Global Information Assurance Certification Paper

Acceptable Use Policy Conflicts: Liberty vs. Security

Academic Acceptable Use Policy and the common conflicts between Security concerns, and the need to safeguard Privacy and Academic Freedom

GIAC Security Essentials Certification (GSEC)
PracticalAssignment Version 1.4c Option 1
John A. Resotko
October 11th, 2004

Table Of Contents

Abstract

This paper is intended to highlight conflicts found in many academic Acceptable Use Policy (AUP) documents between Liberty and Security concerns. The first section defines common conflicts by dividing Liberty and Security concerns into four broad categories. The document continues with examples of conflicts based on investigations of various AUP documents at educational institutions around the country. Using the examples found in these documents, this document will describe strong policy choices that can reduce or alleviate the conflicts between the competing interests of Liberty and Security.

Definition of the Conflict: Network Needs in an Academic Environment

It is a truism for most people that Liberty and Security are competing, opposed interests in most contexts. The widespread use of computer networks and information technology now extends to all parts of people's lives, and with that extension comes additional knowledge of this conflict. With this growth, there come corresponding changes to the nature of this conflict. Most working in information technology would grudgingly admit that some level of security is now required in order to have a reasonable ability to guarantee privacy and freedom of expression for users of computer networks. Without some method to differentiate legitimate, authorized users from possibly malicious abusers of computer technology, no one can be entirely sure about what level of privacy they enjoy when using computer technology. In the business world, these conflicts are often resolved in the Acceptable Use Policy. For most businesses, the AUP represents an attempt to balance legitimate needs against the company interests. "The goal is to provide a policy that protects the company while respecting the privacy and free speech rights of its employees. It can be a tough balancing act, but when in doubt, protect the company." [1] Most draw their policy over what uses will be prohibited, and how to protect the company from legal liability if employees misuse computing and network resources.

In academic environments,the requirements of those using computing resources can be quite broad compared to the business world. The needs of an educational institution include a far greater desire to encourage discourse, the free exchange of ideas, and research. The Acceptable Use Policy is where attempts are made to resolve the conflicts between educational needs, and the need to protect computing resources so that they continue to be available to all within the academic environment. Liberty and Security concerns conflict where the goals of each fall into broad categories of competing interests. These categories make up the next section of this document. Each represents a need common to all users of technology resources which often come into conflict.

Liberty and Security Concerns

Academic Freedom; the unimpeded exchange of information, ideas, and data is

a cornerstone of Liberty . Educational institutions support principles of openness in learning and research, and encourage students to engage in meaningful discourse. The free exchange of ideas encourages debate, expands thought, and ultimately enhances the education of all involved. "A key principle of academic freedom is that freedom of expression and freedom to read are central to the academic mission." [2] Some schools may even provide guidelines which support open expression while attempting to insure that such expression does not infringe on the rights of others.

Privacy; in information technology, this is most often defined by a recognizable division between the communications and information available in public places vs. private places. The Liberty inherent in freedom of speech and freedom of assembly can at times depend upon the ability of people to gather and discuss issues in public or in private if they so choose. Guaranteeing the right to privacy is important, regardless of whether the meeting place is a private home, or a virtual private chat area. All people want reasonable guarantees of confidentiality when they engage in private communications with others. Where computer and network technology is concerned, it is not always clear to the non-technical user where the dividing line is between public and private, or what their own responsibilities are to help insure their own privacy when communicating with others via technological means. “The safest assumption is that there's no absolute right or expectation of privacy online.” [3, pg. 40] However, most computer users want to know that if they intend a communication to be private, and they use an appropriate system to communicate privately, then privacy of the communications will be safeguarded.

Security; reasonable measures to protect the integrity of systems. Security can mean many things depending on the use of a particular system, how it is connected to a network, how people use that system to communicate with each other, and with others outside that system or network. Security for information systems, computers, and networks usually includes, but is not limited to, the following issues:

protection from unwanted intrusion (such as hacking)
protecting the hardware, software, and data of systems from damage
protection from unauthorized use, or intentional misuse
protection of authorized users privacy, data integrity, and availability

Methodology used to provide security guarantees frequently raise privacy concerns. Attempts to guarantee security by identifying unauthorized users or hostile attacks may require the administration to examine log files, monitor connections to and from a system or network, and engage in acts considered intrusive to the privacy of authorized users. The challenge in information technology is to provide security measures which include appropriate guarantees of privacy,and place limits on the use of information gathered for security purposes to protect the legitimate users of that technology.

Network Integrity; the ability to maintain the overall integrity and reliability of the network and the systems which make up the networks. As electronic means of exchanging ideas are widely adopted (email, instant messaging, public forums, blogs), the free exchange of ideas becomes dependent on the integrity of the systems supporting that exchange. In an attempt provide shared access to the finite, limited resources of these systems, administrators often will impose restrictions on the use of these systems. Further, as with security concerns, it may be necessary to conduct periodic monitoring of activity directed at these systems in order to determine if they are being attacked, or if unauthorized intruders have compromised the data or the privacy of legitimate, authorized users. Some of the methods used to maintain systems and networks in their "healthy" state may also be intrusive to the data and information of legitimate users. If a system is disrupted so often that it is unavailable most of the time, it cannot enhance or enable the free exchange of ideas. On the other hand, if a system is under such scrutiny in order to remain operational that no users of that system believe they have any privacy, it also cannot enable or enhance the free exchange of ideas. As a result, these measures are often considered to have a chilling effect on the openness of academic freedom, even when the intent is to insure that the integrity of these systems is maintained to facilitate the free exchange of ideas.

The main challenge in drafting policy which addresses these areas of concern is finding ways to harmonize the competing interests within them. The challenge can be summarized by a simple question: "How to we protect privacy and security while fostering accountability and responsibility?" [3, pg. 8] In an attempt to answer this question, an examination of current Acceptable Use Policy statements is required. A survey of AUP statements at various institutions across the United States, and across the globe, could fill several volumes. This paper will focus on AUP statements which highlight specific conflicts between the concerns of liberty and security.

Survey of Academic AUP Statements

HIRAM COLLEGE

As a more extreme example of a restrictive AUP, one need look no further than Hiram College in Ohio. Hiram College is a small private liberal arts college in north eastern Ohio. The college AUP document states it was last revised in June of 2002, so you would expect it to be a comprehensive and progressive document with regard to 21st century computing needs. The emphasis of the Hiramnet AUP is on providing technology to further the college mission by restricting any and all other behavior on their campus network. Access to the campus networks and computing resources are strictly controlled. "No anonymous users or devices are allowed." [4] Students must apply for their student identifiers, and identifiers for any PC or laptop they plan to connect to the network every semester. "All student identifiers and access terminate at the end

of the spring semester, and all student accounts, files, and programs are deleted. Students need to re-apply for an identifier for access after the end of every summer for the subsequent year." [4] A great deal of the policy language focuses on providing control and security to the administration. What students are allowed to do while connected to the network is also strictly controlled. Providing any kind of services from a student PC is strictly prohibited unless prior academic approval for said service is sought and obtained in advance. [4] This means that a student on a Windows computer cannot share a file folder or printer without obtaining prior authorization first, since that legitimate and legal sharing of files constitutes offering a network service to other students. Any violations of policy or additions of unauthorized hardware to the network, either detected or suspected, may result in the student account identifier being cut off without notice, their computers and network hardware confiscated without notice, and the files on their computers moved, examined, modified, or deleted without notice. [4]

There is no explicit statement of support for academic freedom of expression contained anywhere within the Acceptable Use Policy. Under the Data section of the AUP, the Security statement reads as follows: "Hiram College does not represent that the data on the College network is secure or will be kept private or confidential. The College recommends that users avoid sending confidential or private information across the network and even avoid storing it on computer systems connected to the network." [4] The Data section of the document offers this further statement on data Privacy: "As far as College owned systems connected to the network are concerned, because of ordinary and necessary procedures, the privacy of personal information in these systems cannot be guaranteed." [4] Since a primary tenet of freedom of expression is the ability to discuss topics of a sensitive, controversial, or objectionable nature with a limited audience of your choosing with some level of confidentiality, these two statements could have a rather chilling effect on free speech and the free exchange of ideas in this academic environment. The policy ends by instructing students to report to the Dray Computer Center in person, with proper student id, if they discover they are suddenly unable to access their domain account or other College account. [4] While the document clearly states that access to computing facilities is governed by the policies of the College, it does not outline how students can respond to a documented or alleged violation of the AUP, or what, if any, review or appeal process exists to examine such violations.

While the level of control and management provided within such a strict AUP may serve a smaller college or institution well, it is often unfeasible for institutions operating larger and more diverse networks with large student bodies. This AUP appears to be more concerned with protecting the business of the college first and foremost, with only minimal stated support for academic freedom and privacy.

MICHIGAN STATE UNIVERSITY

The Michigan State University AUP was approved as an administrative ruling in 1992, and is now undergoing major revisions within the MSU Committee structure. Since this document is being written during the AUP review process, I will focus on the state of the AUP in 1992, and the major conflicts which lead to the rewrite. (A copy of the 1992 MSU AUP is included as Appendix A, in case this version is replaced before this paper is published.) The original AUP from 1992 places a strong emphasis on freedom, openness, and diversity in making available computing and network resources to the MSU community. The concern for protecting the privacy of users as a guiding principle has the effect of also placing restrictions on what information system administrators are allowed to look at when investigating problems.

The AUP attempts to divide authority for administrative tasks by defining three classes of entities on the network:

> A "System Sponsor" which is the unit or faculty member responsible for funding a technology system or resource.
>
> A "System Manager" who is the designated authority to "monitor, manage, or otherwise grant temporary access to computing facilities"
>
> A "User" is "any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software, or both." [5]

Under this rather loose definition of what constitutes a user, even a system hacker or someone using a cracked login id and password is technically a user to which privacy guarantees must be extended. While this may have been an acceptable definition of a network user in the early nineties, other provisions of this AUP make this definition problematic, especially those which extend guarantees of privacy to all users in the network computing environment.

In the Enforcement and Adjudication section of the document, "the principal responsibility for investigation of suspected non-compliance with the provision of this ruling rests with the System Sponsors". [5] However, a later paragraph in this section expressly forbids most initial forms of investigation by stating that "The content of User files is not to be surreptitiously or otherwise examined, nor is the User-generated message content of a User network transaction to be monitored, without the prior written permission of either the User involved or the Vice Provost for Computing and Technology." Again, when the document was written, the number of network attacks taking place were relatively small, and formal intrusion incidents were few and far between. With worm programs now routinely infecting PCs on networks, hundreds of email messages containing spam and viruses arriving by email every day, and easily downloadable hacker and cracker tools available to the general public, there are many incidents each

day which this policy explicitly prevents system administrators from investigating and resolving without written permission. Further, under the strictest interpretation of this policy, a hacker who compromises a system and installs a root kit or other files is entitled to the same privacy protections as a legitimate user until the System Sponsor seeks out the Vice Provost for written permission to examine and clean up the security breach on that system. Most users can accept the need to routinely scan incoming email for messages containing viruses or malware, and most can understand the need to scan networks to look for PCs behaving in a manner consistent with a machine infected with malicious viruses or worms. Again, strict interpretation of this policy would prohibit these security measures, now considered commonplace, without the explicit written consent of every user of the network or email system, or the written permission of the Vice Provost for Computing and Technology. The enforcement section makes one concession to maintaining the integrity of the networks; it clearly allows for the "cessation of service, whether by network disconnection or disablement of log-in capability, shall be utilized in preference to file inspection when remedying or investigating instances of alleged disruption." [5] Short of cutting off log-in access or network connectivity, all other actions regarding alleged or confirmed incidents are to be referred to the Vice Provost for Computing and Technology. "They must also do so if systems or networks in multiple campus units have been disrupted or compromised, or if any non-MSU system, network, or party is involved." [5] Since any kind of self-propagating worm or virus infection will broadcast on a network and potentially affect multiple campus units, this requires system administrators to again seek out approval of the Vice Provost before addressing what is nowadays a common network issue. Further, "disciplinary issues concerning students, faculty, or staff should be discussed with the Vice Provost for Computing and Technology before action is taken, in the interests of consistency of treatment." [5]

Since this document was constructed, the MSU campus network environment has grown, connecting multiple colleges, academic units, research facilities, and administrative units. Each of these has their own unique systems, with diverse and sometimes conflicting needs for access and security. As network attacks have grown with the diversity of network systems, it is clear that some authority to investigate and resolve incidents related to security must be delegated. A policy of "cut off access now, investigate later after you have permission" is not sufficiently responsive to deal appropriately with the speed of some network attacks, such as the Blaster and Welchia worm infections of 2003. Clearly, the Vice Provost will be in the position of spending large portions of his time weighing and approving requests by system administrators who may need to examine files or network traffic in the course of trying to protect the privacy and data security of legitimate users from the threats of the twenty-first century.

While this issue in the AUP is clearly in need of revision for the current network environment, other portions of the MSU AUP do an appropriate job of addressing our primary concerns. Users are clearly informed that "the burden of

responsibility is on the User to inquire concerning the permissibility of an action or use" [5] on any systems they use on the network. The section entitled Good Citizenship in Cyberspace instructs the users what their responsibilities are when using network and computing resources. These include: not intentionally trying to obtain data, user ids and passwords of other users; not falsely representing themselves as other users; not attempting to break into, damage, alter, or disrupt the use of other systems or facilities, on campus or off; respecting the copyright and appropriate licensing of software used; and respecting the integrity of computing systems and networks "both on the MSU campus and at all sites reachable by MSU's external network connections." [5]

All these guidelines encourage academic freedom of expression and provide a reasonable responsibility to the users to behave in a manner that protects privacy and assists maintaining the network integrity. These guidelines unfortunately provide little assistance to the network and system administrators who are clearly charged with protecting systems from those who choose not to act as good citizens. While those constraints may be necessary in the interests of fairness and consistency of treatment, they can also handicap those whose job it is to engage in reasonable activities to guarantee privacy and security for all.

CENTRAL MICHIGAN UNIVERSITY

The Office of Information Technology (OIT) at Central Michigan University published their current AUP document in the Fall of 1997, with additional updates applied in the Fall of 1998. The policy statements as a whole attempt to strike a balance between liberty and security, as well as define areas where data is public or private. Some significant effort is made to clearly define the boundaries which can be crossed by authorized agents of the school when resolving problems or investigating incidents involving campus computing and network resources. The document begins by outlining the scope of the policy, and the responsibilities of the user community, in the Introduction. [6] The introduction clearly states that services may be suspended if OIT "becomes aware of possible inappropriate action, or detects illegal usage or practices designed to operate to the detriment of the user community, it will take immediate corrective action. Such actions may include suspension of services to the user(s) determined to be at fault." [6] While the section goes on to indicate that suspended services may be restored, no reference to a University adjudication process or procedure is mentioned other than that services can be restored "only when it is again safe and appropriate, or in some cases, only upon successful appeal to the Assistant Vice President of Information Technology or it's designee." [6] Specific details about what may constitute a violation of the policy are presented in later sections.

The AUP offers more specific information in the second section, Ownership, Privacy, and Freedom of Expression, on matters of privacy and academic freedom. For the most part, the OIT considers anything stored on storage media owned by the University as property of the University "unless the contents are

licensed software, licensed databases (e.g., InfoShare), intellectual property owned by others, or protected by CMU's Intellectual Property Rights Policy." [6] The files and data stored on University systems at CMU have no general expectation of privacy, as "The university has the right of access to the contents at any time for any legitimate purpose including moving or deleting files to preserve system security and performance, or examining files when there is a legitimate "need to know" ". [6] Privacy resides entirely with the decision on where to store files. This means that, unlike Hiram College, the files that a student keeps on their personal desktop or laptop computer remain their private property, even if that student connects to the CMU networks. The explicit privacy statement in the policy is;

> Privacy: Users have the right to expect that their computer uses are confidential from other users, and CMU users who invade the privacy of others may have their access suspended and may also be subject to university disciplinary action through appropriate channels. CMU will make reasonable efforts to maintain the confidentiality of the storage contents and to safeguard those contents from loss, but cannot be held liable for the inadvertent or unavoidable loss or disclosure of the contents, or for disclosure resulting from the unlawful acts of others. CMU has the right of access to the content only in those cases where it has a legitimate "need to know". [6]

Immediately following this statement is a long list of situations where CMU deems it appropriate to access and review computer records, including all the items you'd expect such as email harassment, network disruptions, academic dishonesty, violations of policy or law, violating another user's rights, FOIA requests, subpoena or discovery requests. [6] Also included in the laundry list is "an employee is devoting excessive amounts of work time to personal email or other personal computer work," [6] This seems somewhat anomalous, since the list explicitly includes violation of policy, which would presumably include employee workplace policy. If CMU already has a workplace policy prohibiting excessive use of computing resources and email for personal use during work hours, referencing violations of workplace policy or work rules as cause to examine computer records should be sufficient. The section ends by stating that information accessed would be shared with appropriate officials "If access provides evidence of violation of law, these rules or other university rules." [6] Again, this section references the concept of "need to know" access to data, stating strongly that "the only "need to know" access to storage media contents will be conducted by the Director, Associate Directors or systems administrators of OIT and have the pre-approval of the Assistant Vice President of Information Technology." [6]

The statement on Freedom of Expression ends this section by explicitly prohibiting system administrators from removing information from accounts or forums except in specific circumstances. The only times such removal is allowed

is when "the information involves illegality, endangers computing resources or the information of others, is inconsistent with the general mission of the university, or creates a substantial risk of liability for the university." [6] This statement starts with a strong commitment to protect information, but ends weakly because the last two conditions are open to very broad interpretation by the CMU administration and OIT officials. For example, if a student published comments in an open discussion forum which were critical of the administration of a research grant by faculty or staff, and those comments threatened the grant funding, could those comments be deemed "a substantial risk of liability for the university"? [6] While the statements regarding freedom of expression support that freedom in general, the last two clauses of the statement could unintentionally cause a chilling effect one one specific area of free speech: criticism of CMU by faculty, staff, or students in electronic forums. The OIT at CMU attempts to address this in the last paragraph of the AUP document, through the creation of an internal electronic newsgroup called cmu.issues. The stated intent is to provide a forum where open political advocacy can take place, "However, to encourage and stimulate discussion and dialogue on issues of public concern, CMU employees and student may correspond via email with "cmu.issues" which is an internal electronic bulletin board (public newsgroup). This bulletin board is not to be used by employees on work time, and users are forbidden from implying that their views in any way represent official university policy." [6] This is by no means a complete solution, but at least it provides a place where staff and students can freely express their ideas and concerns on various issues.

The section describing Individual Responsibilities outlines the obligations of users of the CMU computing facilities. All of the expected statements against harassment, copyright violations, and misrepresenting your identity are described. Some areas where CMU provides additional clarification of user responsibilities draw a line between statements made by the University, and statements made by computer users anywhere on the network. "All responsibility for statements made in public computer mediated communication rests with the individual posting the statements." [6] Another clear line drawn by CMU relates to storage space on CMU owned devices. The distinction is drawn between the limited amount of space offered to users for their personal files, and space required for system files, data, and administrative software. Those two realms of data are separate at all times, and crossing this line is strictly prohibited. "Use of such system storage space is restricted to OIT managed processes and hence, unauthorized use for additional personal file storage will be considered misuse of computer facilities." [6] Again, this issue appears to stand out from the rest of the section on individual user responsibilities, primarily because it appears to be a workplace rule or policy that should be more clearly stated in employee policies, not the AUP for all users of computing resources.

The responsibilities section strictly prohibits illegal activity, and also goes one step further to define unauthorized use as theft of university resources. "Use of

the facilities by unauthorized persons is theft and is illegal under existing law." [6] In the examples of Illegal use, the policy lists harassment as illegal, then goes on to provide a separate statement on the issue. "Harassment. Harassment or destructive use is not acceptable." [6] The policy then lists under examples of Harassment the following: "For example, users shall not develop or use programs or communications that: harass other users; infiltrate a computer, computing system or network; damage or alter the hardware or software of a computer, computing system or network; degrade system performance." Clearly, only one item on this list relates to harassment issue. The rest belong under the statement on illegal uses, or in a separate category specifically addressing system intrusion and attacks with intent to damage, alter, or degrade systems. Existing law, as well as most employee workplace rules, address harassment issues more clearly. These two sections create some confusion on whether issues of harassment will be addressed as a AUP violation, an applicable violation of local, state, or federal law, or both. It should also be made clear that when issues of harassment pass from an AUP violation to a violation of law, the AUP will not protect someone in clear violation of applicable law.

The Security section of the document is primarily concerned with maintaining the uniqueness of user IDs, and requiring users to maintain the security of their individual passwords. One paragraph stands out from the rest: Review of Audit records. These paragraphs in the security section explicitly state that OIT computer systems maintain logs and audit trails. The section indicates that these are normally available for diagnostic purposes, but could be reviewed for other purposes. "Audit records may also be used in situations where it is necessary to determine what has occurred to cause a particular system problem at a particular time." [6] This implies, but does not explicitly state, that audit and log files may be used to investigate possible AUP violations. What might cause such a review is not stated, but once again CMU invokes the phrase "need to know" in this context:

> "The review of audit information will be performed only when there is a legitimate "need to know" and a request from a senior officer of CMU and approved from the Assistant Vice President of Information Technology. In such cases, a written record will be maintained of the occasion, including the name of the person accessing the audit records, the date and time of access, whose records were accessed, the extent (date and time range) of the information retrieved, and the circumstances occasioning the access. This record will be kept in the Information Technology administrative manual files under the designation "Computer Systems Audit Record Accesses." [6]

Since CMU is a public institution, and its records are subject to FOIA requests, essentially all investigative documentation becomes part of the public record, whether or not anything incriminating was discovered by the examination of the

audit files. While the record as described does not include the detail information found in the log, it also does not include any resolution or conclusions drawn from the examination of the audit files. Creating an official university record indicating that the computer use of a person or persons was examined in detail, but failing to include any conclusions of that investigation, positive or negative, could create an unintentionally misleading picture of their use of the computing resources at CMU.

The Examples of Uses section clearly states what is considered acceptable use at CMU: "Use in support of teaching and learning, or scholarly activity at CMU. Use in support of administrative data processing at CMU. Communications in support of a recognized CMU student organization. Routine correspondence and publication by faculty, staff, and students." [6] This last line is especially relevant, since the list of unacceptable uses clearly states that "Posting of information on the CMU network is to be viewed as similar to publication. Because of this, do not post instructions for how to do some illegal act...; do not ask how to do illegal acts by posting to the network; do not post messages that are libelous, harassing, or an invasion of someone's privacy". [6] While there is clear law against publishing libelous statements, harassing statements, or explicit invasions or privacy, publishing information on how to commit an illegal act is not strictly illegal in every case, and may still protected by the first amendment in some circumstances. Publishing the information may not be considered equivalent to committing the illegal act, nor is the information alone sufficient to be considered inciting others to commit an illegal act. Since the AUP states earlier in the document that freedom of expression will be protected unless the information "creates a substantial risk of liability for the university" [6], the administration would be well within its rights to remove communications that describe how to commit illegal acts from CMU controlled forums to address possible liability risks. That being the case, it should be clearly listed as unacceptable in the policy for the specific case of illegal activity, inciting others to commit illegal acts, or requests on how to perform an act that is illegal under current state, federal, or local law. In some academic disciplines, such as Criminal Justice and Law, it may be necessary to write about illegal acts in detail in order to have meaningful discussions of related issues, such as detection, deterrence, legal prosecution, and criminal defense within a courtroom setting. Blanket prohibition of such discussions may be counter to the stated goal of using computing facilities to support scholarly activity, so careful judgment is necessary before these statements can be enforced.

Overall, the CMU statement of policies does a good job of balancing liberty concerns with the need for security and network administration. Some clear conflicts remain. Liberal use of the phrase "need to know" throughout the document provides senior members of the administration with a loosely defined way to justify privacy violations and examination of files without predefined formal process. The AUP would benefit from a more clear definition of what "need to know" really means in the context where it is used. Another useful addition could

include a procedure to follow when determining when a situation actually falls under the "need to know" heading for further investigation.

THE UNIVERSITY OF PENNSYLVANIA

The AUP of the University of Pennsylvania covers many of the concerns of Liberty and Security, and refers to more detailed documents when such use is appropriate. This University actually has detailed, separate document governing AUP issues, academic freedom (referred to as Open Expression), and privacy in the electronic environment. The AUP document begins with a summary which states that the purpose for this policy is that it “defines the boundaries of “acceptable use” of limited University electronic resources”. [7] The summary also states that the AUP is based on a single principle: “that the electronic information environment is provided to support University business and its mission of education, research and service. All other uses are secondary.” [7] A broad list of categories considered unacceptable includes those that “threaten the integrity of the system; the function of non-University equipment that can be accessed through the system; the privacy or actual or perceived safety of others; or that are otherwise illegal are forbidden.” [7] The summary then informs users that they “assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable University policies, as well as City, State, and Federal Laws and regulations” [7] as listed in the rest of the AUP document. The summary makes a brief statement indicating penalties can include loss of access, employment termination, expulsion, and risk of both civil and criminal liability.[7] The summary does inform users that the document includes a laundry list of “self-contained compilation of rules that can be modified as the electronic information environment evolves”. [7] This will provide a good reference point for understanding how the principles of the summary are applied, while implying that the list is always a work in progress. Finally, the summary encourages all users to review and understand the contents of the entire policy. Since one common complaint of all users is that AUP documents are too long, this summary provides a quick, yet surprisingly comprehensive overview of the key policy issues. The assumption of personal responsibility is clearly placed on the users, who are encouraged to review and understand the policy and how it affects their use of the network. Ignorance of even the most basic principles of the AUP is a frequent excuse for AUP violations, so a summary of key principles is a good first step for informing the users of their responsibilities, and heading off conflicts.

The detailed sections of the AUP spell out the principles found in the summary. Under the Purposes section, the University clearly spells out the purposes for computing resources, and goes so far as to categorize possible uses into priority groups: highest , medium, low, and forbidden. [7] The highest priority was also identified in the summary, and is restated here as “Uses that directly support the education, research, and service missions of the University.” [7] While the purpose categories also allow for “reasonable and limited personal

communications" [7], that usage of resources is in the medium category, and can be superseded by anything deemed a higher priority. The primary stated purpose of this category is to inform users that resources are finite, and that "The University may enforce these priorities by restricting or limiting usage of lower priority in circumstances where their demand and limitations of capacity impact or threaten to impact usages of a higher priority." [7] In summary, users do not have the freedom to run anything and everything they wish on the University computing and network systems, and if the University deems something a lower priority, it may be restricted or removed from University networks or systems.

The next section is entitled Implied Consent, but covers several other key issues. The statement of implied consent begins the section, informing users with access to University computing resources that each person "is responsible for their appropriate use, and by their use agrees to comply with all applicable University, School, and departmental policies and regulations, and with applicable City, State, and Federal laws and regulations, as well as with the acceptable use policies of affiliated networks and systems." [7] This consent statement is immediately followed by discussion of academic freedom principles, referred to as "open expression" at the University. The AUP asserts that the University's Guidelines on Open Expression [8] states the University commitment to "the rights to freedom of thought, inquiry, and expression." [7] The University position on such freedom is so strong that it can effectively trump other policies. "As provided in these Guidelines, in case of conflict between the principles of the Guidelines on Open Expression and this or other University policies, the principles of the Guidelines take precedence." [7] This indicates a strong commitment to the principles of academic freedom by the University, especially if they are willing to give precedence to the free expression of ideas over other university policies. However, this "free speech" protection affects only other University policy. It should be clear from this statement that if an AUP violation falls into the realm of violating City, State, or Federal laws and regulations, the Guidelines of Open Expression will not protect a user from appropriate actions for that violation.

The Implied Consent section of the AUP continues with a definition of General Standards for the Acceptable Use of Computer Resources on campus. Unlike other AUPs which provide a "dos and don'ts" list, the General standards outline the policy in terms of behavior required of its users. The terms "respect for" and "behavior" appear in six of the eight general guidelines [7], which are broad enough to cover most areas of concern seen in other AUP documents (such as compliance with policy, not representing yourself as another, respecting system integrity, acting responsibly, respecting the rights of others, respecting the intended uses of resources.) [7] Again, for those users unwilling to read further into the document, the guidelines provide a general description of acceptable behavior, not just a laundry list of rules for users to dissect for loopholes. This is an approach with a great deal of flexibility in terms of interpretation, while providing a clearer picture to the users of what they are allowed to do without

having to spell out every possible violation in detail.

The guidelines are immediately followed by Enforcement and Penalties for Violation. This paragraph refers to the specific rules developed at the end of the document, which provide the laundry list of prohibited actions and behaviors for those unclear on how the General Standards may apply to their actions. This section reiterates the statements made in the summary, with only a small amount of additional detail, that those found violating this or related policy "may face sanctions up to and including termination and expulsion", and a that "violations can be subject to disciplinary action" [7] through appropriate existing disciplinary procedures depending on if the offender is a student, faculty, or staff member. This section ends with a single sentence: "System owners, administrators, or managers may be required to investigate violations of this policy and to ensure compliance." [7] There is no stated or implied assurance of privacy in such investigations in this sentence, other than those involved in such an investigation would by default be bound by the same AUP guidelines. This may be troubling to some users. Even if considered redundant by some, an additional sentence assuring users that such investigations would comply with existing privacy policy would go a long way to reduce conflicts on this issue.

Unlike other AUPs, this document states the mechanism for amending and interpreting the AUP. Amendment requires the Provost to consult with the University Council Committee on Communications, while official interpretations can be submitted to the same committee for review. In either case, the results are subject to submission for "publication "For Comment" in the *Almanac*, a reasonable waiting period, and publication "Of Record" in *Almanac*." [7] This provides an open process for changes to the AUP in which users have the opportunity to submit comment prior to changes taking effect. This review process would add to the time needed to change the AUP in response to new and emerging threats, but also allow for a more open process between the user populations representing liberty and security concerns in a computing environment. An additional provision allows users to seek a waiver from the Vice President for Information Systems and Computing, or the appropriate designee of that office, when "restrictions in this policy interfere with the research, educational or service missions of the University." [7] Again, if there is a clear conflict between a desired action and current policy, this represents another avenue for the user community to voice concerns and meet their computing needs when an exception is needed to fulfill the University's primary mission and purpose.

The final section of the document contains the Specific Rules Interpreting the Policy on Acceptable Use of Electronic Resources. This list of rules is "not an exhaustive list of proscribed behaviors, but are intended to implement and illustrate the General Standards" [7] as well as other relevant University policy and applicable laws. The rules are divided into four major categories; Content of Communications; Identification of Users; Access to Computer Resources; and

Operational Integrity. As with the General Standards, all the more obvious disruptive actions threatening liberty and security are prohibited. However, the first two items under Content of Communications may come in conflict with each other in certain circumstances. The first rule states that, except when policy and law are clearly violated, that "the content of electronic communications is not by itself a basis for disciplinary action." [7] This is immediately followed by the rule that "Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications (as defined by law) are prohibited." [7] The conflicts between free speech and what is defined as obscene, be it obscene speech or graphic representations, currently fill many volumes in most legal libraries. Enforcement of any alleged AUP violation involving obscenity would require some involvement from university legal departments. Since many legal cases involving obscenity use some form of acceptable community standard to determine when something is considered obscene, this could be problematic. Universities are made up of diverse populations with differing backgrounds and, by extension, differing community standards for obscenity. As an example, imagine a user posts a message to a forum that discussed another work (such as a movie, novel, or play) which contained numerous quotations from the work that included foul language and descriptive words which another reader of this forum finds obscene. The offended reader complains, so which rule applies? To the user posting the message, the language is not obscene, so by the first rule, the content of their message alone is not a basis for discipline. By the standards of the second user, the content is considered obscene, and since the poster has violated the second rule, the protection of the first rule no longer applies. Who would be right? The answer to this and similar questions is not easy in obscenity cases. Adding the caveat "(as defined by law)" does not necessarily make the issue clearer in the case of conflicts over obscenity and what is considered obscene. Rather than single this out as an exception, it may be a better approach to include an additional rule informing users that issues involving apparent conflicts between first amendment rights and community standards for appropriate communications will be handled by the appropriate University committee or other existing enforcement authority. Otherwise, you could run the risk of having to sanitize all communications to meet the expectation of the least tolerant community for what is "appropriate" and what is "obscene".

The Appendices of the AUP at the University of Pennsylvania provide a list of the most relevant University policies and applicable state and federal laws and regulations which may apply to the use of computing resources. In the list of applicable University policy, the two policy statements that all computing is "required to conform" [7] to are the Code of Student Conduct, and the Guidelines on Open Expression. This is followed by a list of additional University policies that are considered applicable to the use of computing resources. The Policy on Privacy in the Electronic Environment [9] is far down on this second list, seventh in a list of eleven applicable policies. It is listed after policy statements which may not apply to all users, such as Patent Policy, and the Policy Regarding Faculty

Misconduct in Research. Considering that privacy policy applies to all users of the network, regardless of their role on campus, the lack of emphasis on this policy throughout the AUP document could be somewhat discouraging to those seeking strong privacy assurances. Users who never read past the summary will never reach a link to either the Guidelines of Open Expression, or the Policy on Privacy in the Electronic Environment. As a result, they may never have a clear understanding of their rights and responsibilities with regard to the critical issues of liberty at University of Pennsylvania.

While the AUP at the University of Pennsylvania provides both detailed and summary information regarding security and appropriate use issues, forcing users to refer to multiple documents for information on academic freedom and privacy could discourage users from fully investigating their rights and responsibilities when using computing resources. The addition of statements in the summary which directly reference key points in the Guidelines of Open Expression and the Policy on Privacy in the Electronic Environment would enable the summary to clearly communicate the University's key points on matters of security and liberty.

Resolution of Conflict Through Strong AUP Policy Choices

After reviewing several Acceptable Use Policy documents, it seems that the strongest AUP statements recognize the conflict areas between liberty and security, then take positive and direct action to address them. Strong policy statements provide the levels of security necessary to guarantee both privacy and freedom of expression for legitimate users of computing resources, while preserving system integrity and availability, and defending against attacks and inappropriate use of resources.

Another way to view the conflict between liberty and security is to consider the concept of a Social AUP compared against a Legal AUP. “Material violates the Social AUP if it is legal but you dislike it or find it offensive..... Material and behavior violates the Legal AUP if it violates the law... Put another way, academic freedom requires that we distinguish between what we dislike and what we outlaw.” [2] A strong AUP attempts to define the rules governing both the Social and Legal behavior of users. Many issues related to academic freedom of expression straddle both social and legal realms. Great care must be taken to insure that the free exchange of ideas in an academic environment does not fall victim to excessive restrictions designed to protect the institution from all possible forms of legal liability. Conversely, placing too strong an emphasis on academic freedom can hinder those tasked with safeguarding said freedoms because privacy issues prevent any meaningful investigation of violations. In more recent discussions at Michigan State University, the Network Communications Committee expressed the reservation for a recent draft Acceptable Use statement that the document “might allow the privacy and other

rights of the individual to not be protected to the greatest extent possible.... The desire is that the pendulum not swing too far in the opposite direction from the previous case of essentially iron-clad protection of the individual." [10] This balancing act must be reflected in the AUP wherever social and legal issues collide. While there is no one way to resolve these issues that would fit all academic institutions, there are some critical areas to examine in order to minimize the conflicts between liberty and security in AUP statements.

At Michigan State University, "the current discussions of "Acceptable Use" of computing and networking facilities were initiated in part to find a balance between an individual's right to privacy and the public health of MSUnet that would allow the various system staffs to better combat the ever increasing threats to normal operation." [10] Critical to finding and maintaining this balance is some formal definition of the "public health" of the network and computing environment. If the policy goal is to define usage and restrictions which help guarantee that services remain available for all users, then you need a definition of what the "healthy" state of your network should look like. Often, this is done by creating a list of undesired activities, such as hacking, sniffing, stealing identification and passwords, and altering systems and services without authorization. If you have a clear statement of what systems and services your computing environment offers in its "healthy" state, you can clearly enumerate what makes the environment "unhealthy", and what behaviors need to be proscribed to maintain the health of systems. Without the "healthy" state as your baseline, you can make a long list of prohibited actions and activities, but someone else will think of something not on the list which threatens the health and function of your computing resources. Without a definition of "healthy", you don't have as clear an idea of when action is necessary under the AUP to insure health, or to restore health after an incident occurs.

From the examples examined, strong AUP documents contain some definition of privacy, and the limitations and boundaries of privacy across systems. In addition to the basic definitions, strong AUP statements make some effort to describe the issues which could precipitate a loss of privacy, and the limitations of acceptable levels of intrusion if the institution has some legitimate need to violate privacy (for example, when investigating alleged violations of policy). "in order to maintain integrity of the networked environment, appropriate restrictions on some aspects of individual privacy and use may be necessary." [11] When drafting an AUP, there is a need to ask some basic questions related to privacy. Do all your users know what data is considered private or public when they visit a website, fill out an online form, or send an email? A strong privacy policy may not be able to answer every possible question posed by every possible situation in a campus environment. A privacy statement should define what is considered a reasonable level of privacy in general; detail levels of privacy for common systems which apply to all users; and then to point users to additional resources, or a separate privacy policy if needed.

On the administrative side of this issue, another layer exists: what kinds of incidents can and should be investigated? If data is examined in the course of an investigation that is considered private in other circumstances, who is allowed to look, and what protections are they then required to use to guarantee privacy during the investigation? Who watches the watchers, and how are audits conducted? After an investigation is completed, who is responsible for the security, storage, or disposal of collected information? Such administrative issues are usually handled outside the AUP in other documents, such as employee handbooks, or policy and procedure related to the conducting of information audits. Regardless of how such issues are resolved at the administrative level, the privacy statement in the AUP should include some basic statement regarding how privacy will be protected by those charged with investigating and resolving alleged AUP violations. Privacy guarantees assume a level of trust between the watchers and those watched. Every effort should be taken to build that trust by communicating where and how privacy issues are respected, and when privacy can be violated in pursuit of another institutional value such as security, or the integrity of systems and computing resources. In conjunction with such statements, the privacy policy should state how far into “private” data an authorized investigation may go, who has the right to authorize the investigation, and what penalties apply to those who inappropriately use data during an incident investigation in a way that violates privacy rights. Simply stating a commitment to privacy in the AUP is not enough to engender trust among the user population. Some effort, no matter how brief, should be made to communicate how privacy is respected, and what limitations on privacy exist in the computing environment.

The statements in an Acceptable Use Policy will at some point collide with other policies that apply to the use of computing and network resources. No AUP can anticipate all possible conflicts of policy, nor should it attempt to do so. However, strong AUP statements will include some provisions or mechanisms to resolve "collisions" between Acceptable Use Policy and stronger policy that may already be in place on campus. Establishing an order of precedence between related policy documents, or simply stating which policy prevails when two closely related policies collide helps define the rules that apply to resolve such conflicts. The example in the University of Pennsylvania's AUP states that when conflicts between it and the Guidelines for Open Expression occur, the Guidelines take precedence. [7] This relationship of precedence should be clearly stated for the more commonplace areas where the AUP comes into conflict with other policy, such as:

AUP conflicts with Student Codes of Conduct
AUP conflicts with Faculty Conduct or Governance Guidelines
AUP conflicts with Employee or Workplace Rules
AUP conflicts with City, State, or Federal regulations and law

In many cases, it will be quite clear by the nature of the conflict which policy, regulation, or law holds precedence. However, if it is clearly stated in the AUP document, there can be no confusion among users, and no attempts by the user

population to excuse a violation of another policy because their action did not explicitly violate the AUP.

Where possible, if existing bodies in the University are responsible for adjudication of alleged policy violations, some reference to those bodies should accompany the listed policies. It should not be necessary for the AUP document to restate in detail the scope and purpose of each body, but some reference to the group associated with each policy would be helpful to the user reading the document. It is important to state clearly that usage of computing and network resources which does not violate the AUP, but does violate other stated policy, rules, procedures, or regulations must still be addressed by an appropriate mechanism. Even if the investigation of a possible AUP violation leads the investigator to discover that other policy had been violated using computing and network resources, action appropriate to the policy violated must be taken. Taking the University of Pennsylvania as an example, the school has established a Committee on Open Expression to mediate in cases where the Guidelines on Open Expression were violated, and to issue rulings on the interpretation of the Guidelines when conflicts arise. [8] It should be strongly noted that someone using computing and network resources to violate existing local, state, or federal law cannot be ignored simply because the investigation shows they didn't actually violate the AUP in the process. In such cases, the AUP needs to clearly state that suspected criminal activities will be investigated by appropriate authorities.

Summary

Strong Acceptable Use Policy statements cannot arise from a vacuum, nor can they arise from the thoughts of a single person. Clear, open communications between administrative policy makers, and the various and diverse user communities that make up the University are necessary to identify the issues critical to the process of writing, or rewriting an AUP. The administrative needs of those maintaining systems and networks, as well as the business goals and legal concerns of the University must be balanced against the concerns of the faculty, staff, research, and academic communities. A strong AUP document should undergo review by University legal council, administrative and business groups with AUP concerns, as well as faculty, staff, and student populations in order to be as comprehensive as possible. It should be clear that an AUP document cannot possibly counter all concerns, address all possible risks, or satisfy all user populations. A properly constructed AUP should provide the guidance necessary to resolve the unavoidable conflicts between liberty and security concerns in a way that is both clear and fair to all parties concerned.

References

1.Grossman, Mark. Drafting an Acceptable Use Policy, New Jersey Law Journal, 6 Sept 1999 v. 157, pp 1005-1006.
2.Kadie, Carl. "Content: The Academic Freedom Model." Third Conference on Computers, Freedom, and Privacy. Burlingame, California, March 1993, http://www.eff.org/Censorship/Academic_edu/CAF/statements.cfp93.kadie
3.Gelman, Robert B. and McCandlish, Stanton. Protecting Yourself Online: The Definitive Resource on Safety, Freedom & Privacy in Cyberspace. San Francisco: HarperCollins, 1998
4.Hiram College Computing Facilities and Services. Hiramnet Acceptable Use Policy, 1 June 2002, http://home.hiram.edu/computers/acceptableusepolicy.asp, (27 July 2004)
5.Michigan State University. Michigan State University Acceptable Use of Computing Systems,Software, and the University Digital Network, 4 Aug. 1992, http://www.msu.edu/aup, (10 October 2004)
6.Central Michigan Office of Information Technology. Compting and Network Resrouces Policy, 22 Dec. 1998, http://www.oit.cmich.edu/it/policies_computing.asp, (18 Aug. 2004)
7.University of Pennsylvania. Penn Computing: Policy on Acceptable Use of Electronic Resources, January 1993, http://www.upenn.edu/computing/policy/aup.html, (27 July 2004)
8.University of Pennsylvania. Guidelines on Open Expression, April 1991, http://www.vpul.upenn.edu/osl/openexp.html, (27 July 2004)
9.University of Pennsylvania, Policy on Privacy in the Electronic Environment. Almanac, Vol. 47. 15 Sept. 2000. http://www.upenn.edu/almanac/v47/n04/OR-eprivacy.htm, (27 July 2004)
10.Atkinson, T. V. Memo to Gift, David. "NCC Recommendations for Acceptable Use Documents", 29 March 2004, http://msu.edu/unit/ncc/Documents/AUP/AUPcovMar2004.pdf, (12 Sept. 2004)
11.Michigan State University Network Communications Committee. Draft: MSU Acceptable Use of Computing and Network Resources, 17 March 2004, http://msu.edu/unit/ncc/Documents/AUP/AUP17Mar2004.pdf, (12 Sept. 2004)

Acknowledgments

I would like to acknowledge the many discussions and debates I have engaged in as a member of the Michigan State University Network Communications Committee, or NCC. I have served on the committee since 1996, during which time I have participated in many discussions of the strengths and flaws found in the Michigan State University AUP from 1992. Even though these discussions did not provide me with quotable references, I must acknowledge their influence on my thinking, and on my analysis of the AUP documents found at other institutions. The concept of considering the integrity of networks and systems, and attacks and threats to those systems, in a similar paradigm to the "public health" concept in living populations is a direct result of numerous discussions between the committee and David Gift, Vice Provost for Libraries, Computing, and Technology at Michigan State University. The breakdown of Liberty and Security concerns into four broad categories owes a great deal to these discussions as well. Further acknowledgments must go to the members of the NCC Subcommittee on Acceptable Use Policy, who have wrestled with policy issues related to the redrafting of the MSU AUP for over a year. Where possible, I have quoted from the public draft documents published by NCC on this topic. The detailed analysis of the college AUP documents, and my conclusions based on that analysis are strictly my own.

APPENDIX A

Found at http://www.msu.edu/au/

Michigan State University Acceptable Use of Computing Systems,

Software, and the University Digital Network

(Administrative Ruling)

---

* MichNet Acceptable Use Policy
  <http://www.merit.edu/mn/about/policies-acceptableuse.html>

* Computing at MSU <http://computing.msu.edu>

* MSU Home Page <http://www.msu.edu/>

I. Foreword

Access to modern information technology is essential to the pursuit and achievement of excellence across the MSU mission of instruction, research, and service outreach. The privilege of use of computing systems and software, as well as internal and external data networks, is important to all members of the University community. The preservation of that privilege for the full community requires that each individual faculty member, staff member, and student comply with institutional and external standards for appropriate use.

To assist and ensure such compliance, Computing and Technology, with the advice and counsel of the all-University Computing and Communications Systems Advisory Committee, establishes the following administrative ruling, applicable to all faculty, staff and students.

II. Definitions

A "System Sponsor" is the individual under whose authority a computing system, local network, or external network connection is funded. Individual computer systems and local networks may be sponsored by faculty members (e.g., using research grant funds), or by departments, colleges, or other units, in which latter case the unit administrator is the System Sponsor. For the purposes of this ruling, the Director of the

MSU Computer Laboratory is the System Sponsor for the inter-building MSU digital network and for MSU external network connections, including those to BITNET, CICNET, and MERIT and other parts of the national Internet.

A "System Manager" is the person who is authorized by a System Sponsor to grant and create user privileges, maintain the system filestore, and generally ensure the effective operation of a system. (For example, in the case of UNIX systems, the System Manager typically will be the "superuser" who uses the "root" user ID.) In some cases, the System Manager and the System Sponsor may be the same individual.

"Facility Staff" are the individuals who are authorized to monitor, manage, or otherwise grant temporary access to computing facilities (such as microcomputer laboratories) in which one or more systems are used on an open access basis by either specific populations of faculty, staff, and students, or the entire campus community.

A "User" is any individual who uses, logs in, attempts to use, or attempts to log in to a system, whether by direct connection or across one or more networks, or who attempts to connect to or traverse a network, whether via hardware, software, or both. The term "User" thus includes System Sponsors, System Managers, and Facility Staff.

III. Implications of Diversity in the Information Technology Environment

1. The provision and use of computing and networking privileges is governed by Michigan State University's Anti-Discrimination Policy. System Sponsors are responsible for ensuring full compliance.

1.1 Access to computing or networking hardware or software is not to be restricted based upon ethnic or national origin. Restrictions predicated on citizenship are in general to be avoided, and must in every case receive prior approval from the Vice Provost for Computing and Technology, who will consult with the Office of the University General Counsel in each instance.

2. Because computing systems at MSU serve diverse purposes and diverse constituencies, System Sponsors are accorded wide discretion in establishing reasonable and appropriate policies applicable to their systems. (For example, some System Sponsors, to achieve their particular goals, may permit or encourage the playing of computer games. On other systems, System Sponsors may legitimately prohibit game-playing in order to conserve scarce resources.) The effectiveness of such policies depends substantially on their systematic communication to Users,

typically at the time usage authorization is first granted by the System Manager or by Facility Staff.

3. Users must expect considerable variation in what constitutes acceptable use from system to system, and must make reasonable efforts to inform themselves about the particular policies applicable to each system they use. In cases of doubt, the burden of responsibility is on the User to inquire concerning the permissibility of an action or use, prior to execution. Questions should be directed in turn to Facility Staff, the System Manager, and the System Sponsor.

4. Even within a single system, it is sometimes appropriate for System Sponsors and/or System Managers to establish different categories of user accounts or ID's, sometimes with different attendant charges or privileges, and to authorize a single user to access accounts or ID's in two or more categories. In such cases, Users must restrict their usage of each account or ID to that appropriate for it. Similar considerations apply when accounts or ID's are held on multiple systems. (Example: a student may have a limited resource account for classwork and an unlimited resource account for research. Unauthorized use of the unlimited resource account to create a competitive advantage in the classwork is inappropriate and may be construed as academic dishonesty.)

5. Michigan State University utilizes a wide variety of software, with an equally wide range of license and copyright provisions. Users are responsible for informing themselves of, and complying scrupulously with, the license and copyright provisions of the software that they use.

5.1 No software copy is to be made by any User without a prior, good faith determination that such copying is in fact permissible. All Users must respect the legal protection provided by copyright and license to programs and data.

5.2 The licenses of certain advanced software tools (e.g., some expert system generators) require that intellectual products produced with such tools be provided to the licensor. System Sponsors are responsible for ensuring that such requirements are publicized to Users appropriately by System Managers and Facility Staff. System Sponsors and Users are jointly responsible for ensuring compliance with such requirements.

IV. Good Citizenship In "Cyberspace"

1. All Users must respect the privacy and usage privileges of others, both on the MSU campus and at all sites reachable by MSU's external network connections.

1.1 Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other Users, whether on the MSU campus or elsewhere, or develop or retain programs for that purpose, without the authorization of the file owner or the Vice Provost for Computing and Technology. Reasonable file copying (e.g., in back-ups) and password changes are permitted among the routine tasks of System Managers and of appropriately authorized Facility Staff.

1.2 Users shall not represent themselves electronically as others, either on the MSU campus or elsewhere, unless explicitly authorized to do so by those other Users. To be valid, such authorization of one User by another User must not circumvent established, system-specific policies defining eligibility for resource access.

1.3 Users shall not intentionally develop or retain programs that harass other Users, either on the MSU campus or elsewhere.

1.4 Users shall not obstruct or disrupt the use of any computing system or network by another person or entity, either on the MSU campus or elsewhere, whose usage is protected by law, ordinance, regulation, policy, or administrative ruling.

2. All Users must respect the integrity of computing systems and networks, both on the MSU campus and at all sites reachable by MSU's external network connections.

2.1 Users shall not by any means attempt to infiltrate (e.g., gain access without proper authorization) a computing system or network, either on the MSU campus or elsewhere.

2.2 Users shall not attempt to damage, or alter without proper authorization from the System Sponsor, either the hardware or the software components of a computing system or network, either on the MSU campus or elsewhere.

3. All Users of MSU's external network connections shall comply with the evolving "Acceptable Use" policies established by the external networks' governing bodies.

(Editor's note: the following documents are on file in the Computing Information Center, form the Network Services server, and via FTP from the individual organizations)

3.1 The current NSFNET policy is attached as Appendix A of this ruling.

3.2 The current CICNET policy is attached as Appendix B of this ruling.

3.3 The current MERIT policy is attached as Appendix C of this ruling.

3.4 The MSU Computer Laboratory will publish revisions of external networks' "Acceptable Use" policies, making them available to Users in both printed and electronic form.

3.5 In cases of doubt, Users bear the burden of responsibility to inquire concerning the permissibility of external network uses, prior to execution. Such questions should be directed to the MSU Computer Laboratory's main office.

4. Computing and networking resources are sometimes in scarce supply. Resource contention may variously involve disk space, CPU time, terminal or workstation keyboard access, printer access, plotter access, software access and network bandwidth. Priorities between uses (e.g., instruction versus research versus system maintenance) and between Users (e.g., students in different classes) will vary from system to system and according to time of day, week, semester, and year.

4.1 System Sponsors, and by their delegation System Managers and Facility Staff, have broad discretion to set and revise reasonable usage priorities and operational policies (such as hours of operation, usage time limits, populations to be served, etc.) They may also take such routine steps (e.g., removing hung jobs, updating system configurations and user defaults, reprioritizing resource-intensive jobs, managing print queues, backing up systems, etc.) as may be reasonably necessary for the operation of their systems or facilities.

4.2 Users are expected to comply fully with the instructions of Facility Staff, System Managers, and System Sponsors. In particular, Users will vacate terminals, workstations, or the facility and will surrender other resources (such as printers and software) promptly when asked to do so, both at closing times and when necessary to permit access by others.

4.3 Where possible, Users should be provided systematic means (e.g., through facility, departmental, or college computing advisory committees, or via CCSAC at the All-University level) to advance suggestions and criticisms concerning the priorities and their implementation. Appropriate avenues for complaints concerning services provided by Facility Staff also should be provided.

V. Enforcement and Adjudication

1. The principal responsibility for investigation of suspected non-compliance with the provisions of this ruling rests with System Sponsors. At their discretion, they may delegate it to System Managers and/or Facility Staff.

1.1 The investigation of alleged or suspected non-compliance with this ruling is to be conducted with due regard for the rights of all Users, such as the rights to privacy and intellectual property.

1.2 System Sponsors may suspend service to Users without notice when reasonably necessary to the operation or integrity of the system or the networks connected to it; they may also delegate this judgment and authority to System Managers.

1.3 Cessation of service, whether by network disconnection or disablement of log-in capability, shall be utilized in preference to file inspection when remedying or investigating instances of alleged disruption.

1.4 The content of User files is not to be surreptitiously or otherwise examined, nor is the User-generated message content of User network transactions to be monitored, without the prior written permission of either the User involved or the Vice Provost for Computing and Technology. However, System Managers and others charged by them with forwarding misdirected or undeliverable electronic mail and/or delivering print-outs and plots may examine such mail or hard-copy to the extent reasonably necessary for such purpose.

2. Subject to the non-discrimination provisions herein, faculty members acting as System Sponsors for computing systems or local networks established with their own research grant funds may change, suspend, or revoke User privileges in the best interests of the research being conducted.

3. When an instance of non-compliance is suspected or discovered in a computing system or network established by a department, college or other administrative unit, a unit administrator (typically the System Sponsor) shall proceed in accord with Section 5.6.3 of Academic Freedom for Students at Michigan State University.

3.1 System Sponsors may elect to refer the issue to the Vice Provost for Computing and Technology for handling. They must always do so if systems or networks in multiple campus units have been disrupted or compromised, or if any non-MSU system, network, or party is involved.

3.2 Internal disciplinary action may be appropriate in some cases of non-compliance with this ruling. Relevant General Student Regulations include 1.05, 1.06, 2.02, 2.04, 4.03, 4.05, 4.06, and 5.02; allegations are adjudicable under Article IV of Academic Freedom for Students at Michigan State University. Disciplinary issues concerning students, faculty, or staff should be discussed with the Vice Provost for Computing and Technology before action is taken, in the interests of consistency of treatment.

3.3 Criminal or civil action against faculty, staff, or students may be appropriate in some instances. Such cases should be discussed with the Vice Provost for Computing and Technology, in the interests of consistency of treatment.

Approved:

Network Communications Committee of C.C.S.A.C. (May 29, 1992)
C.C.S.A.C. (June 8, 1992) Vice Provost for Computing and Technology (August 4, 1992)

URL: http://www.msu.edu/aup/
Updated: September 17, 1998

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event