Prepared by the Office of the Executive Vice President for Academic Affairs/Provost
This is a NEW Executive Policy

UNIVERSITY OF HAWAI‘I

EXECUTIVE POLICY ON INSTITUTIONAL DATA GOVERNANCE
September 2012

E2.215 – Institutional Data Governance

> *“Data governance is the exercise of authority and control (planning, monitoring, and enforcement) over the management of data assets.”*
>
> *DAMA: Guide to the Data Management Body of Knowledge*

I. 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.

II. GOALS

The goals of data governance at the University are to:

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

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

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

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

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

III. DEFINITION OF INSTITUTIONAL DATA AND POLICY STATEMENT

"Institutional Data" is defined as data elements that are created, received, maintained and/or transmitted by the University of Hawai'i in the course of meeting its administrative and academic requirements.

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.

IV. 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 creation or acquisition, privacy and security, and integrity and quality of that data and information;

B. 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;

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

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

V. SCOPE

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

1. Users employed by the University or any affiliates (including external agencies such as RCUH, Sodexho, 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;

4. Sensitive information which are subject to privacy considerations or have been classified as confidential and are therefore subject to protection from public access or inappropriate disclosure. Sensitive information, including personally identifiable information (PII), is defined in Executive Policy E2.214, Security and Protection of Sensitive Information.

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

C. 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 are subject to the requirements of Executive Policy E2.214, Security and Protection of Sensitive Information, which apply to all University-related data.

VI. PRINCIPLES

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

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

B. Institutional Data shall be protected. – Institutional Data must be safeguarded and protected according to security, privacy, and compliance rules and regulations established by

the federal and state government, and University of Hawai‘i policies. Refer to the UH Data Governance website (www.hawaii.edu/uhdatagov) for a listing of applicable rules, regulations, and policies involving the proper handling of sensitive information. This policy is not intended to supercede federal and state rules and regulations, but to promote and reinforce them.

C. Institutional Data shall be accessible according to defined needs and roles. – Institutional Data shall be made accessible in accordance with the University’s administrative policy on data sharing (forthcoming). Users deemed to have a legitimate educational interest shall be assigned appropriate access based on their roles.

D. 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.

E. Resolution of issues related to Institutional Data shall follow consistent and public processes. – The Data Governance Committee shall 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.

VII. BEST PRACTICES

A. Unnecessary duplication of Institutional Data is discouraged. – Data Stewards (defined in section VIII, Roles and Responsibilities) shall be responsible for minimizing redundant storage and processing of Institutional Data in multiple repositories where reasonable and appropriate.

B. Quality standards for Institutional Data shall be defined. – Data quality standards shall be defined, implemented, monitored, and communicated by System Executive Data Stewards of Institutional Data Systems (defined in section IX, Definitions). Examples of data quality standards include: data validation rules, timeliness of updates, defined error rates, etc.

C. Training and education for Data Users and their supervisors shall be provided. – Training and education on the

appropriate handling of sensitive information must be completed before Data Users (defined in section VIII, Roles and Responsibilities) are allowed access to sensitive information. Supervisors must also complete the same training and education as their employees.

D. Guidelines and procedures for the effective management of Institutional Data throughout its lifecycle (from creation to destruction) shall 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.

E. Activities that reduce the potential exposure of sensitive information shall 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.

F. Contingency plans for managing security breaches and disaster recovery shall 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 sensitive information.

VIII. 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.

A. Executive Vice President for Academic Affairs/Provost – The Executive Vice President for Academic Affairs/Provost is the lead institutional officer responsible for developing and implementing the University's data governance program. Authority and responsibility resides with the Executive Vice President for Academic Affairs/Provost on policy and system (multi-campus) issues.

B. Vice President for Information Technology and Chief Information Officer – The Vice President for Information Technology and Chief Information Officer is 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.

C. 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 Data Governance Committee serves in an advisory capacity to UH leadership on strategic matters and conflict resolution issues.

D. Data Governance Committee (DGC) – The Data Governance Committee is a systemwide group dedicated to implementing a data governance program at the University. Committee members are appointed by the Executive Vice President for Academic Affairs/Provost. Membership is based on ex-officio roles for system-based personnel and two-year terms for campus-based personnel. Rotating memberships of campus-based personnel are intended to promote knowledge and awareness of data governance throughout the system. Refer to the UH Data Governance website for the membership roster.

   The DGC's charges are to:

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

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

3. provide guidance and recommendations concerning the University's Institutional Data, including expanding access, improving quality, assuring security, and improving performance;

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

E. Institutional Research and Analysis Office (IRAO) Director – A member of the DGC, the IRAO Director oversees the office that maintains the System of Record for student-related data and information and 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 operational and policy research data within the University's Institutional Data Systems (see section IX, Definitions). The individual updates the DGC on data quality issues and is responsible for decisions around mediating and correcting inconsistencies in data definitions.

F. UH System Information Security Officer – A member of the DGC, the UH System Information Security Officer leads the University's Information Security Program. The individual works with system and campus leadership to improve the security posture of the University. The individual convenes the Data Security Leadership Council and the UH Information Technology (IT) Security Leads groups and updates the DGC on security and privacy issues. Refer to the UH Data Governance website for both membership lists.

G. 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 sensitive information, particularly personally identifiable information. They have responsibility to restrict the use and exposure of such information to those specific situations where it is essential and appropriate.

There are two levels of Data Stewards at the University of Hawai‘i: executive and functional.

1. 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.

   a. Campus Executive Data Stewards
      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.

      Campus Executive Data Stewards for student data have the additional 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. Refer to the administrative procedure on data sharing (forthcoming) for details on the types of requests a Campus Executive Steward authorizes, the review process, and the appeal/exception process. Human resource and financial data sharing requests are managed centrally by the UH System Offices of Human Resources and Financial Management.

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

      System Executive Data Stewards review and approve data sharing requests. These requests involve 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. Refer to the

administrative policy on data sharing (forthcoming) for details on the types of requests a System Executive Data Steward authorizes, the review process, and the appeal/exception process.

System Executive Data Stewards also have the authority to grant access to Institutional Data Systems for system and campus personnel. Refer to the listing of Institutional Data Systems and their associated System Executive Data Stewards and Vice Presidents who are accountable for those systems on the UH Data Governance website. If a request for access is denied, the requestor may appeal or request an exception from the Vice President. The DGC will provide a recommendation to the Vice President who will then decide on the matter. The Vice President's decision is final. For more detail, refer to the administrative procedure on access (forthcoming).

System Executive 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 System Executive Data Stewards.

2. Functional Data Stewards are responsible for the day-to-day use and management 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:

   a. Ensure Institutional Data is managed appropriately, according to policies and procedures;

b. Recommend enhancements for their respective program areas to improve data quality, access, security, performance, and reporting;

c. Serve as a conduit between functional and technical personnel to promote communication and a shared understanding of requirements;

d. Fulfill data requests according to administrative procedures on data sharing.

H. Data Custodians – Data Custodians are the managers and/or administrators of systems or media on which sensitive information resides, 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 such as, but 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 sensitive information, including implementing and administering controls that ensure the transmission of sensitive information is secure and access controls to prevent inappropriate disclosure are in place.

I. Data Users – Data Users are individuals who, in order to fulfill their job duties and responsibilities, require access to sensitive information as defined in Executive Policy E2.214, Security and Protection of Sensitive Information, and are therefore granted access. Data Users are responsible for understanding and complying with all applicable University policies and procedures for dealing with sensitive information and its protection. 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 Data Steward responsible for that area.

IX. DEFINITIONS

A. Institutional Data – “Institutional Data” is defined as 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.

B. Institutional Information – “Institutional Information” is defined as a collection of Institutional Data which can 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, 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.

C. System of Record – A “System of Record” is Institutional Information that is 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.

D. Institutional Data Systems – Institutional Data Systems are systemwide data repositories that collect and store Institutional Data and Institutional Information. These repositories house both transactional (operational) and reporting types of Institutional Data and Institutional Information, 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.

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

E. 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.)