



- Home
- Report Issues or Incidents
- About the UH Information Security Program

Policies & Compliance

HIPAA

UH Information Security Awareness Training

Spearphishing

Information Security for

Students

Research

Faculty & Staff

System Administrators & Developers

Technical Guidelines

Awareness Resources

SEAR the Phish

Mobile Device Security

Data Privacy Day

National Cyber Security Awareness Month

Security

Policies & Compliance

These University of Hawai'i policies, State of Hawai'i Revised Statutes, and external regulations all have information security implications. Anyone accessing University of Hawai'i resources, including data, computer, and network resources, is responsible for ensuring compliance with all applicable policies and regulations.

UH Policies related to Information Security

Policy/Law	Title	How it Applies to UH
EP 2.210	Use and Management of Information Technology Resources Policy	Describes the appropriate use of UH information technology resources which applies to students, faculty, staff, and authorized guest users.
(Recently Updated) EP 2.214	Institutional Data Classification Categories and Information Security Guidelines	The objective of this executive policy is to organize UH Institutional Data into data classification categories based on different levels of security risk and penalties that may result from the inadvertent exposure and inappropriate disclosure of those data.
(Recently Updated) EP 2.215	UH Institutional Data Governance Policy UH Data Governance web site	Establishes system-wide standards to protect the privacy and security of data and information under the stewardship of the University.
EP 2.217	UH HIPAA Policy	To ensure that UH complies with the Health Insurance Portability and Accountability Act
EP 2.218	Online Approvals of Internal University Transactions	Describes institutional requirements regarding the use of online approvals and signatures
EP 7.208	Systemwide Student Conduct Code	Describes the rules and regulations that UH students must comply with.
(New)	Mandatory Training and	To describe the mandatory

Resources

University Security Resources

Security Tips

External Resources

Contact

Frequently Asked Questions

Contact Us

AP 2.215	Continued Education Requirements for Data Users	training and continuing education requirements for UH employees, students, and affiliates who are considered Data Users
AP 7.022	Procedures Relating to Protection of the Educational Rights and Privacy of Students	Establishes procedures governing a UH student's access to their own education records and access to education records by the public and other governmental agencies.
AP 8.710	Credit Card Program	Procedures for processing credit card transactions in accordance with University policies, banking and payment card industry requirements, etc.
AP 8.711	Electronic Payments via University Websites	Policies and procedures for processing electronic payments in accordance with University policies, banking and payment card industry requirements, etc.
AP 8.450	Records Management Guidelines and Procedures	Provides guidelines and instructions for the retention, scheduling, storage, microfilming, transfer, and disposition of University records.

Hawai'i Revised Statutes

Policy/Law	Title	How it Applies to UH
HRS 92F	Uniform Information Practices Act (UIPA)	Requires the University to open government records for public inspection except Social Security numbers, personal records, etc.
HRS 487J	Social Security Number Protection	Requires the University to protect an individual's Social Security number.
HRS 487N	Security Breach of Personal Information	Requires the University to provide notice if there has been a security breach of personal information.
HRS 487R	Destruction of Personal Information Records	Requires the University to securely dispose of personal information.

External Standards and Regulations

Policy/Law	Title	How it Applies to UH
HIPAA	Health Insurance Portability and Accountability Act	Regulates the use, disclosure, and protection of individuals'

	UH HIPAA web site	health information.
FERPA	Family Educational Rights and Privacy Act	Requires the University to provide students with access to their education records, an opportunity to have the records amended, and some control over its disclosure.
FISMA	Federal Information Security Management Act	Requires federal agencies to implement an information security for information/information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor (e.g. UH), or other source.
GLBA	Gramm-Leach-Bliley Act ("Safeguards Rule")	Regulates how non-public personal information is to be protected.
FACTA	Fair and Accurate Credit Transactions Act ("Red Flags Rule")	Requires an identity theft prevention program to identify and detect red flags and to prevent and mitigate identity theft.
PCI DSS	Payment Card Industry Data Security Standards	Requires the University to implement security controls around cardholder data to reduce credit card fraud.
DMCA	Digital Millennium Copyright Act ("OCILLA")	Requires the University to take action on copyright infringement that originates on the network.

^
BACK TO TOP

MAILING ADDRESS

Information Technology Services
2520 Correa Road
Honolulu, HI 96822

STUDENT EMPLOYMENT

Information Technology Services posts available positions for UH students on [SECE](#)

UH SYSTEM HOME



[HOME](#) [ABOUT](#) [NEWS](#) [CONTACT](#)

Use of this site implies consent with our [Usage Policy](#) | The University of Hawai'i is an Equal Opportunity/Affirmative Action Institution
© 2015 Information Technology Services | All Rights Reserved | University of Hawai'i System