not limited to e-mail and GroupWise Messenger, created/sent/stored on CSA IT resources and communications systems is the property of the County and subject to disclosure upon the demand of the County at any time. Systems administrators are authorized to examine and/or retain files within the scope of their responsibilities. This includes but is not limited to troubleshooting and/or repairing County IT resources. System administrators must not disclose the contents of such files unless the contents are in violation of this policy, other County, department, or agency policies, or federal, state, or local law. Content in violation of policies or the law will be reported to management.

Ethics/Confidentiality

All CSA customers have the right to have their records kept confidential by the county and state; this includes any records stored in CSA, County, and State computer systems or networks. Violating a customer's confidentiality rights is a violation of California State law. Accessing these records for any reason, other than in the course of official duty, is punishable as a misdemeanor. Accessing these records for any reason, other than in the course of official duty, and using the information for personal gain is punishable as a felony. Entering a case of a friend, family member, co-worker or person otherwise known to you constitutes a conflict of interest, is strictly prohibited, and subject to disciplinary action. If an accidental conflict of interest occurs, supervisory staff must be notified.

In addition, any person who knowingly and willingly accesses any computer system or computer network without proper permission is guilty of a public offense as described in Section 502(c) of the California Penal Code.

General Use

CSA's computer and communications systems are solely intended for appropriate business use. Users may use CSA's e-mail system, E-fax and Internet access for personal use on their own time, i.e., break and lunch time; however, the rules of this policy apply at all times. GroupWise Messenger is restricted to business use only at all times. CSA management reserves the right to require the employee to modify or delete e-mail, software, or any other personal computer data. All data or software from sources external to the CSA network must be virus checked. CSA management can review material stored and transmitted on CSA computer systems at anytime and there is no expectation of privacy.

When using CSA computers and communications systems (including e-mail, E-fax and instant messaging) all employees must adhere to the following rules:

- **DO NOT** conduct illegal activity.
- **DO NOT** create, send, or store any material (i.e., text documents, jokes, cartoons, sound, or movie bytes) that may be considered offensive/harassing if it relates to any individual or group's race, color, sex, sexual orientation, national origin, religion, disability, political belief, or age.
- **DO NOT** use unauthorized software. Authorization requests must be submitted to Information Systems for approval; approved software must be installed only by Information Systems Technical Support staff. Under no circumstances will authorization be given to install unlicensed software on CSA equipment or allow multiple use of single user software. Technical Support staff has the authority to delete unauthorized software when detected; supervisors will be notified. Software licensed to CSA may not be installed on an employee's personal computer.
- **DO NOT** give your password to another person. If a password is compromised for any reason, the password shall be changed as soon as practical. Directly accessing the CSA network under another user's User ID is prohibited.
- **DO NOT** send chain letters or pyramid letters. A chain or pyramid letter is a letter or e-mail sent to a number of persons, each of whom makes and sends copies to a number of other persons who likewise do the same.
- **DO NOT** open e-mail attachments that are executable files. These files may be identified by extensions including, but not limited to, .exe, .zip, .com, .bat, and .vbs.
- **DO NOT** send "All Staff" e-mails without managerial approval.
- **DO NOT** use any communication system for purposes of solicitation (i.e., AVON, Tupperware, used cars, time bank).
- **DO NOT** use GroupWise Messenger for non work related personal correspondence between users.
- **DO NOT** forward or set up a rule to automatically forward emails containing PII or customer/case information to a personal email address or to someone without a business need to know.

Internet Access

Internet access is provided to designated CSA employees and is intended for business purposes. When accessing the Internet through CSA equipment, the employee must adhere to the following rules:

- **DO NOT** download any shareware or executable programs. Executing a program means to run a program or perform a program language instruction. These files may

be identified by extensions including, but not limited to, .exe, .zip, .com, .bat, and .vbs.

- **DO NOT** download or stream (play live) any video or music files that are not directly work related. These files use excessive amounts of Internet bandwidth and storage space. These files may be identified by extensions including, but not limited to: .wav, .mid, .wma, .pls, .mp3 .m3u, .avi, .mpeg, and .mpg. This includes playing the radio on your computer, watching news "clips", sports events, movie previews, TV show excerpts, and more.
- **DO NOT** use any external proxy services.
- **DO NOT** access external web based e-mail systems.
- **DO NOT** make any attempts to bypass CSA's forbidden site policies.
- **DO NOT** follow any links or searches that would reflect unfavorably on CSA, if it were disclosed publicly.
- **DO NOT** accept or assign any charges for Internet access to the County or CSA.
- **DO NOT** provide any CSA or County credit card number to any Internet site unless authorized to do so by Office Services.
- **DO NOT** employ ANY methods to circumvent the above listed restrictions.

User Agreement

Each employee will read the above policy and security agreement. Any violation of this policy can result in immediate disabling of a users account and may lead to disciplinary action.