The problem

In the last year there have been significant increases in the volume and complexity of security related incidents involving campus workstation, laptops and servers. These incidents have negatively impacted campus productivity and required the costly intervention of ITS staff and local area network staff in the Colleges and Divisions to mitigate. Increasing regulatory and audit compliance pressures are also requiring more stringent security to be implemented at the campus workstation and server level.

Solution Strategy

Cal Poly needs to adopt a campus wide approach including ASI, Foundation, State and Auxiliaries to address these issues. Active involvement of ITS and campus LAN Coordinators is essential to establish campus wide policy, standards and guidelines. A phased implementation methodology should be adopted. The following documentation should inform and guide this process:

- Cal Poly’s Information Security Program
- Cal Poly’s Responsible Use Policy
- CSU audit recommendations
- State and Federal legislation mandates
- Industry Best Practices

Goals

1. Reduce on-campus disruptions that impact teaching and learning, the administrative processes of the university and the productivity of students, faculty and staff.

2. Protect confidential information.

3. Ensure campus compliance with state and federal legislation regarding the protection of sensitive personal information.

Short Term Objectives

1. Consolidate existing policies and procedures into a streamlined technology access plan.

2. Research, develop, and implement appropriate network access policies and procedures (software, patches, configuration, etc. required before connecting to Cal Poly network).

3. Ensure vendor security patches and fixes are applied expeditiously to ALL on-campus workstation, laptops and servers with priority being given to Microsoft operating systems.

4. Ensure ALL on-campus workstation, laptops and servers utilize up to date anti-virus software with priority being given to Microsoft operating systems.

5. Research, develop, and implement best practice security procedures (patching, account guidelines, password management, OS configurations, etc.) on ALL on-campus workstation, laptops and servers.

6. Develop and implement standard “security incident” reporting and tracking procedures throughout campus.

7. Establish campus-level security response team and conduct selected tests to validate its procedures.