Information Technology Policies and Guidelines

The following policies and guidelines are an abridged version of the Santa Clara University Administrative Policies and Procedures manual. Information Technology reserves the right to revise, delete or amend these policies and guidelines at any time.

SCOPE OF THE POLICY. IT will provide assistance for University supported applications and systems. Faculty, staff, and currently registered students are eligible to access the university computing resources and are eligible to receive IT support.

USE OF THE FACILITIES. Access to university computing resources is a privilege. Proper ID is required for entrance to the facilities. As a general guideline, no individual should make use of computer facilities in any manner, which infringes on the rights of others to make equal use of those same facilities. Users are expected to adhere to established policies and procedures such as those on usage, respect for intellectual property and copyrights, and observing canons of etiquette for applicable resources.

ACCOUNT POLICIES. The university academic computing systems are available for use except during those periods when scheduled or emergency academic computing servicing is required. Users will be notified by written or electronic means should such servicing be required. Accounts will be deleted yearly. Accounts are subject to deletion on a more frequent basis, should system resources necessitate it. Accounts will be allocated a set amount of disk space, which will be reviewed quarterly.

SECURITY AND PRIVACY. Unauthorized access to resources or data is not permitted. *The ability to access a resource or item of data dose not explicitly or implicitly imply authorization.* Account security is provided via a password mechanism. Providing one's account password to another user is considered to authorize the second individual access to all information in the account. The account owner accepts responsibility for the actions of any other person they authorize to use their account. Attempts to compromise the security of the network or its connected systems are prohibited. Any attempt at this, or the introduction of viruses. Worms, Trojan horses, or other forms of hacking or electronic subversion will result in the immediate loss of access. Further, University, civil, or criminal action may be taken as appropriate.

The computer systems and networks at SCU are a University resource and are provided as business and scholarship tools only. Users of the systems do so at their own risk. In particular, they assume the risk of malfunction, destruction, corruption, alteration, or mistransmission, of any information, software or hardware, whether due to negligence on the part of the University or its employees, forces beyond the University's control (such as fire, flood, or earthquake), or any other cause. Users agree to hold the University harmless for any damages whatsoever that may arise from the use of the systems.

In general, the practice is to treat information with as much privacy as possible. However, situations may arise where employees with legitimate business purposes may have the need to view information (including e-mail) on the systems. Any material on the systems or arriving within an account (such as e-mail) may be accessed for, and only for, administrative purposes by the University. Such access must be approved by an appropriate area Vice President or Dean/Dean's level director. Employees and students of the University are counseled to not place personal information on these accounts and to close any accounts on University systems upon leaving the University.

NETWORK AND ETIQUETTE. Many of the University systems are connected to an Ethernet local area network with access to international wide area networks. The continued access to these networks depends on the cooperation of all participants. Ethical behavior should be observed at all times and no individual should engage in behavior over the network that would be inappropriate for a face-to-face meeting. Violators will be subject to loss of access or more severe action, depending on the circumstances.

Unacceptable Use of the Campus Networks: Specific examples of unacceptable used of the network include, but are not limited to, the following:

1) Users on the network shall avoid interfering with the purposes and goals of the network, avoid disrupting the network host systems (nodes) and avoid disrupting network services.
2) Activities that are likely to result in the loss of recipients' work or data are prohibited.
3) Advertising and marketing from commercial organizations is not permitted. Similarly, institution-owned computing and network resources should not be used for unauthorized commercial purposes.
4) Any communication, which violates applicable laws and regulations, is not allowed.
5) "Chain letters", "broadcast" messages to lists or individuals, and other types of use that would cause congestion of the networks or otherwise interfere with the work of others, are not allowed.
6) Any communication that would in some way injure the recipient or be deemed as inappropriate either by written policy or general sprit of the University Community is not allowed.

SOFTWARE COPYRIGHT AND COMPLIANCE POLICY. The unauthorized copying of any software or information/data which is licensed or protected by copyright is theft and, thus, unethical. Failure to observe software copyrights and /or license agreements may result in disciplinary action by this institution and/or legal action by the copyright owner.

Printed Name: _____ Signature: _____ Date: _____