

September 6, 2000

MEMORANDUM

To: Distribution List (see bottom of page 2)

From: Pat Burns, Director of ACNS

RE: Activities of Campus Information Technology Security Committee (CITSC)

This correspondence is to inform you of activities of the Campus Information Technology Security Committee (CITSC). This committee was formed this summer, at the direction of the Information Technology Executive Committee (ITEC), to codify some of the ad hoc issues dealing with our IT environment. The membership of the CITSC is provided as Attachment A. The charge to the committee is provided as Attachment B. A synopsis of the committee's activities is:

1. Appropriate and acceptable use of the University's Information Technology resources – Acceptable use defines the activities in which individuals are permitted by law to engage, while appropriate use defines the nature of the activities in which responsible users should be engaging. As an example, while it may not be prohibited by law to send a personal e-mail stating one's political position to one's US Congressional Representative, it may be an inappropriate use of the University's IT resources.
2. Protecting individuals' privacy in the electronic age – Electronic information is especially amenable to being read and widely shared. While Colorado law protects the individual well in the area of electronic communication, federal law does not. The committee will take a philosophical stance on protecting individuals' rights, and recommend policies that will serve to protect privacy.
3. Protecting the University's Information Technology resources – The University has experienced various, significant attacks via the network. Indeed, the recent spate of virus attacks has illustrated how disruptive to the University's work environment such attacks can be. This aspect of the committee's charge will seek to achieve an appropriate balance between protecting the University's IT resources and usability of our IT resources.

The Process

The committee has met three times. At the last meeting, the CITSC requested that this communication be prepared and broadly circulated to the campus to inform you of this activity, to inform you of the process that the committee envisions to address the three topics above, and by this memo to solicit your input into the process.

After policies and procedures are developed, the committee will circulate them broadly for comment, to groups on the Distribution list at the end of this memorandum in addition to being posted on a Web page for comments.

Your Input

The Committee has formed two subcommittees, one dealing with policy and the other dealing with technical aspects. The coordinators of these two committees are:

Pat Burns, Patrick.Burns@ColoState.EDU - Coordinator of the Policy Subcommittee

Scott Baily, Scott.Baily@ColoState.EDU - Coordinator of the Technical Subcommittee. Participation in this subcommittee of additional individuals, beyond the CITSC committee members, is occurring.

Please feel free to contact Scott or myself if you have input or questions.

Distribution List:

CSU Legal Office

Deans, Directors and Department Heads

Faculty Council

Subnet Managers Group

University Information Technology Support Services (UITSS) Committee

University Instructional Technology Committee (UITC)

ASCSU

Graduate Student Council

Attachment A

Campus Information Technology Security Committee (CITSC) Membership

- Donna Aurand - Office of the General Counsel (advisory role)
- Scott Baily – Associate Director for Networking, ACNS
- Pat Burns – Director of ACNS
- Jim Dolak – Associate Director of Housing
- Kevin Foskin – Director in Office of the Dean, Liberal Arts
- Laurie Hayes – Vice Provost
- Don Hesser – Director of Information Systems
- Donn Hopkins – Chief of University Police Department
- Ann Hudgens – Director of Judicial Affairs
- Tom Milligan – Public Relations
- Michael Schulman – ASCSU
- Rusty Scott – Natural Resources
- Wayne Trzyna – Computer Sciences
- Julie Wessling – Assistant Dean of Libraries

Attachment B

Charge to Campus Information Technology Security Committee (CITSC)

The Campus Security Committee (CSC) is constituted to address issues associated with appropriate use of information technology by students, faculty and staff (including administrators) at Colorado State University. The committee is charged with:

1. Devising policies for acceptable and appropriate use of information technology, achieving an appropriate balance among protection of individuals' rights, protection of the information technology resource, and the reputation of the University.
2. Recommending disciplinary actions to take against those who violate these policies.
3. Devising appropriate technical recommendations for implementation at the University.
4. Giving due consideration such that these policies and procedures may be carried so that they do not conflict with existing and emerging policies and procedures at the University, particularly any issues of charging back for network services.

It is envisioned that two subcommittees, one to address policy issues, and the other to address technical issues, may at the committee's option, be formed to address the issues above. The committee shall have all of its recommendations approved by CSU Legal Counsel, who shall act in an advisory capacity, in the course of the committee's activities. The Committee shall also seek input on its activities from the broadest practicable constituencies that it deems appropriate, possibly the Council of Deans, CAAG, ASCSU, GSA, Faculty Council, the University Information Technology Support Services committee (UITSS), the University Instructional Technology Committee (UITC), etc.

The committee shall forward to the Information and Instructional Technology Planning Group (IITPG) a progress report in November 2000, and a final report, if possible, in May of 2001. The IITPG shall review this report and forward the final report and its recommendations to the Information Technology Executive Committee (ITEC) in June 2001.

Finally, the Committee is charged with reviewing and modifying this charge as it deems appropriate as its first formal activity.

Areas of focus for the Committee

Policy Issues

- To elevate the awareness of potential security threats and the potential consequences the University faces as a result.
- Acceptable and Appropriate Use Policy
 - Acceptable use - what the law permits
 - Appropriate use - what we should be doing (perhaps more restrictive than what we legally can do), how to use information technology best to support and advance the mission of the University
 - See interim policy at <http://www.colostate.edu/services/acns/aup.html>
- Information Content
 - Web pages, e-mail, other interpersonal communications
- Distinction between university-owned equipment, and student-owned equipment (e.g. residence halls and apartments)
- Distinction between faculty and student use to foster and create new knowledge and use by staff for the work function
- Notification - are individuals to be notified before, during or after an investigation occurs?
- Best use of limited resources: network capacity, disk space, etc.
 - Handling of MP3 files (“Napster”) and other “recreational” traffic
- Establish “General Principles”
- Establish and publish recommended disciplinary actions for various types of offenses
 - Public relations concerns

Technical Issues

- Incident Response and Recovery
 - Single point of contact, with established and publicized step-by-step procedures
 - Develop appropriate actions when security violations are suspected
 - Course of action for following up on violations originating outside of CSU
- Review physical infrastructure
- General recommendations for securing central and departmental servers, desktop computers, and other network-attached devices
 - Security measures recommended for various platforms and environments
 - This may include such things as Kerberos authentication and authorization, Public Key Infrastructure (PKI), intrusion detection, secure (strongly encrypted) connections to central and departmental servers
 - Evaluate network-based solutions including firewalls and other network architectures that provide various degrees of protection for several classes of computers.
- To develop “best practices” guidelines for University IT staff to use as a baseline for their environment. This will include recommendations for password management, tightening security on servers and desktop machines, etc.

- Central and local staffing issues
 - Draw upon local expertise (departmental IT support personnel)
 - Appropriate activities for central and local support staff
 - To create a pool of local resources the University can draw upon when expertise in specific areas is required