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

: Dengage 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

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

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 excus [(ac)4 (c)61rsonaer(()]TJ 0 Tp(ons)4 ( )e6 (ni)(i)6 (nt)1orutu ph(ubj)6 ()2 (eda (

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

Conformance to standards may not always be feasible where compliance is not technically possible,

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

the Univ

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 Las Tc -0.004a6 (i‘)]TDT 40( )]TJ ET 36]TJ 7g 0.004 Tfue Eti)