Executive Policy Chapter 2, Administration
Executive Policy EP2.210 Use and Management of Information Technology Resources
Effective Date: January 2018
Prior Dates Amended: October 1999, October 2014
Responsible Office: Office of the Vice President for Information Technology/Chief Information Officer
Governing Board of Regents Policy: RP 2.202 Duties of the President
Review Date: August 2020

I. Purpose

A. To establish the basis for university-wide policies and procedures for the acceptable use and management of all University of Hawai'i ("UH" or "University") information technology resources. UH information technology resources shall include equipment, infrastructure and systems owned or operated by UH, for use by its community (ref. III.B., Executive Policy, Context).

B. To define and provide effective protection, equal access, and administrative guidelines for the use of those resources.

C. To supplement existing laws, regulations, general codes of conduct, agreements, and contracts that are currently in place.

II. Definitions:

A. Accessibility or Accessible

An Individual with Disabilities is afforded the opportunity to acquire the same information, engage in the same interactions, and enjoy the same services, programs, and activities as an individual without disability in an equally effective, timely and independent manner with substantially equivalent ease of use. A person with a disability must be able to obtain the information as fully, equally, and independently as a person without a disability. Although this might not result in identical ease of use compared to that of persons without disabilities, it still must ensure equal opportunity to the educational benefits and opportunities afforded by the technology and equal treatment in the use of such technology.

B. Electronic Communications Privacy Act of 1986 ("ECPA")

The ECPA, as amended, protects wire, oral, and electronic communications while communications are being made, are in transit, and when they are stored on computers.

C. Family Educational Rights and Privacy Act ("FERPA")

The FERPA, as amended, protects the privacy of student educational records.

D. Individuals with Disabilities

Individuals who have a physical or mental impairment that substantially limits one or more major life activities, have a record of such impairment, or are regarded as having such impairment.

E. Reasonable and Appropriate Accommodations

Facilities modifications and/or service adjustments determined by the Deans, and Directors, in consultation with the students and employees with disabilities, Information Technology Services (“ITS”) staff, Disabilities Services Office, or other appropriate resources. Assistive technology and assistance with ITS facilities and computers are examples of reasonable and appropriate accommodations.

III. Executive Policy

A. 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

B. Context

This document is the basis for university-wide policies and practices for the acceptable use and management of all University of Hawai‘i (“UH” or “University”) information technology resources. It is intended to define and provide effective protection, equal 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 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 discrimination 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, developed, procured, or administered by the University, as well as to individual activities that take place over the Internet or other external network connections using University systems, connections or user accounts, in conducting University business.

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, 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 Hawai‘i’s penal code is included herein as Appendix A and portions of the State Ethics Code are included as Appendix B.

C. Responsible Use

1. Privileges and Responsibilities

The University 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.

2. 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. Unauthorized use of someone else's password is strictly prohibited, and may constitute violation of law and well as standards of conduct.

      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 1986, as amended, which protects the confidentiality of personal electronic communications or the Hawai‘i 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 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, Pub. L. No. 105-304, 112 Stat. 2860 (1998), as amended, notifications of claimed infringement using University of Hawaii services should be filed with:
Information Technology Services
University of Hawai'i
2520 Correa Road
Honolulu, HI 96822
Tel: 808-956-3501
Fax: 808-956-7322
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 strictly prohibits the use of its information technology resources for downloading pornography or other such

illegal conduct. 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.

D. 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.

E. 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.

F. 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.

G. Commitment to Access

The University is committed to a policy of equal opportunity and nondiscrimination on the basis of disability status. Therefore, these policies and procedures ensure that Individuals with Disabilities, will not, on the basis of those disabilities, be denied equal access to the University’s programs, services, and activities. All University units are responsible for ensuring that the services, programs and activities they provide via information technology resources and digital media are as accessible, effective, and timely to Individuals with Disabilities as they are to people without disabilities. Each individual or unit responsible for web content must be aware of this Policy and know how to provide accessible content. Those responsible must also monitor and evaluate the content regularly for accessibility.

The University is committed to ensuring equal opportunity for Individuals with Disabilities in accordance with the Americans with Disabilities Act of 1990 (“ADA”), as amended by the ADA Amendments Act of 2008, and Section 504 of the Rehabilitation Act of 1973, which prohibits discrimination on the basis of disability in employment or in the provision of educational services as well as the Higher Education Opportunity Act.

This policy applies to all information technology and digital media that is created, purchased, used, and implemented by or for any University units and used to carry out any University programs, services and/or activities through websites or web-based applications, software, hardware, and electronic documents, except when an exception has been granted. In addition, this Policy applies to all information technology resources and digital media used to conduct university business, except information technology resources created or published by students, faculty, or staff for personal use.

All web content should be in compliance with Section 508 Standards and should also meet the Web Content Accessibility Guidelines (WCAG) 2.0 Level AA. Additional standards for other information technology resources may be identified over time and added to this Policy. If an Individual with Disabilities finds the content on any University website inaccessible, they may email itsada@hawaii.edu or call the ITS Help Desk at (808) 956-8883 for assistance.

Priority for implementation of this policy and standards should be given to programs, services, and activities that are either highly critical or are broadly used by the campus, a school, or a college, taking into account feasibility, funding, technical capacity, and needs of staff training.

Conformance to standards may not always be feasible where compliance is not technically possible, is unreasonably expensive or difficult in, or requires fundamental alteration of services, and programs that it may require extraordinary measures due to the nature of the information technology resources or the intent of the web page. Undue financial and/or administrative burden or non-availability may qualify as an exception from this Policy. It is an institutional decision to be made by the Deans and Directors after consultation with the Vice President for Information Technology and Chief Information Officer, the affected unit and others with relevant perspectives or expertise.

However, these difficulties do not relieve University programs, services, and activities from their accessibility and equal access obligations. After consultation with the Vice President for Information Technology and Chief Information Officer, Deans and Directors must be prepared to provide content, services, programs, and/or activity in equally effective alternative format and/or access upon request.

Rights and Responsibilities

1. Information Technology Services (“ITS”)

   ITS recognizes the responsibility to identify and maintain the academic and technical standards that are fundamental to providing quality resources while ensuring the rights of persons with disabilities. To meet this obligation, ITS:

   a. Has the responsibility to ensure that all of its resources, viewed in their entirety, are accessible;
   b. Has the right to select among equally effective methods of accommodating Individuals with Disabilities;
   c. Has the right to refer Individuals with Disabilities to the appropriate agency with requests for accommodations that exceed those currently possible at ITS;
   d. Has the right to deny a request for services for Individuals with Disabilities. If a request is denied, ITS has the responsibility to inform the individual of the reasons for the denial.

2. Individuals with Disabilities

   Individuals with Disabilities have the right to an equal opportunity to use and benefit from the resources that ITS has to offer. To ensure this right, Individuals with Disabilities:

   a. Have the responsibility to identify themselves as needing appropriate, reasonable accommodations;
   b. Have the responsibility for making their needs known in a timely manner;
   c. Have the same obligation as any other UH faculty, staff, or student to comply with University policy and procedures;

d. Have the responsibility to follow standard UH policies and procedures;
e. Have the right to confidentiality of all information regarding their disability. Individuals with Disabilities have the right to choose to who information about their disability will be disclosed.

In addition to the provisions contained herein, separate guidelines shall be established concerning accessible technology and digital media and procurement of information technology goods and services.

H. 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.

1. 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.

2. 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.

3. 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.

4. 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.

5. System administrators shall configure systems to enforce appropriate password policies

   Most server operating systems have configurable options for password security. 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.

6. 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.

7. 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 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 system as the instrument of the attack may find that they can only safeguard themselves by blocking all traffic from the University. 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.

8. 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.

I. 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, 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, Chancellor 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 Chancellor, Dean, Director or Vice President. 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, Chancellor or Vice President, who shall be responsible for investigating the situation by drawing on expertise outside the unit as needed.

Any and all discipline or appropriate disciplinary actions will be imposed in accordance with the applicable collective bargaining agreements. For all included employees covered by collective bargaining, appeals of disciplinary actions shall be filed in accordance with the applicable collective bargaining agreement.

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.

IV. Delegation of Authority

Vice Presidents, Chancellors, Deans and Directors are hereby directed with the authority to implement this Policy. The Vice President for Information Technology and Chief Information Officer is responsible for issuing and updating any requirements, standards or guidelines that support this Policy and shall facilitate the regular communication with campuses, colleges, departments, and units to address consistent implementation of this Policy throughout the University system. For individual or unit responsible for web content, help on this Policy can be found on the Information Technology Accessibility website (www.hawaii.edu/access) or by utilizing the additional contact information listed below.

V. Contact Information

Office of the Vice President for Information Technology and Chief Information Officer
808-956-3501
gyoshimi@hawaii.edu

https://www.hawaii.edu/its/

The EEO Officer and ADA Coordinator for each campus are responsible for overseeing compliance with regard to state and federal regulations that prohibit discrimination on the basis of disability and require reasonable accommodation. Questions or concerns regarding complaints of discrimination and reasonable accommodation, should be directed to the appropriate EEO Officer and/or ADA Coordinator. For advice on student auxiliary aids and services should be directed to the student disability services office at each campus.

VI. References

- Link to superseded Executive Policy EP 2.210 in old format

  https://www.hawaii.edu/policy/archives/ep/e2/e2210.pdf

- Link to Executive Policy EP 1.202 – University Statement of Nondiscrimination and Affirmative Action

  https://www.hawaii.edu/policy/docs/temp/ep1.202.pdf

- List associated executive policies and administrative procedures
  - Hawai‘i Computer Crime Statute (Hawai‘i Revised Statutes)
  - Hawai‘i State Ethics Code (Hawai‘i Revised Statutes)
  - EDUCOM Code Software and Intellectual Rights

Approved:

Signed _____ January 10, 2018
David Lassner Date
President