UNIVERSITY OF HAWAI'I

PRESIDENT, UNIVERSITY OF HAWAI'I AND
CHANCELLOR, UNIVERSITY OF HAWAI'I AT MĀNOA

October 12, 1999

EXECUTIVE MEMORANDUM NO. 99-7

TO: University Executive Council
Provosts
Deans and Directors
Faculty Senates, All Campuses
Student Governments, All Campuses

FROM: Kenneth P. Mortimer Kenneth P. Mortimer
President, University of Hawai'i and
Chancellor, University of Hawai'i at Mānoa

SUBJECT: **EXECUTIVE POLICY ON USE AND MANAGEMENT OF INFORMATION TECHNOLOGY RESOURCES**

I am hereby officially promulgating a new Executive Policy E2.210 "Use and Management of Information Technology Resources." It will also be posted on the World Wide Web. This policy supercedes the interim policy which had previously been in use.

I would especially like to thank those of you who provided your thoughtful input on the draft of this document which was circulated late last year. It should surprise nobody that the input received was often contradictory in nature. This version of the policy addresses all of the concerns and issues raised, although not necessarily to the complete satisfaction of all parties.

Nonetheless, I am confident that everyone will agree that adoption of this policy represents a major step forward in protecting all members of the University community and the institution. It establishes a framework for the appropriate use and management of institutional information technology resources based upon principles of due process within the context of existing policy and law. And like any institutional policy, it can be modified over time based on our experience, needs and the changing technology environment.

Please ensure that this policy is made available within your units. Your support and assistance in seeing that this policy is followed will be appreciated.

Attachment

E2.210 -- Use and Management of Information Technology Resources

I. Preamble

"Academic institutions exist for the transmission of knowledge, the pursuit of truth, the development of students, and the general well-being of society. Free inquiry and free expression are indispensable to the attainment of these goals ... The responsibility to secure and to respect general conditions conducive to the freedom to learn is shared by all members of the academic community. Each college and university has a duty to develop policies and procedures which provide and safeguard this freedom."

- Excerpt from the American Association of University Professors (AAUP)
Joint Statement on Rights and Freedoms of Students

II. Context

This document is the basis for university-wide policies and practices for the acceptable use and management of all University of Hawai‘i (hereafter called UH or University) information technology resources. It is intended to define and provide effective protection, equitable access, and administrative guidelines for the use of those resources. The purpose of these guidelines is not to replace but to supplement existing laws, regulations, general codes of conduct, agreements, and contracts that are currently in place.

In support of its mission of teaching, research, and public service, and within its institutional priorities and financial capabilities, the University of Hawai‘i provides access to computing, network and information systems and services for the students, faculty and staff who form the basis of the UH community. Collectively, these computing, network and information systems and services comprise the institution’s information technology infrastructure. The University strives to create an intellectual environment in which its community can effectively access and create information and collaborate with colleagues both within the UH system and at other institutions. As it does so, the University is committed to maintaining an information environment that is free of harassment and is accessible to all members of its community. Such an environment can only exist when the users and managers of the information technologies behave responsibly and respectfully.

This policy creates the basis for such an environment by outlining the philosophy and general principles for appropriate use and management of information technology resources by University faculty, staff and students. It applies to all computing, information and network systems and services owned or administered by the University of Hawai‘i, as well as to individual activities that take place over the Internet or other external network connections using University systems, connections or user accounts.

Appropriate use of technological resources is framed by the same legal and ethical considerations as are applicable to other public resources. Access to UH networks and computer systems is a privilege granted subject to existing University policies (e.g., the Student Conduct Code) as well as all applicable local, state, and federal laws (e.g., copyright law, child pornography prohibitions, computer crime statutes).

The University requires that all its students, faculty, staff and approved guests abide by these policies. In addition, users of specific technology resources and services that are provided in cooperation with larger communities or third parties (e.g. the Internet), must also adhere to codes of conduct which the University accepts implicitly or explicitly on behalf of all its users. The University strives to inform all users of these policies, but users are responsible for their own actions. The University accepts no responsibility or liability for the specific acts of individuals that violate this or any other authorized policy, code of conduct or statute.

For informational purposes, the computer crime statute from Hawaiʻi's penal code is included herein as Appendix A and portions of the State Ethics Code are included as Appendix B.

III. Responsible Use

A. Privileges and Responsibilities

The University of Hawaiʻi defines and provides access to institutional computers, information systems and networks as a privilege rather than a right. Reliable and safe access to the University's information resources requires that users accept their responsibilities to behave in ways that protect the community, and by so doing they also preserve their own access.

All users must respect the rights of others, the integrity of the facilities and controls which are implemented to maximize the community's reliable access, and all pertinent license and contractual agreements that underlie the University's technology infrastructure. It is the policy of the University to deny access to any member of the user community who violates this policy or who uses the University's technology resources to violate other duly established policies or laws.

B. Principles of Responsible Use, with Examples

All users have the responsibility to operate the University computing systems in an ethical, lawful and responsible manner. These principles of responsible use are derived directly from standards of decency and common sense that apply to the use of any shared public resource. They apply equally to users who are students, faculty, staff or any authorized guest user of the University's systems, networks and services. Each of the following principles includes examples of prohibited behaviors. These examples are intended to illustrate the range of unacceptable actions rather than to exhaustively elaborate all specific behaviors that may violate the principle.

1. Users must adamantly protect their personal passwords

   Passwords are the basic security mechanism which authenticate individuals as eligible to use University resources. The username and password also authorize individuals to perform specific actions based on the identity of the user, such as permitting students to drop classes or faculty to view class lists. Many legal and ethical violations begin when the culprit obtains use of someone else's password, wittingly or unwittingly shared.

   Passwords should be chosen that are difficult to guess and should not be written down. Experts recommend changing passwords on a regular basis. Under no circumstances should a password be shared with a family member, friend or acquaintance, much less any stranger or caller. Appendix C contains a guide to the selection and management of personal passwords. Users should immediately report any suspected unauthorized use of their username to their system administrator.

2. Users must respect the privacy of others' passwords, information and communication, and may not attempt to use University resources to gain unauthorized access to any site or network or to maliciously compromise the performance of internal or external systems or networks

Digital environments present certain new opportunities for abuse, but the infractions and consequences are often comparable to those in the physical world. Just as an unlocked door is not an invitation to theft, everything that is technically possible is not permissible or legal.

Users must not store or run programs intended to obtain others' passwords. Users must not look over others' shoulders to try to obtain passwords or otherwise try to obtain unauthorized access to the information or communication of others. Users may not "sniff" networks or undertake comparable measures to obtain access to passwords or other information not made publicly available by the owner. Users may not attempt to gain unauthorized access to other systems, networks and services external to the University via the University's Internet or other network connections. Nor may programs be stored or executed that attempt to gain unauthorized system-level access to computers or network devices either inside or external to the University.

Users may not store or execute programs or engage in or abet any activities designed to test or compromise system or network performance without the prior written authorization of the responsible system administrator(s). This includes programs that introduce a virus, worm or other destructive/disruptive programs. Users may not launch "denial-of-service" attacks against internal or external systems and networks from within the University.

Violations of this policy may also be subject to prosecution under the federal Electronic Communications Privacy Act (ECPA) of 1985 which protects the confidentiality of personal electronic communications or the Hawaiʻi Penal Code provisions for computer crime. Under no circumstances will excuses be accepted that such behaviors were intended purely for educational purposes or to help system administrators improve security.

3. No individual may falsely represent themselves or "spoof" another physical network connection

Violations of laws, codes of conduct or usage policies are usually attempted under false identities. Academic integrity dictates that members of the University community be accountable for their actions. Users may not attempt to represent their network activities as originating from a network address other than the actual source (i.e. "spoofing"). Nor should users falsely identify themselves in their email or postings. There are legitimate uses for anonymity in certain specific communications forums, but it is generally not considered appropriate in most on-line discourse.

4. Users must observe all laws relating to copyright, trademark, export and intellectual property rights

Intellectual property is the lifeblood of a university, and all members of the university community should respect the work of others inside and outside the academy. Software may not be duplicated or installed except in strict accordance with applicable licensing agreements. Software not eligible for export may not be freely stored on University systems or transmitted outside the U.S. And University servers and networks may not be used to house or distribute unauthorized software, music, video or other information resources. The University will actively participate in the prosecution of members of the community who violate the law, for example, by mounting illegal music or software distribution servers using University resources.

The University of Hawaiʻi adopts the EDUCOM Code, a statement on Software and Intellectual Rights, incorporated herein as Appendix D. EDUCAUSE, which has since incorporated EDUCOM and its programs, is a non-profit consortium of colleges and universities committed to the use and management of information technology for teaching and learning.

Pursuant to the Digital Millennium Copyright Act (1998), notifications of claimed infringement using University of Hawaii services should be filed with:

Director of Information Technology
University of Hawaii
2532 Correa Rd.
Honolulu, HI 96822
Tel: 808-956-3501
Fax: 808-956-5025
Email: dmca-agent@hawaii.edu

5. Users must ensure that their electronic communications do not infringe the rights of others and are conducted in accord with the same standards of behavior that apply in other forms of communication

The privilege of Internet access offers numerous opportunities to interact with others all over the world. As an institution of higher education the University supports open and unrestricted communication by members of its community. However, many people have a tendency to send email, post messages, or engage in other behaviors that they would never think to perform in person. Electronic communication may lack the visual and verbal cues such as a smile or tone-of-voice that indicate when someone is joking, so misinterpretation may be more likely than in-person. For this reason, it is suggested that people exercise even more care in their on-line communication than face-to-face.

The same legal and policy standards that define intimidation, harassment or invasion of privacy apply to the electronic environment. For example, persistence in sending unwanted email constitutes harassment and is unacceptable if not illegal. Display of sexually explicit images or sounds where others can see or hear them may create a hostile environment and could constitute sexual harassment according to University policies on sexual harassment. And obscene email is comparable to obscene phone calls or letters. Laws relating to child pornography, obscenity and defamation apply in electronic environments and the University will willingly cooperate in the prosecution of individuals formally charged with such offenses.

Finally, users should be aware that each specific on-line forum or mailing list might have specific standards of content and behavior to which its members are expected to adhere. These may range from “no anonymous messages” to “no posting of job ads on this mailing list.” The University will cooperate in helping the managers of external forums enforce their standards, just as we expect other institutions to cooperate in helping members of the UH community manage their forums based on the public standards of behavior established for their group.

6. University resources are intended to be used for institutional purposes and may not be used for private gain.

The University provides information technology resources at great expense for the purpose of supporting its mission (learning, teaching, research, and public service). It is expected that usage will be primarily educational in nature in support of this mission.

All applicable laws and policies relating to the ethical use of public resources apply to University information technologies as well. The Hawai‘i State Ethics Code prohibits use of University resources for private business purposes (see Appendix B) and under no circumstances may individuals use institutional technology resources for commercial purposes without prior written authorization. This includes activities such as the use of University email or web sites for marketing a home business, hosting a commercial home page, or providing friends who are not members of the University community with access to institutional equipment and services. Users may not run private servers or bulletin board systems for non-University purposes through University networks or provide such connectivity to others. Political campaigning may not be engaged in using the University's electronic information systems

7. Users may not engage in activities which compromise institutional systems or network performance for others

The University administers its technology resources on a shared-use basis for the benefit of the entire community. This is only possible when all members of the community respect the need of others for services. In addition, portions of the Internet itself may be vulnerable to disruptions in service by malicious activities. As a whole, the Internet protects itself through an informal and evolving code of behavior among system administrators. The University of Hawaii is committed to be a good institutional citizen of the Internet, noting that non-cooperating institutions are sometimes blacklisted from certain services which could prevent members of the University community from achieving their legitimate academic requirements.

As a general rule, the University tries to be permissive rather than prohibitive in these matters, but certain behaviors by individuals can compromise the availability and reliability of services for the entire community. Examples of such activities include the unauthorized running of "server" programs on institutional systems or hosting non-educational web sites intended to do nothing more than generate high "hit counts." Nothing in this section is intended to discourage faculty or staff from operating authorized servers in a responsible manner in support of the mission of the University. While it attempts to manage resources on a content-neutral basis, the University does reserve the right to curtail specific uses of its technology infrastructure that unduly interfere with the institution's ability to provide the best possible service to the overall community.

Users may not engage in the transmission of unsolicited bulk email ("spamming"), regardless of how important it may seem to the sender. Email is a form of individual communication, not a public forum, and should not be used to express opinions or forward views to those who have not expressed a wish to engage in the dialog. This policy shall in no way limit the use of email as a legitimate means for the University community to share information and communication.

Under no circumstances may users create, transmit or forward electronic chain letters. Chain letters are often social notes, wishes of good fortune or most insidiously, bogus virus warnings which request the recipient to forward the message to friends and colleagues *ad infinitum*. Such notes can have a significant and consequential impact on institutional resources as they are forwarded around University systems. Users may not initiate or participate in the targeting of a particular person or system with mass quantities of email ("mail bombs"). In the paper world junk mailers bear the full costs of such activities when they choose to buy a stamp and envelope, but with University email the costs are borne by the entire community and the taxpayers of the State.

Activities such as spam, chain letters, and mail bombs degrade performance of networks and systems, may violate agreements with third parties such as the University's Internet Service Providers, and may even endanger the availability of the email services for the entire institution. Violations may be cause for the revocation of the offender's access to University resources.

IV. Confidentiality and Security of Electronic Information

The University strives to maximize the confidentiality and security of its information systems and services within the limitations of available resources. As with paper-based systems, no technology can be guaranteed to be 100% secure. All users should be aware of this fact and should not have an expectation of total privacy regarding information that is created, stored, sent or received on any networked system. The most important first line of defense in information security is the password, and it is for that reason that the University username and password must be adamantly protected as described above. And institutional custodians of private information should exercise prudence, using secure technologies when appropriate and feasible.

The Internet environment offers tremendous opportunities to provide convenient access to University information and services to authorized individuals wherever they may be. Users who serve as custodians of institutional information should be particularly aware of the potential for unauthorized access to or tampering with on-line information and services in the Internet environment. Techniques such as the use of encryption, secure web servers or restricting access based on specific criteria may be appropriate based on the balance between access and security applicable to any specific application or service. Technology administrators are responsible to provide reasonable measures of protection of the underlying technology systems and infrastructure they manage. But risk assessment and risk management strategies are the responsibility of the functional custodians of specific information and services, in consultation with technology managers who should describe the specific technical safeguards in place.

V. Ownership and Disclosure of Information

The University owns the computers and networks that comprise the institutional information technology infrastructure. The electronic allocation of file space to a user does not assign legal ownership of the content. Rather, it is the granting of permission to use these institutional facilities subject to the policies and regulations of the University and applicable statutes. Collective bargaining agreements and related University policies govern ownership of intellectual property.

Files stored on University systems may be subject to disclosure under the U.S. Freedom of Information Act or the Hawai‘i Uniform Information Practices Act. In addition, it is the policy of the University to cooperate with all legally empowered investigations initiated by law enforcement agencies when presented with a legitimate court order such as a warrant or subpoena. As has been made abundantly clear in highly publicized legal cases, this may include archives of electronic mail sent or received. In addition, the contents of files on University systems may be inspected in the context of a duly authorized University investigation.

Users should be aware that most institutional systems are backed up on a routine basis to ensure the ability to recover from computer or network failures or disturbances. Backup procedures are generally not designed or intended for long-term storage of files. However, all users should be aware that files or email messages that they have deleted may still persist on backups and may therefore be subject to disclosure in a duly authorized investigation.

VI. Privacy of Student Information

University computing, information and network resources must be used in a manner consistent with appropriate rules and laws governing the individual privacy of students. This includes the Family Educational Rights and Privacy Act (FERPA) (codified in 20 U.S.C., section 1231g) as amended; Hawai‘i Revised Statutes, Chapter 708-891, 892 and 893; Chapter 20-20, Hawai‘i Administrative Rules, entitled "Protection of Educational Rights and Privacy of Students;" and UH Administrative Procedure A7.022.

VII. Commitment to Access

The University of Hawai‘i is firmly committed to compliance with the Americans with Disabilities Act of 1990 (ADA), which prohibits discrimination on the basis of disability in employment or in the provision of educational services. Technology may be either a barrier or a tool for compliance, depending on how it is used. All units of the University are responsible for ensuring that services they provide via technology be accessible, just as for their on-campus programs and services. If unsure of their obligations, administrators are advised to consult with their Equal Employment Opportunity officer for guidance on compliance with the ADA or other related mandates.

VIII. Special Responsibilities of System and Network Administrators

Administrators of information technology bear a heavy responsibility to maximize the availability and utility of the systems they manage while at the same time honoring individual users’ justifiable expectations of an information and communications environment that is “safe” for its users. In addition to having all the responsibilities of any other user as described above, system administrators are granted certain system privileges which make it possible for them to manage the technical resources under their control. System privileges may permit access to initial passwords, files, voice mail, telephone or electronic communication, and information about individual usage patterns. These privileges are necessary for doing their jobs, but have tremendous potential for abuse as well. Such abuse is a violation of University policy and this section outlines the unique responsibilities and obligations of system and network administrators.

These special responsibilities accompany the granting of any network or system privileges to any member of the University community, whether faculty, student or staff. System administrators to whom this applies include individuals who administer departmental, college or institutional servers; individuals who administer network devices such as modems and routers; individuals responsible for telephone services; and individuals who have any level of privileged access to institutional information systems. Under no circumstances will abuse of system privileges be tolerated and violations will be considered as legitimate cause for disciplinary action up to and including termination and/or legal prosecution. Individuals who are not willing to accept these responsibilities should not be in positions which require system privileges in order to perform their duties.

In addition, individual systems and servers can be carelessly mismanaged not only to the detriment of the users of that system or service but to the detriment of the entire institution. Before making the decision to install a server, the responsible administrator should be prepared to commit the time and resources necessary to ensure proper management. This includes designation of a professional system administrator who will have the time and expertise to understand the technical implications of their systems, maintain current on vulnerabilities, software patches and new releases, and be able to address urgent issues on an immediate basis. Failure to do so may endanger not only the integrity of services provided to one’s own users but to the institution as a whole. The University will not hesitate to disconnect improperly managed systems that endanger the integrity of institutional networks, systems or services and it will be the sole responsibility of the unit’s system administrator or its management to remedy the situation.

While the following list is not considered to be all-inclusive, it establishes the framework for unacceptable behaviors. University management has the responsibility to ensure that system administrators within their units address these matters and should not permit the establishment of servers and services within their units unless they understand the potential for abuse and accept responsibility for compliance. And users should be welcomed to discuss any or all of these matters with their system administrators. All perceived violations of these guidelines should be reported to the appropriate dean, director, provost or vice-president.

A. *System administrators shall protect individual passwords*

Users have the right to expect that their passwords be treated with complete confidentiality. Passwords should never be divulged to a third party except as necessary in the course of distributing a new password to a user. System administrators should take the utmost care in how passwords are distributed, striving for the best possible balance between a user's needs for privacy and convenience. Any time a password is transmitted to a user the user should be advised to change their password immediately to protect against any possible disclosure during the transmission.

B. *System administrators shall not browse, inspect or copy users' information*

System administrators may not browse the contents of user files or messages -- whether on-line or from backups -- without the user's permission. Inspection of information is permitted only upon specific authorization from a dean, director, provost, vice-president or legal authorities as part of a duly authorized investigation or for official University business. As a matter of professionalism, system administrators should avoid direct or indirect contact with users' information and communication content whenever possible. In spite of their best efforts system administrators may from time-to-time encounter confidential information in the performance of their duties. Under no circumstances should such information be acted upon, divulged, or used for the personal benefit or profit of anyone. Violations of this trust endanger the viability of the institutional information infrastructure and will not be permitted. . However, system administrators may perform routine scans and are encouraged to utilize standard security tools to check for potentially damaging or illegal software on institutional systems.

C. *System and network administrators shall not routinely collect information on individuals' information usage patterns*

The University expects that the members of its community will access a rich variety of information and communication resources in the course of their academic activities. System administrators shall not monitor or collect data regarding the activities of individuals unless specifically authorized to do in the context of a duly authorized investigation. This is not intended to interfere with the responsibility of system administrators to collect and analyze general anonymous information about the overall patterns of usage of information technology resources. Such information is a vital tool in ensuring the adequacy of the institutional technology environment to meet the needs of its users. Nor are system administrators obliged to spend undue efforts disabling the routine logging activities that are built into many server operating systems.

D. *System administrators shall configure software systems so as to maximize the confidentiality of user communication*

Administrators of email servers in particular bear a responsibility to respect the privacy of their users' communication. Email systems should be configured so as to maximize privacy. For example, email that is rejected for technical reasons should be returned to the sender rather than to the "postmaster." And routine error notification messages to the postmaster should contain only message headers, not the message contents. Users are encouraged to ask their email administrator how email systems are configured and under what circumstance their email may be disclosed.

E. *System administrators shall configure systems to enforce appropriate password policies*

Most server operating systems have configurable options for password security. UH system administrators should use these options to comply with the UH password policy in Appendix C. In addition, system administrators should ensure that all activities relating to security changes are handled in accord with a written policy and are documented. E.g., system privileges should not be given to individuals who do not need them to perform their job, and the granting of such privileges should be documented. Procedures should be in place for emergency access to critical passwords needed in case of system failure when the usual system administrator(s) may not be available. The level of formality and detail of the security policy and practices may be dependent on the role and importance of specific systems and services.

F. *System administrators shall stay abreast of any vulnerabilities of their systems and manage security in accord with appropriate recommendations*

System administrators are responsible for remaining up-to-date at all times with security issues relevant to the systems they administer. This may be done through means such as their vendors' information channels or Computer Emergency Response Team (CERT) bulletins. System administrators are required to use this information to apply all recommended security patches in a timely manner.

G. *System administrators should configure their systems to minimize the chance for abuse, and act promptly to end abuses upon notification*

Certain kinds of disruptions rely on the naiveté of system administrators on the Internet. Any perception that the University of Hawai'i is a haven for such abusers endangers the ability of the University community to communicate with others. For example, external sites that have been attacked by someone using a University of Hawai'i system as the instrument of the attack may find that they can only safeguard themselves by blocking all traffic from the University of Hawai'i. As just two examples of the kinds of measures that should be taken, email administrators should block anonymous email relays through their systems and network administrators should block the forging of IP source addresses from within networks they manage. As noted above, the University will not hesitate to disconnect improperly managed systems that endanger the integrity of institutional networks, systems or services and it will be the sole responsibility of the unit's system administrator or its management to remedy the situation.

H. *System administrators shall publicize backup policy*

As noted above, backups present a means by which information may be recovered that users believe to have been deleted. Backup policies determine the persistence of deleted information and therefore users have a right to know the backup policy of all systems they use. System administrators should post this policy or make it easily available to their users upon request.

IX. Due Process

All alleged violations of this policy shall be processed according to the principles of due process, for example, allegations should always be investigated by a party other than the accuser. It is the policy of the University to avoid creating unnecessary enforcement mechanisms for technology that are different than for other media. Therefore, the authority that would be responsible for comparable infractions shall also be responsible for enforcing violations that take place via technology. E.g., if sexual harassment occurs via technology, responsibility for enforcement shall reside with the same authority that would handle any other sexual harassment allegation.

In general, when an alleged violation of this policy by a user is encountered, the responsible staff or system administrator shall first notify the user. The user will be expected to take immediate remedial action or respond by indicating that they do not believe they have violated the policy. Depending on the seriousness of the alleged violation, or should the violation persist after notification to the user, further investigation and consequent enforcement action may be initiated.

Allegations of violation of statute or conduct codes will be filed with appropriate internal or external authorities, typically the Dean of Students, Senior Vice President, or legal authorities. If the allegation relates to personal harassment the system administrator should direct the complainant to file their allegation with the responsible authority. System administrators will cooperate fully in duly authorized investigations and should attempt to provide assistance to aggrieved parties. But system administrators are not obligated to file personal complaints on behalf of aggrieved parties since that decision belongs with the complainant.

In cases where the alleged violation relates to endangering the availability or performance of the technology infrastructure (e.g. a denial-of-service attack), authority for investigation and action up to and including suspension of access to University technology resources may be delegated to the senior manager responsible for the impacted technology. Inspection of user files necessary to the investigation should be approved in advance by a dean, director, provost or vice-president. If access to University technology is suspended as a result of the investigation, the alleged violator may appeal their suspension to the appropriate provost, dean or director. Such violations may also be referred to appropriate internal or external authorities or for prosecution as a criminal offense or violation of other code of conduct.

Allegations of misconduct by system administrators should be filed with the responsible dean, director, provost or vice president, who shall be responsible for investigating the situation by drawing on expertise outside the unit as needed.

Regardless of its commitment to due process, the University reserves the right to summarily suspend access to facilities and services or take emergency actions as necessary to protect the safety, integrity and performance of its institutional systems and services. Such actions may be necessary due to inadvertent errors or problems unrelated to misconduct by any individual, but system administrators must be able to take certain actions in times of crisis to preserve and protect the overall services provided to the University community.

Appendix A (Updated September 2001)

Hawai‘i Computer Crime Statute
(Hawai‘i Revised Statutes)

COMPUTER CRIME

§708- Computer fraud in the first degree.

(1) A person commits the offense of computer fraud in the first degree if the person knowingly, and with intent to defraud, accesses a computer without authorization and, by means of such conduct, obtains or exerts control over the property of another.

(2) In a prosecution for computer fraud in the first degree, it is a defense that the object of the fraud and the property obtained consists only of the use of the computer and the value of such use is not more than $300 in any one-year period.

(3) Computer fraud in the first degree is a class B felony.

§708- Computer fraud in the second degree.

(1) A person commits the offense of computer fraud in the second degree if the person knowingly, and with the intent to defraud, transfers, or otherwise disposes of, to another, or obtains control of, with the intent to transfer or dispose of, any password or similar information through which a computer, computer system, or computer network may be accessed.

(2) Computer fraud in the second degree is a class C felony.

§708- Computer damage in the first degree.

(1) A person commits the offense of computer damage in the first degree if:

(a) The person knowingly causes the transmission of a program, information, code, or command, and thereby knowingly causes unauthorized damage to a computer, computer system, or computer network; or

(b) The person intentionally accesses a computer, computer system, or computer network without authorization and thereby knowingly causes damage.

(2) As used in this section, the "damage" must:

(a) Result in a loss aggregating at least $5,000 in value, including the costs associated with diagnosis, repair, replacement, or remediation, during any one-year period to one or more individuals;

(b) Result in the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals;

(c) Result in physical injury to any person;

(d) Threaten public health or safety; or

(e) Impair the administration of justice.

(3) Computer damage in the first degree is a class B felony.

§708- Computer damage in the second degree.

(1) A person commits the offense of computer damage in the second degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby recklessly causes damage.

(2) Computer damage in the second degree is a class C felony.

§708- Use of a computer in the commission of a separate crime.

(1) A person commits the offense of use of a computer in the commission of a separate crime if the person knowingly uses a computer to identify, select, solicit, persuade, coerce, entice, induce, or procure the victim or intended victim of the following offenses:

(a) Section 707-726, relating to custodial interference in the first degree;

(b) Section 707-727, relating to custodial interference in the second degree;

(c) Section 707-731, relating to sexual assault in the second degree;

(d) Section 707-732, relating to sexual assault in the third degree;

(e) Section 707-733, relating to sexual assault in the fourth degree;

(f) Section 707-751, relating to promoting child abuse in the second degree; and

(g) Section 712-1215, relating to promoting pornography for minors.

(2) Use of a computer in the commission of a separate crime is an offense one class or grade, as the case may be, greater than the offense facilitated. Notwithstanding any other law to the contrary, a conviction under this section shall not merge with a conviction for the separate crime.

§708- Forfeiture of property used in computer crimes.

Any property used or intended for use in the commission of, attempt to commit, or conspiracy to commit an offense under this part, or which facilitated or assisted such activity, shall be forfeited subject to the requirements of chapter 712A.

§708- Jurisdiction.

For purposes of prosecution under this part, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

§708- Unauthorized computer access in the first degree.

(1) A person commits the offense of unauthorized computer access in the first degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information, and:

(a) The offense was committed for the purpose of commercial or private financial gain;

(b) The offense was committed in furtherance of any other crime;

(c) The value of the information obtained exceeds $5,000; or

(d) The information has been determined by statute or rule of court to require protection against unauthorized disclosure.

(2) Unauthorized computer access in the first degree is a class B felony.

§708- Unauthorized computer access in the second degree.

(1) A person commits the offense of unauthorized computer access in the second degree if the person knowingly accesses a computer, computer system, or computer network without authorization and thereby obtains information.

(2) Unauthorized computer access in the second degree is a class C felony.

§708- Unauthorized computer access in the third degree.

(1) A person commits the offense of unauthorized computer access in the third degree if the person knowingly accesses a computer, computer system, or computer network without authorization.

(2) Unauthorized computer access in the third degree is a misdemeanor."

§708-890 Definitions. As used in this part, unless the context otherwise requires:

"Access" means to gain entry to, instruct, communicate with, store data in, reprieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

"Computer" means any electronic, magnetic, optical, electrochemical, or other high-speed data processing device performing logical, arithmetic, or storage functions, and includes all computer equipment connected or related to such a device in a computer system or computer network, but shall not include an automated typewriter or typesetter, a portable hand-held calculator, or other similar device.

"Computer equipment" means any equipment or devices, including all input, output, processing, storage, software, or communications facilities, intended to interface with the computer.

"Computer network" means two or more computers or computer systems, interconnected by communication lines, including microwave, electronic, or any other form of communication.

"Computer program" or "software" means a set of computer-readable instructions or statements and related data that, when executed by a computer system, causes the computer system or the computer network to which it is connected to perform computer services.

"Computer services" includes but is not limited to the use of a computer system, computer network, computer program, data prepared for computer use, and data contained within a computer system or computer network.

"Computer system" means a set of interconnected computer equipment intended to operate as a cohesive system.

"Damage" means any impairment to the integrity or availability of data, a program, a system, a network, or computer services.

"Data" means information, facts, concepts, software, or instructions prepared for use in a computer, computer system, or computer network.

"Obtain information" includes but is not limited to mere observation of the data.

"Property" includes financial instruments, data, computer software, computer programs, documents associated with computer systems, money, computer services, or anything else of value.

"Rule of court" means any rule adopted by the supreme court of this State, the Federal Rules of Civil Procedure, or the Federal Rules of Criminal Procedure.

"Statute" means any statute of this State or the federal government.

"Without authorization" means without the permission of or in excess of the permission of an owner, lessor, or rightful user or someone licensed or privileged by an owner, lessor, or rightful user to grant the permission."

Appendix B

Hawai‘i State Ethics Code
(Hawai‘i Revised Statutes)

Section 84-13(3) of the Hawaii State Ethics Code, chapter 84 of the Hawai‘i Revised Statutes prohibits the use of state time, equipment or other facilities for private business purposes:

> **§84-13 Fair treatment**. No legislator or employee shall use or attempt to use the legislator’s or employee’s official position to secure or grant unwarranted privileges, exemptions, advantages, contracts, or treatment for oneself or others; including but not limited to the following:
>
> …
>
> (3) Using state time, equipment or other facilities for private business purposes.

Appendix C

Guide to Password Selection and Management

Passwords should be changed regularly -- experts suggest the **maximum** use of a password for between three and six months. Systems that allow password expiration should be set within this range. Furthermore, users are advised to change the initial password on a new account immediately, since in most cases, once a password is changed, even system administrators will have no way of knowing a well-chosen password.

Passwords should never be reused. Systems that can prohibit reuse of old passwords in the new password selection process should be configured to do so, keeping a history of a minimum of seven old passwords to be disallowed.

User accounts should be deactivated when multiple unsuccessful attempts are made to enter the password. This is often a sign that an unauthorized user is attempting to break in. Experts recommend between three and five maximum attempts, and systems that permit locking accounts based on unsuccessful tries should be configured accordingly, based on the sensitivity of the system. When a user account is locked, the authorized user generally has to call the system administrator to have a new password set.

Passwords should be selected that are difficult to guess. Passwords should not be middle names, phone numbers, pet names or variations on the username (login name). In addition, passwords should not be any word that is found in a dictionary, forward or backwards, as dictionary searches can be automated. Passwords should be at least six characters in length and contain a mix of upper and lower case alphabetic with non-alphabetic characters (numerals or punctuation).

A good way to build a password is to use a phrase that you can easily remember, using numbers and symbols. For example, "One is the loneliest number by Harry Nilsson" can be used to build the password 1itl#bHN. Or “sixteen ounces per pound” could be 16Oz/#.

Appendix D

EDUCOM Code
Software and Intellectual Rights

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, the right to privacy, and the right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

Note: The EDUCOM Code, a statement of principle about intellectual property and the legal and ethical use of software, was developed by the EDUCOM Software Initiative and intended for adaptation and use by individuals, colleges and universities.

Source: EDUCOM Review, EDUCOM, Washington, DC, Vol. 26, Number 1, spring 1991, page 13.