Santa Clara University
School of Engineering

Network Security Policy

Date of last revision: 3/31/2005

Purpose:

Measures adopted to prevent the unauthorized use, misuse, modification, or denial of use of knowledge, facts, data, or capabilities of the School of Engineering computer network, wired or wireless.

Scope:

This policy supplements existing University policies, http://www.scu.edu/humanresources/policy/306.cfm?menu=300, and the Information Technology department's policy, http://it.scu.edu/policies/NetPolicy.shtml, and is applicable to the School of Engineering. As such it is not exhaustive. The Engineering Design Center in concert with the Engineering Computing Service Committee reserve the right to revise, delete or amend these policies and guidelines at any time. Please refer to the aforementioned policy documents for any topic not specifically covered herein.

Definitions:

ENGINEERING COMPUTER – Any computer connected to the Engineering network intended primarily for university business use by faculty, staff, or students. Generally speaking, all non-portable computers connected to the Engineering network are considered "Engineering Computers."

NON-ENGINEERING COMPUTER – Any computer temporarily connected to the Engineering network and intended for either personal or university business use. Laptops are an example.

NETWORK SECURITY PERSONNEL – The Engineering Design Center Security Administrator or authorized representative (e.g. IT dept. personnel).

PRIMARY OPERATOR – The person(s) responsible for the system. In general, the Primary Operator for a system in an office, cubicle, or research area is the person who is assigned to that space.

SYSTEM-LEVEL ACCESS – Complete, non-restricted access to the system to diagnose problems, install patches, and investigate anomalies. On Unix-like systems this is generally the "root" account, while on Windows-based systems it is generally the "Administrator" account.

IP Address Assignment. The School of Engineering maintains a range of IP addresses for use by Engineering faculty, staff, and students. All Engineering Computers are to be assigned static IP addresses by the Design Center staff unless otherwise authorized by the Design Center staff. All Non-Engineering Computers are to be assigned DHCP addresses unless otherwise authorized by the Design Center staff. Systems in violation of this policy may have their network access terminated until they can be found and brought into compliance.

System-Level Access. The Primary Operator acknowledges full responsibility for the security of an Engineering Computer unless System-Level Access is granted to Security Personnel.
Either party may renegotiate the provision of System-level access at any time provided both the Primary Operator and the Network Security Personnel reach an agreement.
The System-Level Access policy does not apply to Non-Engineering Computers. The security of such systems is always the responsibility of their owners.

Incident Response. When any computer system on the Engineering network is found to be compromised, infected, behaving strangely or in violation of policy, Network Security Personnel must act to ensure that the incident is contained. Security Personnel will assume the following responsibilities: 1) At their discretion, removal of the system from the Engineering network, 2) forensic analysis of the system 3) authorize when the system can be returned to the Engineering network. Personnel responsible for the system's security at the time of the incident will clean, and/or rebuild and properly secure the system.

Inappropriate and/or Illegal Activity. Illegal activity, such as copying copyrighted material without permission, ``cracking", ``phishing", and other attempts to break or circumvent security mechanisms, and stealing data or identities through false-front web sites or similar means, is strictly forbidden by University as well as Design Center policy. Computers used in these activities will be removed from the network and their owners referred to the appropriate Dean for possible sanction. The Primary Operator of a computer is responsible for ensuring that the computer is used in accordance with University and Design Center policies.

Abuse of Resources. The Design Center network and workstations are shared resources. As such, the entire Design Center user community can be adversely affected if any one user attempts to use more than a reasonable amount of these shared resources. File copying via Peer-to-peer (P2P) programs, release of ``fork bombs", excess use of `find' across NFS mounts, and other activities that consume excessive amounts of disk space and/or network bandwidth may result in removal of the originating computer from the Design Center network or the disabling of the offender's Design Center account, or both. Serious or repeat offenses will be referred to the appropriate Dean for possible sanction.