Principles to Guide Efforts to Improve Computer and Network Security for Higher Education

Background

On August 27, 2002, an invitational workshop was held at Columbia University to articulate the core values of higher education, with the goal of ensuring that such a set of principles would guide colleges and universities as they decide how to improve the security of computers and networks. The workshop was sponsored by the National Science Foundation and organized by the EDUCAUSE/Internet2 Computer and Network Security Task Force.

Based on research into principles articulated by a variety of academic groups (for example, the American Association of University Professors and the American Library Association) and statements by invited experts, the group proposed that higher education's efforts to improve computer and network security be guided by six principles:

- civility and community
- academic and intellectual freedom
- privacy and confidentiality
- equity, diversity, and access
- fairness and process
- ethics, integrity, and responsibility

We recognize that these principles are broad; each institution must ultimately determine the principles that are most relevant and valued by its own community. These principles are offered as a basis for discussions. Each must be interpreted appropriately within the contexts of the various activities of the academic community.

It is our belief that computer and network security are an essential requirement for the support and protection of the core values of higher education. Simultaneously, it is important that we not imprudently implement security policies or procedures that undercut higher education's fundamental principles.

We invite the community to provide suggestions and changes to this document. Our intention is to consolidate input and develop a set of revised principles that will be available to higher education. The resulting set of principles is not intended to bind institutions, but to serve as a starting point for campus discussions about computer and network security.

Civility and Community

Civility and community are among higher education's core values. Respect for human dignity, regard for the rights of individuals and the furtherance of rational discourse must be at the foundation of policies and procedures related to computer and network security.

Rationale:

- Key values of the higher education community include respect for human dignity, respect for rights and property of individuals, and the right of freedom of expression
- Communities are defined by a set of common values, common experiences, shared knowledge, and an ethical framework as well as a responsibility and commitment to the common good
- Higher education represents and resides within multiple, interrelated communities
- Among the objectives of higher education is a commitment to open discourse

Implications:

- We recognize the tension that may exist between standards of civility and the right to freedom of expression and the exercise of other individual rights
- The difference between ideas and the expression of ideas should be recognized and respected
- Policy should identify standards of behavior as well as standard security practices and principles; tangible actions should be proposed
- The upholding of community standards is best achieved through voluntary compliance, although more formal systems of accountability may be necessary

Academic and Intellectual Freedom

Academic freedom is the keystone of American higher education. It ensures freedom of inquiry, debate, and communication, which are essential for learning and the pursuit of knowledge. Intellectual freedom ensures information access and use, which are essential to a free, democratic society.

Rationale:

- The common good depends on the search for truth and its free exposition
- Faculty are entitled to freedom in:
  - — Classroom discussions
  - — Research and publication of results
  - — Artistic expression
- Individuals are entitled to:
  - — Seek, receive, and impart information
  - — Express themselves freely
  - — Access material regardless of origin, background, or views of those contributing to their creation

Implications:

- All higher education personnel (for example, faculty and technical personnel) must be trained and directed to respect academic and intellectual freedom
- Networks and systems must be secure in order to prevent unauthorized modification of online publications and expression but open enough to enable unfettered online publication and expression
- Authentication and authorization systems needed to ensure compliance with license agreements for online information should protect the privacy of those using the information
- User authentication/authorization logs should be kept separate from system usage logs, with no linking of the two datasets

Privacy and Confidentiality

To the extent possible in the electronic environment, users' privacy will be preserved. Privacy must be protected in information systems whether the personally identifiable information is provided or derived. Fair information practices should govern the collection and disclosure of personal information.

Rationale:

- Higher education's belief in self-determination and the ability to make independent decisions depends upon privacy
- Privacy must be protected to comply with federal and state laws and regulations
- Privacy serves as a safeguard for academic and intellectual freedom
- Confidentiality limits access to information to only those with a need to know

Implications:

- Systems should provide the means to implement fair information practices, and users should be informed of system logging policies and practices, including how log data are secured, de-identified or aggregated, and disposed of and who has access to the log data as long as such information does not jeopardize system security
- System design must respond to the privacy choices specified in advance by the individual
- Systems must be designed to enable only authorized access while keeping the identity of authorized users confidential as required in the context
- IT professionals must be held to the ethical standards established by the academic community

Equity, Diversity and Access

Approaches to security and privacy should respect the equity and diversity goals of higher education. Access to appropriate information and the Internet should be provided equitably to all members of the community.

Rationale:

- Equity and diversity are fundamental values in higher education and American society
- Technology can enable new sectors of the community to participate in higher education
- Not everyone interacts with computer or network-based systems with a common set of technical or personal resources
- Attention to issues of diversity and equity of access create stronger, more secure systems

Implications:

- Additional system demands imposed for the purposes of computer and network security should not unreasonably inhibit users whose purposes are legitimate but whose technology resources are limited
- Systems should accommodate a variety of authentication/authorization protocols so that individuals are not inequitably denied access
- Personal disabilities should be accommodated through secure systems
- Accommodations for various groups of users should be kept confidential

Fairness and Process

Access to computer systems, network and scholarly resources is a fundamental benefit of joining an academic community. Revoking or limiting that access must only be done as a result of a serious offense after which a defined process is followed.

Rationale:

- Account and network access is an essential tool for individual success within the academy. It is also essential for the delivery of quality services to students, faculty and staff. Such access should be provided widely to every member of the enterprise (for example, students, faculty, and staff)
- Colleges and universities need to develop and communicate explicit policies governing the fair and responsible utilization of computer and network resources by the academic community
- Such policies should protect higher education's core principles (for example, academic and intellectual freedom) from undue constraint by external forces
- All policies should be accompanied by a description of fair process to be followed when any member of the community violates the established policies

Implications:

- Campuses must define “due process” for each member of the community
- Campuses must be prepared to support core higher education values (for example, academic and intellectual freedom, privacy, and civility) and not overreact to individual reports of abuse
- Campuses should look to the appropriate policy and office for guidance in handling incidents (for example, copyright policy, campus posting, and non-commercial use)
- Security policies, guidelines, and practices should be discussed and reviewed within each institution’s shared governance system

Ethics, Integrity, and Responsibility

Computer and network security is dependent on and should be designed to further the highest standards of ethics and integrity in campus communities. Good security practices are important to the entire community and are the shared responsibility of each member.

Rationale:

- Ethics and integrity associated with computer and network security is a shared responsibility among all campus constituents
- Colleges and universities are communities of trust, requiring appropriate respect for confidentiality and privacy
- Computer and network security provides a tangible opportunity for teaching and modeling acceptable behavior
- Ethics and integrity reinforce fair and equitable access to electronic resources

Implications:

- Inappropriate individual access or use of information infringes on both the rights and responsibilities of the entire community
- Disruption of services restricts the transmission of knowledge and exploration of knowledge
- One form of response to a break in security should be education
- Security based on people’s integrity and ethics is stronger than security based on technology alone

For More Information

The EDUCAUSE/Internet2 Computer and Network Security Task Force is working to improve the security of college and university computing environments and to increase awareness of IT security issues across higher education. A web site on *Security: A Resource on Computer and Network Security for the Higher Education Community* is available at http://www.educause.edu/security. Contact the Security Task Force by e-mailing Security-Task-Force@educause.edu or calling 202.872.4200.