

Policy Governing Computer Security and Resource Allocation

(In the text that follows, the policy is set in straight type; additional explanatory material is set in italics and is not to be considered part of the policy itself.)

1. Rationale

In support of its mission to provide excellent education, modern research, and meaningful service, the University of Kentucky provides extensive computing resources to its students, faculty, staff, and users throughout Kentucky who rely on University resources such as the library, College of Agriculture services, and distance learning. These resources, which are defined for the purposes of this policy to include network capacity as well as computing systems, contribute to the work and lives of all members of the University and, therefore, must be administered with great care.

Careful and ethical use of computing resources is the responsibility of every *individual* user and is governed by the *Policy Governing Access to and Use of University of Kentucky Computing Resources* and the *Policy Governing Creation and Use of World-Wide Web Materials*. Unfortunately, as the volume of computing has grown significantly and the nature of network traffic has evolved, careful and ethical computing behavior by *individual users* is not always sufficient to protect University computing resources from security threats nor to guarantee equitable allocation of computing resources, especially network capacity. Therefore, University information technology professionals, both those in University-wide units and those in individual units, in their roles of conserving, protecting, and administering the computing resources for the University, are often required to select and implement technology designed to provide protection and to control resource allocation. In this policy, resource allocation refers to providing a fair share of the resources to the greatest number of users by managing access to certain computing resources or certain modes of computing.

Monitoring and management technology designed for security and resource allocation purposes may also have the unintended effect of limiting or otherwise restricting legitimate computing applications by members of the University community. As a result, a conflict may arise between the University's goal of supporting such computing and its responsibilities to ensure security and to equitably distribute the use of the resources.

Whenever a conflict exists between competing objectives, a carefully crafted policy is needed 1) to provide advice to those charged with making decisions for the University related to implementing the goals, 2) to serve as a basis for appeals of such decisions, and 3) to help educate users of University computing and network resources. A computing policy must balance the rights of use by individual members of the University community and the responsibility of the University to deter abuse. This policy is intended to serve the function of specifying procedures to be followed in cases when decisions are appealed, and to inform members of the user community of rationale for the security policy and their rights. This policy applies to all units of the University; small, self-contained units, such as an individual user, department, or research laboratory, may act independently, as long as the actions do not have an impact outside of the unit or violate the basic principles and appeals procedures specified in the policy. Actions by a small, self-contained unit that may have broader security or resource allocation impacts, such as the addition of networking components (switches, routers, hubs, minihubs, etc.), must follow the procedures specified in section 2.2, below.

2. Procedures

Each event that compromises the security of the University's computing resources is unique in some ways. Likewise, each inequity in computing resources has its own specific cause. However, patterns usually can be discerned and may lead to general, rather than individual remedies. Whenever possible, the University will conduct sufficient research to reveal patterns and apply general rather than narrow mechanisms for correction.

The governing principles for all decisions regarding corrective actions are:

- A. Take the necessary security measures or control the allocation of resources with the least possible infringement on the legitimate computing activities of individual users.**

- B. Protect the two basic rights regarding computing – “privacy” and “a fair share of the resources” – extended to every individual.**

(“Legitimate computing activities” and the “two basic rights” are to be understood here as they are defined in the *Policy Governing Access to and Use of University of Kentucky Computing Resources*.)

The Chief Information Officer of the University may be required to take immediate action in response to urgent security problems; both of these governing principles can be suspended temporarily, to ensure security. In the event of emergency or exigent situations, the Chief Information Officer of the University can authorize the University's information technology professionals to take action as necessary to protect the integrity of the University's operations.

2.1 Computer Security and Resource Allocation Advisory Committee

In accordance with accepted industry practice, the President will establish a Computer Security and Resource Allocation Advisory Committee. The Committee will consist of representatives of instructional, research, clinical, and administrative computer users from across the entire University, including faculty, students, and staff, and will be chaired by a faculty member. The chief computing administrators of the University will serve as ex-officio members of the Committee.

The Computer Security and Resource Allocation Advisory Committee will have the following principal responsibilities:

- 2.1.1 Provide information and education regarding security and resource allocation matters to the University computing community
- 2.1.2 Review significant changes in technology to be employed by the University for achieving security or resource allocation objectives, following the mechanisms described in Section 2.2, below.
- 2.1.3 Adjudicate appeals from individual users or groups of users seeking to redress an alleged infringement of their legitimate computing activities caused by a change in computing resources or procedures implemented for security or resource allocation purposes.
- 2.1.4 Periodically review the results of security and resource allocation studies and audits of University computing resources.
- 2.1.5 Periodically assess the allocation of the University's computing resources (using University staff and data and industry best practices recommendations) and suggest actions in consultation and collaboration with the University's information technology professionals.

2.2 Mechanisms

To provide the best possible computing resources to the University community while fulfilling its legal and practical responsibilities for security and equitable resource allocation, the University will employ several practical mechanisms.

- Educational: The University will educate its users. Through appropriate media – including but not limited to University Web sites, traditional publications, electronic communications, and public forums – information technology professionals will inform users of new and continuing problems and will develop corrective actions and preventive measures expected of individual users in order to comply with their obligation to use University computer resources responsibly.
- Legal: In those instances where the University is required by law to implement certain security measures, the University's information technology professionals will seek solutions that will have the least impact on the legitimate computing activities of individual users, while at the same time providing maximum security protection or optimal resource allocation. For example, the University is obligated by law to implement specific levels or types of security for certain classes of data, and the University may be required to assist a copyright holder in the enforcement of certain legal rights. Furthermore, there may be some types of network activities that, while perfectly legitimate *individually*, in the aggregate present increased security risks, or that tend to create an inequitable distribution of available resources.

- Technical: When the University's information technology professionals have identified a particular technology solution¹ that is required to alleviate a security problem or to control the allocation of resources, they will employ the following steps to minimize the impact on the computing users who might be affected:
 - The information technology professionals will determine whether the problem is so urgent that it requires immediate action, in which case they will implement a temporary solution before continuing with the following steps.
 - The Computer Security and Resource Allocation Advisory Committee and potentially-affected users will be informed by the information technology professionals of the problem and the proposed solution.
 - The Chief Information Officer of the University will allow a reasonable time for user comments and alternative suggestions.
 - If a sufficient number of users may be affected, the Chief Information Officer of the University will hold a public hearing to permit discussion of the problem and the proposed solution, together with any alternative suggestions.
 - The University's information technology professionals will adopt an appropriate solution to the problem and will implement it, endeavoring to cause the least possible impact on the computing community.
 - Small, self-contained units of the University do not have to consult with the Computer Security and Resource Allocation Advisory Committee when implementing internal security or resource allocation measures that do not have an impact beyond the unit, as long as the governing principles and spirit of this policy are not violated. Individuals within the unit may appeal such measures as provided below.

¹ Examples of technological solutions that might be considered under this heading include: installation of specialized security hardware; blocking inbound access to certain ports; filtering or removal of e-mail attachments; blocking of classes of network traffic; removal of "malware;" scanning of disks; and tracing of network traffic.

2.3 Appeals

Any member of the University who feels that legitimate computing activities have been unacceptably infringed upon by an action taken by the University for computer security or resource allocation purposes has the right to appeal. All appeals must be made in writing within 60 days of the discovery of the alleged impact. Appeals of actions taken by a small, self-contained unit must be made to that unit first. All other appeals and appeals of a self-contained unit's decision are to be taken to the Computer Security and Resource Allocation Advisory Committee.

The committee will first determine 1) whether an infringement to legitimate computing activities has occurred and 2) whether this infringement is the direct result of an action taken by the University for security or resource allocation purposes. If the determination is affirmative on both points, the Committee will consult with the affected user(s) and with the appropriate information technology professionals to determine possible solutions to the problem. With all deliberate speed, especially in urgent cases such as those relating to clinical or research activities, the Committee will weigh the facts of the case in order to balance security or resource allocation concerns against the infringement on legitimate computing activities, take into account relevant technical and fiscal constraints, and then make its recommendation. The Committee's recommendation will not be final. The University's Chief Information Officer will review the committee's recommendation and provide a written explanation on whether the recommendation is accepted.

3. Principles Governing Decisions Regarding Computing Security and Resource Allocation

The following principles serve as the basis for consideration of all decisions regarding computing security and resource allocation:

3.1 The University is committed to providing the most productive computing environment possible for all of its faculty, students, and staff, consistent with the mission and resources of the University.

This principle is a reiteration of the policy that has guided the University's information systems group's activities since its inception. In the spirit of this principle, the University has acquired, maintained, and regularly upgraded one of the most powerful supercomputers available at any university; the network systems group has installed, maintained, and regularly upgraded one of the most sophisticated communications networks on any university campus; colleges, departments, and other units across the University have striven to provide the most advanced computing possible for their faculty and staffs; and, the University has pioneered and continues to generously provide advanced student computing facilities.

3.2 The University is committed to fulfilling its legal obligations to provide a secure computing environment for all data that it generates and for which it is responsible.

Various federal, state, and local laws place obligations on the University to acquire, generate, and secure a wide a range of data, including, but not limited to, student data, patient data, research data, and personnel data. Each of these categories of data is governed by laws limiting how it is to be stored, who may and may not have access to it and under what circumstances, and how it is to be preserved and protected. These complex legal restrictions may require the University to implement certain procedures that have an impact beyond just the specific data cited in the applicable laws. For example, the University may need to encrypt all packets on a particular network. The University must meet these legal obligations, but will endeavor to do so without undue impact on other computing.

3.3 The University is committed to protecting the integrity of all of its computing resources and data and those of all of its computer users.

The current computing environment is characterized by many threats to the security and integrity of computing resources, most of which originate outside of the University. For example, there are viruses, Trojan horses, denial-of-service attacks, and other similar security problems. Often, naive or innocent users at the University spread the malware that perpetrates these attacks on security. Dissemination can be minimized by hardware and software filters both at the individual and at the University level. The Policy Governing Access to and Use of University of Kentucky Computing Resources places an obligation on individual users to protect their accounts and computers from unauthorized usage; likewise, the University has an obligation to protect the common resources, such as the networks, servers, and mainframe computers, from unauthorized access or usage. The first approach to be taken by the University normally will be educating users. However, when education of users does not suffice, one technique for achieving this protection may entail restricting certain forms of network traffic and types of computing. Unfortunately, such techniques may affect more than just the offending traffic, limiting certain legitimate computing activities. In such cases, the University will have to balance its commitment to this principle against its commitment to the first principle stated above of providing the most productive computing environment possible.

3.4 The University is committed to allocating its available computing resources equitably among all users, giving priority to those instructional, research, and service applications that further the mission of the University.

The computing resources of the University must serve a wide variety of needs and applications. Among these applications are research computations, professional communication by faculty, instructional applications, administrative computing, patient record keeping, and personal and recreational applications. All these applications and many others may fall within the mission of the University. However, the University's computing

resources are finite, and the requirements of some applications may strain the resources, thereby limiting access for other applications. For example, certain classes of file transfer may usurp an inordinate portion of the available network bandwidth, leaving inadequate amounts for other applications. In this event, the University must make and implement resource-allocation decisions. It will always make such decisions in consonance with the mission of the University, giving priority to instructional, research, and service applications.