UNIVERSITY of HAWAI'I®

UH Systemwide Policies and Procedures Information System (PPIS)

Search PPIS Go

UH System Policies and Procedures
Board of Regents Policies
Executive Policies
+ 1. General Provisions
+ 2. Administration
+ 3. Organization
+ 4. Planning
+ 5. Academic Affairs
+ 6. Tuition, Financial Assistance, and Fees
+ 7. Student Affairs
+ 8. Business and Finance
+ 9. Personnel
+ 10. Land and Physical Facilities
+ 11. Miscellaneous
+ 12. Research
Abolished Policies (Post Oct. 2014)
Archived EP

Administrative Procedures

Creation, Maintenance and Abolishment
Frequently Asked Questions

UH-Related Laws and Rules
Hawai'i Revised Statutes (HRS) 304A
Hawai'i Administrative Rules (HAR) Title 20

UH System Offices

Public Safety and Emergency Management Plans

Login

Executive Policy 2.214

Title

Institutional Data Classification Categories and Information Security Guidelines

Header

Executive Policy Chapter 2, Administration
Executive Policy EP 2.214, Institutional Data Classification Categories and Information Security Guidelines
Effective Date: January 2018
Dates Amended: April 2012, April 2009, October 2014
Responsible Offices: Office of the Vice President for Academic Planning and Policy and 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: January 2021

I. Purpose

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.

II. Definitions

A. Institutional Data – Data elements/data records which are created, received, maintained and/or transmitted by the University of Hawai‘i in the course of meeting its administrative and academic requirements.

B. Personally Identifiable Information (PII) – Data or information, or a combination of data or information that when considered together, would identify an individual. The level of security risk when managing PII varies from none to very high, depending on the data elements involved.

C. Physically Secured – The storage of electronic media or paper containing Institutional Data in a non-public, controlled area such as an area accessible only to a trusted, known group of individuals or in a locked room or file cabinet when there is no authorized individual present. Classrooms and lab areas are considered public locations.

D. Protected Data – Institutional Data that are subject to security and privacy considerations that range from moderate to very high. In other words, all Institutional Data that are not considered public. Within the UH Institutional Data Classification Categories, protected data encompasses those that fall under the “restricted,” “sensitive,” and “regulated” categories. See section III-B for category descriptions.

Selected data elements/data records that fall under the sensitive or regulated categories may be subject to federal, state, and local regulations or industry standards such as
1. Family Educational Rights and Privacy Act (FERPA)
2. Higher Education Act (HEA)
3. Health Insurance Portability and Accountability Act (HIPAA)
4. Hawai‘i Revised Statutes, Chapter 487N – Security Breach of Personal Information
5. Chapter 92F – Uniform Information Practices Act
6. PCI-DSS (Payment Card Industry Data Security Standard)
7. NIST SP 800-171 (National Institute of Standards and Technology Special Programs)
8. National Industrial Security Program (NISPOM)
9. Bioterrorism Special Agent Program

This policy is not intended to supersede those regulations, but to promote and reinforce them. Should a provision in this policy conflict with applicable state, federal, or local regulations, the applicable regulation takes precedence and will govern.

III. Executive Policy

A. POLICY STATEMENT
The University of Hawai‘i is committed to protecting the privacy and security of Institutional Data, one of its most valuable institutional assets.

B. DATA CLASSIFICATION CATEGORIES
1. Public – Institutional Data where access is not restricted and is subject to open records requests.
This category includes: 1) student directory information as defined in UH’s Administrative Procedure, AP7.022, Procedures Relating to Protection of the Educational Rights and Privacy of Students; and, 2) public employee information as defined in Hawai‘i Revised Statues (HRS) 92F-12 under the Uniform Information Practices Act. See Attachment 1 for examples.
2. Restricted – Institutional Data used for UH business only. Restricted data will not be distributed to external parties except under the terms of a written memorandum of agreement or contract. Data is maintained in a physically secured location. See Attachment 1 for examples.
3. Sensitive – Institutional Data subject to privacy or security considerations or any Institutional Data not designated as public, restricted, or regulated. Data is maintained in a physically secured location. See Attachment 1 for examples.
4. Regulated – Institutional Data where inadvertent disclosure or inappropriate access requires a breach notification in accordance with HRS §487N or is subject to financial fines. Social Security Number (SSN) and personal financial information fall within this category. Data is maintained in a physically secured location. See Attachment 1 for examples. A UH administrative procedure on breach notification procedures is forthcoming.

Attachment 1 is not intended to be an exhaustive list but is an attempt to capture the more common data elements (and, in some cases, types of data) used by the University to conduct its daily business. Institutional Data that are not listed shall be considered sensitive until otherwise determined. For guidance on Institutional Data not listed in Attachment 1, email datagov@hawaii.edu.

C. DATA MANAGEMENT GUIDELINES AND BEST PRACTICES

1. Social Security Number (SSN) will not be used as an identifier in any University information system and its use as an identifier shall be phased out in all existing systems. This includes use of the SSN as an optional identifier in legacy systems, which is similarly prohibited. The SSN may be included as a data element in an information system only where it is required for financial processing (e.g., payroll or student tax reporting) or other uses consistent with federal and state law. For example, the University may require the use of the SSN as part of the essential process of identifying when a person has contact with the university using different names, or to distinguish between individuals who have the same name. In situations such as these, the SSN may be used only as a data element and not as an identifier. The SSN must be purged from all other information systems.
2. Documents or records that contain Institutional Data from multiple classification categories will be managed according to the highest level of classification.
3. Individuals with access to protected data must complete mandatory training and continuing education requirements. Refer to UH Administrative Procedure 2.215 for details.
4. Lists of student directory data (which are categorized as public) shall not be released to third parties except under the terms of a contract or memorandum of agreement. Refer to UH Administrative Procedure AP7.022, Procedures Relating to Protection of the Educational Rights and Privacy of Students which is UH's interpretation of the federal Family Educational Rights and Privacy Act.
5. When displaying protected data in aggregate (i.e., not on an individualized basis), appropriate care must be taken to protect the identities of the individuals such that a person cannot identify any of the individuals with reasonable certainty. Note that data elements may not be personally identifiable when considered alone. However, when considered in combination with other data elements, they may reveal the identity of an individual. For example, average GPA by major may be reported. But if ethnicity is added, and there is only one individual within an ethnicity category, the identity of the individual and his/her GPA may be revealed. Therefore, appropriate consideration and measures must be taken when considering the mix of data elements being shared and the highest level of data classification category involved.
6. Notwithstanding any records retention policies, paper and electronic transaction records containing regulated data, such as SSN or personal financial information, will be redacted or removed/destroyed when considered nonessential.

D. DATA SECURITY MEASURES

1. Technical guidelines for each data classification category shall be followed to prevent the inadvertent exposure and inappropriate disclosure of Institutional Data that are considered protected data. Technical guidelines by type of storage device are available at www.hawaii.edu/infosec/techguidelines. These technical guidelines are part of the UH Information Security Program which is administered by the Information Technology Services Information Security Team.
2. Upon discovery of an inadvertent exposure or inappropriate disclosure of protected data, ITS' security team should be notified immediately. An investigation by the security team may be required to identify the cause(s) of the incident. Additional information on incident handling procedures are available at http://www.hawaii.edu/infosec/notification.
3. As stated in Executive Policy EP2.215, Information Technology Services (ITS) has the full authority to enforce technical measures to ensure the security and confidentiality of protected data that are stored or transmitted, whether intentionally or unintentionally, on University systems and networks, including but not limited to

immediate disconnection of compromised systems and devices from the University network.

4. ITS has the authority to conduct network and device scanning to identify security weaknesses in any University information system, device, or network that may compromise sensitive information or the operations and availability of institutional services.

ITS also has the authority to require all servers operating on the University network be regularly scanned for sensitive information, vulnerabilities and be protected in accordance with appropriate data security guidelines based on data classification categories.

5. To better protect the University's Institutional Data, ITS may require departments/units/programs to periodically report on the data element/records that they manage. Reporting requirements administered by ITS include PII and Health Insurance Portability and Accountability Act (HIPAA) surveys and server registrations.

The PII survey is part of an HRS §487N-7 requirement where UH must annually prepare a report describing the information systems that contain personal information. ITS is responsible for submitting this report and maintains a secure online system for units to report such systems. Chancellors and Vice Presidents are responsible to ensure that units under their purview report systems containing protected data and update the information at least annually.

6. Chancellors and Vice Presidents should also designate an individual in their organization to be responsible for the units personal information protection and compliance program which includes ensuring that the PII survey is completed accurately, the elimination of unnecessary storage of personal information, and for implementing appropriate security measures for systems under their purview. This individual's name, and contact information shall be sent to the UH Chief Information Security Officer. These designated individuals will form the systemwide Data Security Leadership Council.

7. The UH Board of Regents approved a Federal Trade Commission (FTC) Red Flags Rule Identity Theft Prevention Program for UH. The program falls under the FTC's Red Flags Rule, 16 CFR Part 681, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The purpose of the Identity Theft Prevention Program is to detect, prevent and mitigate identity theft in connection with a "covered account" which involves the University extending credit to an individual to obtain goods or services, or accepting a deposit from the individual, and involves multiple payments or transactions. See Attachment II for details.

8. Personnel related actions

a. Terminations

When an employee with access to protected information voluntarily separates from the University, his/her access will be revoked at the time of separation. The appointing authority shall be responsible for initiating the revocation of access.

In the case of an employer-initiated termination of employment of personnel with access to protected information, access may, as circumstances warrant, be revoked immediately at the time of notification, or as soon as may be consistent with an applicable collective bargaining agreement.

b. Violations

In the event of an inadvertent exposure or inappropriate disclosure of protected data, the chancellor or vice president of the affected unit will be informed. Any resulting investigation into the incident will follow University policies and procedures and applicable collective bargaining agreements should any potential misconduct be identified.

c. Personnel Background Checks

Prior to granting an employee access to protected data, an appropriate background check may be performed by the appointing authority in accord with applicable policies and procedures.

IV. Delegation of Authority

There is no policy-specific delegation of authority.

V. Contact Information

Office of the Vice President for Academic Planning and Policy and Office of the Vice President for Information Technology & Chief Information Officer
Sandra Furuto, 956-7487, yano@hawaii.edu

VI. References

Executive Policy EP2.215, Institutional Data Governance, provides the overall structure for the University's data governance program. It describes the fundamental principles and best practices governing the management and use of Institutional Data and stewardship roles and responsibilities. Executive Policy EP2.214 is a supporting policy on data governance and information security.

These and other University of Hawai'i executive policies, State of Hawai'i Revised Statutes, and external regulations that relate to data governance and Institutional Data classification categories are available at: www.hawaii.edu/infosec/policies.

VII. Exhibits and Appendices

No Exhibits and Appendices found

Approved

Signed	February 08, 2018
David Lassner	Date
President	

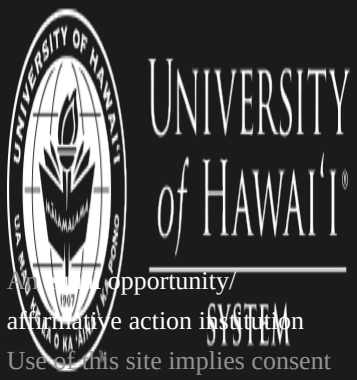
Topics

data; security

Attachments

+ Non-Fillable Attachment(s)

Adobe Reader | Help | PPIS email



2444 Dole Street
Honolulu, HI 96822

Contact UH

If required, information contained on this website can be made available in an alternative format upon request.

Get Adobe Acrobat Reader