UH Systemwide Policies and Procedures Information System (PPIS)

Executive Policy 2.215

Title

Institutional Data Governance

Header

Executive Policy Chapter 2, Administration
Executive Policy EP 2.215, Institutional Data Governance
Effective Date: February 2018
Prior Dates Amended: September 2012
Responsible Office: Office of the Vice President for Academic Planning and Policy
Governing Board of Regents Policy: RP 2.202, Duties of the President
Review Date: February 2021

I. Purpose

The objectives of this policy are to:

A. Establish fundamental principles governing the management and use of data and information at the University, including, but not limited to, the collection and creation, privacy and security, and integrity and quality of that data and information;

B. To ensure compliance with federal and state laws, rules, and regulations, including, but not limited to:

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

C. Set forth best practices for effective data management with ongoing objectives of increasing efficiencies, managing and mitigating information privacy and security risks, and promoting data quality;

D. Establish clear lines of accountability and decision rights through the definition of roles and responsibilities related to data management;

E. Establish a set of standardized terms and definitions to promote consistent interpretations and implementations of policies, procedures, and practices related to data management.

II. Definitions

A. Data Sharing Request Process – A process that governs the release of Institutional Data and provides an understanding of how the data is being used, by whom, and where it is being copied and stored.

B. Data Users – All UH employees, students, and affiliates who, in order to fulfill their job duties and responsibilities, require access to UH Institutional Data.

C. Departmental/Unit/Local Data Repositories – Various UH academic and administrative departments or units copy Institutional Data from Institutional Data Systems into their own departmental, unit, or local data repositories. Any Departmental/Unit/Local Data Repository that contains a copy of Institutional Data are subject to the same policies and procedures which govern the use of Institutional Data. This policy applies to all repositories of Institutional Data, irrespective of where the repository is maintained (for example, a department may contract for cloud storage services to maintain its data repository).

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

1. contained in any form, including but not limited to documents, databases, spreadsheets,

email, and websites;

2. represented in any form, including but not limited to letters, numbers, words, pictures, videos, sounds, symbols, or any combination thereof;

3. communicated in any form, including but not limited to handwriting, printing, photocopying, photographing, and web publishing; and

4. recorded upon any form, including but not limited to papers, maps, films, prints, discs, drives, memory sticks, and other information systems.

E. Institutional Data Systems – UH systemwide data repositories that collect and store both transactional (operational) and reporting types of Institutional Data, including Systems of Record. In some cases, Institutional Data may be purged on a regular basis from an Institutional Data System. Institutional Data Systems are subject to the same policies and procedures that govern the use of Institutional Data. Examples of Institutional Data Systems are the Banner Student Information System, PeopleSoft, Kuali Financial System, STAR, Laulima, etc.
A list of Institutional Data Systems and associated System Executive Data Stewards is available at the following website. Note the list is not intended to be all-inclusive of the University's Institutional Data Systems, but rather, represents Institutional Data Systems that are most likely to contain Protected Data. http://www.hawaii.edu/uhdatagov/stewards.pdf

F. Protected Data – Institutional Data that are subject to security and privacy considerations that range from moderate to very high (i.e., all non-public data). These data fall under the Institutional Data Classification Categories of "restricted," "sensitive," and "regulated." For more information, refer to Executive Policy EP2.214, Institutional Data Classification Categories and Information Security Guidelines.

G. System of Record – Institutional Data that are designated by a Data Steward as representing official values of the University. Official values are the data designated as the most accurate representation of the meaning and context of Institutional Data elements, which are recorded as facts. Official values are not necessarily the originally entered values, and as such, a System of Record may not necessarily be the system where values are originally entered. When questions arise over the meaning or interpretation of data elements or their values, the System of Record is used to resolve discrepancies.

III. Executive Policy

A. VISION

Data governance at the University of Hawai‘i fosters a culture of shared responsibility and active participation among members of the University community in the stewardship of data and information entrusted to the University. The University of Hawai‘i’s institutional data governance philosophy is grounded in the University’s core values of institutional integrity, service, collaboration, and respect, and its commitment to excellence and accountability.

B. GOALS

The goals of data governance at the University are to:

1. Protect the privacy and security of data and information under the stewardship of the University;

2. Support a culture of responsible data use for informed and actionable decision making;

3. Establish systemwide standards that enable holistic understanding of data across institutional boundaries;

4. Promote the efficient use of resources to meet the data and information needs of the University community;

5. Increase the University’s transparency and accountability to external stakeholders and the public by promoting access to relevant information.

C. POLICY STATEMENT

It is the policy of the University of Hawai‘i to hold itself accountable for the privacy and security of its Institutional Data while keeping that data accessible for appropriate use.

D. SCOPE

The scope of this institutional data governance policy applies to the following:

1. Individuals employed by the University or any affiliates (including external agencies such as RCUH, Sodexo, third party vendors, etc.) with access to University-related data and information (i.e., Institutional Data);

2. All Institutional Data created, collected, analyzed, and reported on by UH units as part of their administrative and academic functions, regardless of where they are located and in

what medium they are stored (e.g., physical or electronic), how they are accessed, and how they are transmitted;

3. Institutional Data, such as student demographics, used in surveys or studies;

This policy recognizes the legal responsibilities of individual campuses to protect the privacy and security of their students' data according to FERPA requirements.

This policy does not apply to data created, collected, or analyzed for the purpose of research that does not require the use of Institutional Data. Although those data are beyond the scope of this policy, they should follow the technical guidelines set forth in Executive Policy E2.214, Institutional Data Classification Categories and Information Security Guidelines.

E. PRINCIPLES

The following principles are set forth as minimum standards to govern the appropriate use and management of Institutional Data.

1. Institutional Data is the property of the University of Hawai‘i and shall be managed as a key asset through defined governance standards, policies, and procedures.

2. Institutional Data will be safeguarded and protected according to security, privacy, and compliance rules and regulations established by the federal and state government (see section I-B), and University of Hawai‘i policies. This University of Hawai‘i executive policy is not intended to supercede federal and state rules and regulations, but to promote and reinforce them.

3. Access to Institutional Data will be based on defined roles. Users deemed to have a legitimate educational interest will be assigned appropriate access based on their roles.

4. Institutional representatives will be held accountable to their roles and responsibilities. Roles and responsibilities involving the management and use of Institutional Data will be clearly defined, and individuals assigned to specific roles will be held accountable for their data management responsibilities.

5. The use, storage, and exposure of protected data will be minimized whenever possible.

6. The University strives to ensure the safety and security of its employees and its data assets. It will employ strategies in multiple ways, including the use of technology, physical space, etc. The strategies will take into consideration the privacy of individuals and the

protection of data based on the level of sensitivity.

7. The University's technical resources will be used for institutional purposes only and not for personal and/or private gain or for malicious intent.

F. BEST PRACTICES

1. Minimal access will be granted to Data Users. Individuals, including non-UH personnel (e.g., third party contractors), will be granted the most restrictive set of permissions and privileges based on feasibility and a need-to-know. Not only will the minimal level of access to perform an operation be granted, that access will be granted only for the duration of time necessary to complete the operation.

2. Disclosure of Institutional Data that are considered protected and personally identifiable will be based on a need to know. When possible, Institutional Data being disclosed will be de-identified.

3. Quality standards for Institutional Data will be defined, implemented, monitored, and communicated by System Executive Data Stewards of Institutional Data Systems (defined in sections II, Definitions and III-G, Roles and Responsibilities). Examples of data quality standards include: data validation rules, timeliness of updates, defined error rates, etc.

4. Unnecessary duplication of Institutional Data is discouraged. Maintaining repositories of redundant data increases the risk of inadvertent disclosure or inappropriate access to Institutional Data. Executive Data Stewards and Data Custodians (defined in section III-G, Roles and Responsibilities) will minimize redundant storage and processing of Institutional Data in multiple repositories where reasonable and appropriate.

5. Data Users will complete mandatory training requirements on the appropriate handling of Protected Data before they are allowed access. For more information, refer to AP2.215, Mandatory Training and Continuing Education Requirements for Data Users.

6. Resolution of issues related to Institutional Data will follow consistent and public processes. The Data Governance Committee (DGC) will coordinate the resolution of issues related to risks, costs, access, management, and use of Institutional Data with the appropriate Data Stewards and with UH leadership.

7. Institutional Data will only be released for student surveys that are being administered for

institutional purposes (such as improving services for students) and/or for the benefit students. Campuses make the final decision on which surveys student contact information will be released.
As part of the Data Sharing Request Process, requests involving the release of Institutional Data for student surveys will require an affirmative response from each Campus Executive Data Steward.

8. Institutional Data that was requested through the Data Sharing Request Process for a specific purpose cannot be used for another purpose.

9. Guidelines and procedures for the effective management of Institutional Data throughout its lifecycle (from creation to destruction) will be established. Guidelines and procedures involving the creation or acquisition, storage and maintenance, use, archival, and destruction of Institutional Data will be available to direct Data Users and Data Custodians in their data management practices.

10. Activities that reduce the potential exposure of sensitive information will be implemented through an information security program. The University will establish an information security program that addresses the following areas, including, but not limited to, governance structures, security audits, risk assessments, identity management, access controls, education and training, and network monitoring. The program will perform ongoing audits of high risk areas and enforce remediation measures, as necessary.

11. Contingency plans for managing security breaches and disaster recovery will be established. The process for managing security breaches and other inappropriate uses of Institutional Data will be addressed in University policy. Types of information included will be a definition of a security breach, guidelines on the timing, contents, and means of notice to affected parties, etc. Disaster recovery plans will include contingencies for the physical security of affected sites containing Protected Data.

12. Accessing Institutional Data remotely (for example, off-campus) will be done in a secure manner. Individuals who will be electronically accessing Institutional Data from a location other than their usual work areas will ensure they are not using unprotected or public wireless connections.

G. ROLES AND RESPONSIBILITIES
The following roles and responsibilities are defined, for both individuals and groups, for the

purpose of establishing clear governance and accountabilities over Institutional Data. The terms and conditions for appointments and assignments are outlined for each. Note that for University employees whose duties and responsibilities fall within a controlled access environment, this policy should not impact their daily activities, but rather, should clarify and formalize their roles and responsibilities.

1. Vice President for Academic Planning and Policy – The lead institutional officer responsible for developing and implementing the University's data governance program. Authority and responsibility resides with the Vice President for Academic Planning and Policy on policy and system (multi-campus) issues.

2. Vice President for Information Technology and Chief Information Officer – The officer responsible for setting and enforcing standards and guidelines for data management technologies and systems related to computing infrastructures, data processing performance, data delivery and integration, data architectures and structures, metadata repositories, and access control mechanisms. The Vice President for Information Technology and Chief Information Officer has custodial authority over centralized Institutional Data Systems, including the student, financial, and human resources databases.

3. Chancellors and System Vice Presidents – Chancellors and system vice presidents (collectively referred to as UH leadership) have authority and responsibility over policies and procedures regarding access and usage of data within their delegations of authority. The Vice President for Academic Planning and Policy will consult with UH leadership on strategic matters and conflict resolution issues. The Data Governance Committee serves in an advisory capacity to UH leadership, providing recommendations for actions.

4. Data Governance Committee (DGC) – A systemwide group dedicated to implementing a data governance program at the University. Committee members are appointed by the Vice President for Academic Planning and Policy.

The DGC's charges are to:

a. revise, recommend, and develop policies and standards that govern the University's data and information management practices at the direction of UH leadership;

b. define clear and consistent structures, models, and processes that promote the efficient use of resources to meet the information needs of the University community;

c. provide guidance and recommendations concerning the University's Institutional Data, including expanding access, improving quality, ensuring data security, and improving

performance;

d. provide recommendations to UH leadership as part of a formal appeal process involving disputes around Institutional Data and Institutional Data Systems.

5. Student Data Oversight Committee (SDOC) – A DGC subcommittee focused on improving data quality and access and providing guidance on future directions, priorities, and uses of student Institutional Data Systems. The SDOC has the authority to make decisions on student data issues and may recommend to the DGC policies and principles on data management and use.

6. Institutional Research and Analysis Office (IRAO) Director – A member of the DGC, the IRAO Director oversees the office that is the official reporting entity for student-related data and information for the University of Hawai‘i. The IRAO Director coordinates the cross-functional reporting and analysis of student, finance, and human resource data. The IRAO Director leads the University’s efforts around data quality and works collaboratively with system and campus leadership to improve the consistency and accuracy of data residing within the University’s Institutional Data Systems. The IRAO Director is the System Executive Data Steward for Banner (student module) and its operational data store (ODS).

7. UH System Chief Information Security Officer – A member of the DGC, the Chief Information Security Officer leads the University’s Information Security Program. The Information Security Team reports to the Chief Information Security Officer within Information Technology Services (ITS), and works with system and campus leadership to improve the security posture of the University.
To meet the requirements of the Information Security Program, ITS has the authority to require that all servers be registered and to implement standard security controls, such as network and server scanning, to identify security weaknesses in any University information system or network that may compromise protected data or the operations and availability of institutional services.
Likewise, ITS has the authority to enforce technical measures to ensure the protection of Protected Data that are stored or transmitted, whether intentionally or unintentionally, on University systems and networks, including but not limited to the immediate disconnection of compromised systems from the University network.
The Chief Information Security Officer convenes the systemwide Data Security Leadership Council and the UH Information Technology Security Leads group and updates the DGC on security and privacy issues.

8. Data Stewards – Data Stewards act in accordance and ensure compliance with applicable federal and state rules and regulations and University policies involving Institutional Data. Data Stewards are responsible for minimizing the use, storage, and exposure of Protected Data, particularly personally identifiable information. They are expected to limit the exposure of such data to only situations that are deemed essential and appropriate.
There are two levels of Data Stewards at the University of Hawai‘i: executive and functional.

a. Executive Data Stewards are accountable for the use and management of Institutional Data at their respective campus or within the Institutional Data System under their purview.

(1) Campus Executive Data Stewards

(a) These Data Stewards are vice chancellors or appropriate administrators responsible for the major functional areas within a campus including, but not limited to, student affairs, academic affairs, and administration. They have the authority to govern the use of Institutional Data within their respective areas.

(b) Campus Executive Data Stewards for student data have the responsibility of reviewing and approving data sharing requests within their respective campuses. As part of the review process, a Campus Executive Data Steward will notify relevant parties of data sharing requests for student-related data through an inclusive and open communication process. Human resource and financial data sharing requests are managed centrally by the UH System Offices of Human Resources and Financial Management.

(2) System Executive Data Stewards

(a) These Data Stewards are primarily system level executives with functional responsibility for Institutional Data Systems (see section II, Definitions). They have the authority to govern the use of Institutional Data within these Institutional Data Systems.

(b) System Executive Data Stewards review and approve Data Sharing Requests involving multiple campuses, external parties, and/or electronic linkages to Institutional Data Systems. As part of the review process, the System Executive Data Steward will notify relevant parties of Data Sharing Requests through an inclusive and open communication process.

(c) System Executive Data Stewards also have the authority to grant access to Institutional Data Systems for system and campus personnel.

(d) System Executive Data Stewards have the additional responsibility of responding to the data and information needs of the University community through the Institutional Data Systems they oversee. They sponsor and promote a shared understanding of data through clear data element definitions, and oversee data quality and performance improvements within these systems.

Refer to the UH Data Governance website for a listing of Institutional Data Systems and associated Executive Data Stewards.

b. Functional Data Stewards are responsible for the day-to-day use, management, and distribution of Institutional Data. Functional Data Stewards exist among all levels and across all units within the University. Registrars, financial aid officers, fiscal managers, human resources specialists, and institutional researchers are among those considered Data Stewards.
Functional Data Stewards engage in the following types of data related activities:

(1) Ensure Institutional Data is managed appropriately, according to policies and procedures;

(2) Recommend enhancements for their respective program areas to improve data quality, access, security, performance, and reporting;

(3) Serve as a conduit between functional and technical personnel to promote communication and a shared understanding of requirements;

(4) Fulfill Data Sharing Requests.

9. Data Custodians – Data Custodians are the managers and/or administrators of systems or media on which protected data reside, including, but not limited to, personal computers, laptop computers, PDAs, smartphones, departmental servers, enterprise databases, storage systems, magnetic tapes, CDs/DVDs, USB drives, paper files, and any other removable or portable devices or off-site storage technologies. These may include, but are not limited to, cloud storage or cloud services. Information technology personnel are commonly regarded as Data Custodians, however, any authorized individual who downloads or stores sensitive information onto a computer or other storage device becomes a Data Custodian through that act.

Data Custodians are responsible for the technical safeguarding of protected data, including implementing and administering controls that ensure the transmission of those protected data are secure and access controls are in place to prevent inappropriate disclosure. This can be as simple as utilizing UH FileDrop to transfer Protected Data.

10. Data Users – UH employees, students, and affiliates who, in order to fulfill their job duties and responsibilities, require access to protected data as defined in Executive Policy E2.214, Institutional Data Classification Categories and Information Security Guidelines. Data Users are responsible for understanding and complying with applicable University policies and procedures and all recognized federal and state laws for dealing with protected data.

To ensure compliance and to meet the objectives of this policy, individuals must complete training requirements as outlined in AP2.215, Mandatory Training and Continuing Education Requirements for Data Users. Those who do not comply will be denied access. Specific questions about the appropriate handling or usage of Institutional Data should be directed to the Executive Data Steward responsible for that area.

IV. Delegation of Authority

There is no policy-specific delegation of authority.

V. Contact Information

Subject Matter Experts

Office of the Vice President for Academic Planning and Policy
ovpaa@hawaii.edu
956-6897

Office of the Vice President for Academic Planning and Policy
Sandra Furuto, 956-7487, yano@hawaii.edu
www.hawaii.edu/uhdatagov

VI. References

The following site lists the University of Hawai‘i executive policies, State of Hawai‘i Revised Statutes, and external regulations that relate to data governance and have information

security implications.
http://www.hawaii.edu/infosec/policies.html

VII. Exhibits and Appendices

No Exhibits and Appendices found

Approved

Signed	March 26, 2018
David Lassner	Date
President	

Topics

No Topics found.

Attachments

None