USE OF *DEPARTMENT* COMPUTERS

GENERAL ORDER #7.03

Adopted: 12/13/05
Replaces: Stanford G.O.'s #2.1.33.3, 2.1.33.4, 2.1.33.5

****

POLICY

Employees of the *Stanford University Department of Public Safety* shall adhere to the guidelines set forth in the *University's various computer user policies (located in Stanford University's Administrative Guide Memo 61 through 64)* as well as the *Department of Public Safety's computer use policy. The SUDPS policy may, at times, be more restrictive than the University's policy due to confidential and sensitive nature of law enforcement information.* Employees of the *Stanford University DPS* shall observe all laws, agreements, and policies regarding the confidentiality of information obtained by use of *University or Department* computers and computer equipment.

PROCEDURE

A. USE OF COMPUTERS AND COMPUTER EQUIPMENT

1. This Order is applicable to the use of computers and computer equipment owned or operated by the *Stanford University Department of Public Safety. Department computers and computer equipment shall only be used for SUDPS job-related purposes. Use of SUDPS computers and computer equipment for personal use is not permitted without prior written approval from the employee's immediate supervisor, except as specifically described in later sections of this General Order.*

Personal computers shall not be used while on duty without the prior initial approval of a supervisor and the approval of the Support Services Manager.

2. The *Stanford University DPS Support Services Manager is responsible for overall network administration and security. The Information Technology Systems Administrator reports to and supports the SUDPS Support Services Manager in*

his/her role as the systems data and security administrator. The IT Systems Administrator manages the day-to-day operation of the computer systems within the department. These support functions may include any or all of the following functions: database management, software distribution and upgrading, user profile management, version control, backup & recovery, virus protection and performance and capacity planning. The *IT Systems Administrator* is responsible for issuing all *Department* computers and computer equipment.

3. Only personnel *designated by the Support Services Manager or the IT Systems Administrator* are authorized to move or relocate desktop computers and associated computer equipment.

4. Computers *shall* only contain software and *applications* authorized and installed by *IT Systems Administrator* or his/ her designee. An employee who wishes to add or delete software or to have the standard *desktop configuration* altered for any reason shall obtain *prior* approval from the *IT Systems Administrator*.

5. *Computer users shall respect copyrights and licenses to software, entertainment materials, published and unpublished documents, and any other legally protected digital information.*

6. *Computer users shall not encroach on others' access and use of the Department's computers, network, or other information resources, including digital information. This includes but is not limited to: attempting to access or modify personal, individual, or any other department information for which the user is not authorized; attempting to access or modify information systems or other information resources for which the individual is not authorized; sending chain-letters, unsolicited bulk electronic mail either locally or off-campus; printing excess copies of documents, files, data or programs; running grossly inefficient programs when efficient alternatives are known by the user to be available; unauthorized modification of system facilities, operating systems, or disk partitions; attempting to crash or tie up a university computer, network or other information resource; or otherwise damaging or vandalizing University or Department computing facilities, equipment, software, computer files or other information resources.*

7. *Computer users shall not intentionally develop or use programs which disrupt other computer or network users or which access private or restricted information or portions of a system and/or damage software or hardware components of a system.*

8. *Computer users shall refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access.*

9. Purchases of any *Department* computers, computer equipment, and software must be authorized and approved by the *Support Services Manager*.

10. *Stanford University DPS* employees *shall* respect the confidentiality and sensitivity of information held in *Department* computers and will only disclose information to persons who have a legitimate need for it and who are authorized to receive it.

11. Periodic physical audits and virus scans of computer equipment may be conducted by the *Support Services Manager and/or the IT Systems Administrator*.

12. Games shall not be operated on *Department*-owned equipment.

13. Remote access to *Stanford University DPS* computing equipment must be authorized in advance by the *Support Services Manager and the IT Systems Administrator*.

14. No dialup modems may be attached to *Department*-owned equipment without authorization from the *IT Systems Administrator*.

15. *Only Department issued storage media (including but not limited to: diskettes, USB storage, CD, DVD etc.) will be used on Department computers.*

B. RESPONSIBILITIES FOR LAPTOP COMPUTERS

1. Each laptop user is responsible for:

a. *Exercising an appropriate level of care when using the laptop, to include adequately protecting the computer from damage or theft.*

b. Not adding personal software.

c. Promptly notifying *the IT Systems Administrator* of non-working software or hardware.

d. Using only the password issued by *the IT Systems Administrator* to secure the laptop and its applications.

e. Regularly backing up data to disk *or other storage media and copying that data to a network drive.*

2. *The Department's IT Systems Administrator* is responsible for:

a. Providing training *as needed* for the use and care of the laptop.

b. Returning crashed systems with original software only. *The retrieval of user's data cannot be guaranteed.*

c. Providing upgraded software.

d. Performing periodic audits of laptops to determine or detect:

1). The upgrade version.

2). Any non-working software or hardware.

3). Any virus infection.

4). Any unauthorized software.

e. Distributing *and assigning laptop computers to Department personnel.*

f. Inventory maintenance: maintaining a record of each laptop by division, current user, software inventory, and asset number.

g. Issuing and tracking loaner laptops when needed to replace those in for repair.

C. USE OF THE *STANFORD UNIVERSITY & DEPARTMENT OF PUBLIC SAFETY* NETWORKS

1. *Usage – Computer users shall respect the rights of other computer users. Most University systems provide mechanisms for the protection of private information from examination by others. Attempts to circumvent these mechanisms in order to gain unauthorized access to the system or to another person's information are a violation of University and Department policy and may violate applicable law. Authorized systems administrators may access computer users' files at any time for maintenance purposes, audits and in situations where information contained in an employee's computer files are needed for work related purposes and the employee is not at work to retrieve the needed information. Systems administrators will report suspected unlawful or improper activities to the proper authorities.*

a. *Prohibited Use – Use of the University and Department's computers, networks, or electronic communication facilities (such as electronic mail*

or instant messaging, or systems with similar functions) to send, view, or download fraudulent, harassing, obscene (i.e., pornographic), threatening, or other messages or material that are a violation of applicable law or University policy, such as under circumstances that might contribute to the creation of hostile work environment, is prohibited.

b. *Mailing Lists – Users must respect the purpose and charters of computer mailing lists (including local or network news groups and bulletin boards). The user of an electronic mailing list is responsible for determining the purpose of the list before sending messages to or receiving messages from the list. Subscribers to an electronic mailing list will be viewed as having solicited any material delivered by the list as long as that material is consistent with the list's purpose. Persons sending to a mailing list any materials which are not consistent with the list's purpose will be viewed as having sent unsolicited material.*

c. *Advertisements – In general, the University and department's electronic communication facilities should not be used to transmit commercial or personal advertisement, solicitation, or promotion. Some public bulletin boards have been designated for selling items by members of the Stanford community, and may be used appropriately, according to the stated purpose of the lists(s).*

d. *Information Belonging to Others – Users must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords, or other digital materials belonging to other users, without the specific permission of those other users.*

e. *Political Use – University and department information resources must not be used for partisan political activities where prohibited by federal, state, or other applicable laws, and may be used for other political activities only when in compliance with federal, state, and other laws and in compliance with applicable University and department policies.*

f. *Personal Use – University and department information resources should not be used for personal activities not related to appropriate University or department functions, except in a purely incidental manner. No Stanford University DPS employee shall use the network, its systems, or its data for personal profit for him or herself or for any other person; unlawful or illegal activities; or the creation or dissemination of harassing or demeaning statements towards any individual or group.*

g. *Commercial Use – University and department information resources should not be used for commercial purposes, except in a purely incidental manner or except as permitted under other written policies of the University or with the written approval of a University officer having the authority to give such approval.*

D. *IDENTIFICATION AND AUTHENTICATION POLICY*

1. *Stanford University maintains a set of linked records identifying all employees, students, and others who use the University's computing resources. These records correlate SUNet ID, University ID, and Stanford Identification Card records.*

2. *Each identifier is unique; that is each identifier is associated with a single person or entity.*

3. *An individual may have no more than one University or department ID number and one personal SUNet ID.*

4. *Once an identifier is assigned to a particular person, it is always associated with that person. It is never subsequently reassigned to identify another person or entity.*

5. *Use of authentication information (user name and password) to identify oneself to an on-line system constitutes an official identification of the user to the University and Department, in the same way that presenting an ID card does. Users can be held responsible for all actions taken during authenticated sessions.*

6. *Integrity - Regardless of the authentication method used, users must use only the authentication information that they have been authorized to use; i.e., must never identify themselves falsely as another person or entity.*

7. *Confidentiality – Regardless of the authentication method used, users must keep their authentication information confidential; i.e., must not knowingly or negligently make it available for use by an unauthorized person. Department of Public Safety* personnel using the *department's* network should protect the security of their individual password(s).

8. *Security Precautions – Passwords and PINs should be chosen so that they are not easily guessable; e.g., not be based on the user's name and birthday.*

9. *Department of Public Safety* personnel using the *Department's* network shall log off from the system upon completion of use.

E. INTERNET USE FROM *DEPARTMENT OF PUBLIC SAFETY* COMPUTERS

1. Access to the Internet is provided as a business tool. Reasonable, incidental use for personal purposes is acceptable, so long as such use does not interfere with performance of work duties or the operation of *Department* information systems. *The activities listed below are prohibited except in the case where they have a demonstrated legitimate business purpose and have been approved by the individual's supervisor*.

2. *Accessing certain types of Internet sites is prohibited absent a legitimate business reason (i.e., investigative purposes), and only then with the prior approval of a supervisor. Prohibited sites include:*

a. *Adult/Sexually Explicit*

b. *Gambling*

c. *Games*

d. *Personals & Dating*

e. *Streaming Media*

f. *Spyware*

g. *Hacking*

h. *Phishing & Fraud*

3. All Internet access at the *Department of Public Safety* is *subject to being monitored by the IT Systems Administrator or designee*.

F. E-MAIL USE FROM *DEPARTMENT* COMPUTERS

1. *University* e-mail is provided as a business tool. Incidental use *of the University's e-mail system* for personal purposes *shall be allowed as* long as such use does not interfere with *the* performance of *one's* work duties or the operation of *the University* information systems *usage complies with all the guidelines set forth in this procedure.*

2. *The inclusion of quotes or personal sayings that reflect one's personal views (political, religious, or otherwise) as part of one's official department "signature" is not appropriate.*

3. *Employees shall not use University computers or systems to maintain or check non-University e-mail except in the course of an authorized investigation.*

4. *University* electronic mail systems and messages are not private. They remain the property of *Stanford University.* The *University* reserves the right to monitor the use of its electronic mail systems.

G. ***SYSTEMS ADMINISTRATOR RESPONSIBILITIES***

1. *While the University Trustees are the legal "owners" or "operators" of all computers and networks purchased or leased with University funds, oversight of any particular system is delegated to the head of each department, in this case, the Director of Public Safety. The Director may designate another person to manage the system. This designate is the "systems administrator" who has additional responsibilities to the University as a whole for the system(s) under his or her oversight. The Director of Public Safety has the ultimate responsibility for the actions of the systems administrator.*

2. *University Responsibilities – The systems administrator should use reasonable efforts to:*

a. *Take precautions against theft of or damage to the system components.*

b. *Faithfully execute all hardware and software licensing agreements applicable to the system.*

c. *Treat information about, and information stored by, the system's users in an appropriate manner and to take precautions to protect the security of a system or network and the information contained therein.*

d. *Promulgate information about specific policies and procedures that govern access to and use of the system, and services provided to the users or explicitly not provided. This information should describe the data backup services, if any, offered to the users. A written document given to users or messages posted on the computer system itself shall be considered adequate notice.*

e. *Cooperate with the systems administrators of other computer systems or networks, whether within or outside of the University, to find and correct*

problems caused on another system by the use of the system under his or her control.

3. <u>*Policy Enforcement*</u> *– Where violations of this policy come to his or her attention, the systems administrator is authorized to take reasonable actions to implement and enforce the usage and service policies of the system and to provide for security of the system.*

4. <u>*Suspension of Privileges*</u> *– A systems administrator may temporarily suspend access privileges if he or she believes it necessary or appropriate to maintain the integrity of the computer system or network. The systems administrator shall report any violations or suspected violations of this policy to the Director of Public Safety through the Support Services Manager.*

H. ***CONSEQUENCES OF MISUSE OF COMPUTING PRIVILEGES***

1. *A user of University or Department information resources who is found to have purposely or recklessly violated any of these policies may be subject to disciplinary action up to and including termination and/or legal action.* Inappropriate or offensive use of the systems includes, but is not limited to: sexually explicit images, messages, or preferences, ethnic or racial slurs, betting pools, and chain letters.

2. <u>*Cooperation Expected*</u> *– Users, when requested, are expected to cooperate with systems administrators in any investigation of system abuse. Users are encouraged to report suspected abuse, especially any damage to or problems with their files. Failure to cooperate may be grounds for cancellation of access privileges, or other disciplinary actions.*

3. <u>*Corrective Action*</u> *– If systems administrators have persuasive evidence of misuse of computing resources, and if that evidence points to the computing activities or the computer files of an individual, they shall pursue one or more of the following steps, as appropriate to protect other users, networks and the computer system:*

a. *Provide notification of the investigation to the Director of Public Safety through the Support Services Manager. Depending on the circumstances and if appropriate or warranted, the Director or his/her designee shall inform the University's Information Security Officer.*

b. *Temporarily suspend or restrict the user's computing privileges during the investigation.*

c. *With authorization from the University's Information Security Officer and/ or the Director of Public Safety, inspect the user's files, diskettes, tapes, and/or other computer- accessible storage media on University owned and operated equipment.*

d. *Refer the matter for possible disciplinary action to the Director of Public Safety.*

LAURA WILSON
DIRECTOR