Procedures for Removing Networked Devices* From the Cal Poly Network

March 1, 2005

The procedures below outline the steps taken when removing a device from the Cal Poly network when a formal complaint is received or the device is determined to be in violation of Cal Poly's Information Security Program, Information Technology Resources Responsible Use Policy (RUP) and/or other computing policies outlined at http://security.calpoly.edu/policies/rup/.

Under Policy Application, Item #3, the RUP states:

> *"The University reserves the right to limit access to its resources when policies or laws are violated and to use appropriate means to safeguard its resources, preserve network/system integrity, and ensure continued service delivery at all times. This includes monitoring routing information of communications across its network services and transaction records residing on University resources, scanning systems attached to the Cal Poly network for security problems, disconnecting systems that have become a security hazard, and restricting the material transported across the network or posted on University systems."*

Procedure to Remove a Networked Device* from the Cal Poly Network

1. If Cal Poly is notified of a complaint from an outside entity, a complaint from a Cal Poly user, and/or an electronic alert from network hardware and/or software, Cal Poly will investigate the incident. The primary point of contact for investigating complaints is the Policy Assurance Officer in Information Technology Services (hereafter referred to as "ITS").

2. ITS will create a Remedy ticket with all information known about the incident.

3. ITS will determine the source of the incident, including the hardware address and physical location of the device. All pertinent information will be recorded in Remedy.

4. ITS will attempt to contact the listed owner of the network device using the phone directory listing for that user and location. ITS will also attempt to contact via telephone the LAN Coordinator of the network device. Contact will include notification of the network device location and what can be done to stop the occurrence (if known). This information will also be sent in e-mail form. A note may also be left on the device asking the owner to contact ITS immediately, but e-mail will be the official means to communicate.

5. The maximum time to respond to violations is eight (8) hours, depending on the severity and risk potential to the network, i.e., if conditions warrant, the removal may be immediate. If there is no response from the parties involved, or they are unable to repair the occurrence, ITS will remove the offending network device from the Cal Poly network. Whenever possible, this will be done using software commands within the network

switch. Where that is impractical, ITS Network Administration or Technical Services will be contacted to manually remove the device from the network at the switch. All aforementioned parties will be notified of the network disconnect and the reasons for doing so. If the device is a personal computer belonging to an individual, the department will be notified as well. If the device is assigned to a student club, the faculty advisor will be notified and held responsible.

6. Once designated technical staff have determined that the network device is free of the root cause for the occurrence and further investigation or action consistent with the RUP or other campus policies is no longer required, ITS will enable network connectivity for this device.

7. In instances where the Cal Poly network is being placed at high risk by the offending network device or a serious security threat or emergency situation exists (e.g., denial of service attack, developing virus/worm outbreak, etc.), ITS will remove the offending device immediately from network connectivity and before alerting the responsible party (e.g., advisor, owner, LAN coordinator, etc.) of the removal. The notification will take place as soon as possible before, during, or after the removal in accordance with the "ITS Emergency Response Protocol" which is located at: http://www.irmppc.calpoly.edu/2003/NetworkDisconnect110403.pdf

8. If there is a recurrence of the same problem or a pattern of problems with the same network device is detected, ITS will take the additional step of asking the appropriate official (e.g., dean, department head, director, program manager) to commit in writing to ensuring that the device is properly secured in the future.

Contact Information

Information Technology Services, Office of the CIO
Policy and Program Assurance
Mary Shaffer, mshaffer@calpoly.edu
Office: (805) 756-5538
FAX: (805) 756-2000

DEFINITION (*):
A networked device includes but is not limited to the following types of equipment assigned to individuals, departments, clubs, auxiliary organizations or individuals from off-campus utilizing university network resources: personal computers, laptops, workstations, wireless devices (e.g. PDAs, laptops, handheld phones, base stations or pods), networked printers/copiers, servers, switches, routers, hubs, mini-hubs, splitters, wireless access points, firewalls, network security devices, network appliances, modem pools, or any device that is network-capable and connected to university network resources.