University of Hawai‘i
Executive Policy on Data Governance
(Draft 2/1/12)

I. Definition

"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

II. Vision

Data governance at the University of Hawai‘i fosters a shared responsibility for and participation in the stewardship of data and information entrusted to the University, and promotes a governance philosophy grounded in the University’s core values of institutional integrity, service, collaboration, and respect as well as commitments to excellence and accountability.

III. Goals

The goals of data governance at the University are to:

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

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

• Promote an integrated view of data across organizational boundaries in the system;

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

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

IV. Purpose

The objectives of this policy are to:

• 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, integrity and quality of that data and information;

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

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

V. Scope

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

• 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 - see Definitions below);

• Data originating from any Systems of Record (see Definitions below).

• All Institutional Data managed by UH units that may be used for administrative, academic, or educational research activities;

• All categories of data, regardless of the medium in which the data is held or transmitted (e.g., physical or electronic);

• Sensitive information which are subject to privacy considerations or has been classified as confidential and are therefore subject to protection from public access or inappropriate disclosure. Sensitive information, also referred to as personally identifiable information (PII), are defined in E2.214, Executive Policy on Security and Protection of Sensitive Information (www.hawaii.edu/apis/ep/e2/e2214.pdf);

The scope of this policy does not apply to data created or collected outside of the University’s Systems of Record. While data created or collected outside of the University’s Systems of Record are beyond the scope of this policy, it should be noted that those data, like all University-related data, are subject to the requirements of Executive Policy E2.214.

This policy recognizes the legal responsibilities of individual campuses to protect the privacy and security of their students’ data.

VI. Principles

The following principles are set forth as minimum standards to govern the appropriate usage and management of Institutional Data (see Definitions below).

• 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 guidelines, standards, policies and procedures.
• **Institutional Data shall be protected.** – Institutional Data must be safeguarded and protected according to approved security, privacy and compliance guidelines, laws, and regulations established by the University of Hawai‘i, the state, or the federal government.

• **Institutional Data shall be accessible according to defined needs and roles.** – Institutional Data and Metadata shall be accessible to all, in accordance with defined access and use policies and procedures determined by the Data Governance Committee and Data Stewards (defined below). Users requesting access shall be assigned to appropriate roles that have clearly documented guidelines in accordance with all University of Hawai‘i, state, and federal laws and regulations.

• **Institutional representatives will be held accountable to their roles and responsibilities.** – Roles and responsibilities for data management will be clearly defined, and individuals assigned to specific roles will be held accountable for performing data management responsibilities, as a part of their regular job responsibilities.

• **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**

• **Unnecessary duplication of Institutional Data is discouraged.** – Data Custodians (defined below) shall be responsible for sharing Institutional Data out of official Systems of Record, when reasonable and according to policies and procedures, so as to minimize redundant storage and processing of that data in multiple repositories. Exceptions are allowed for purposes of business continuity and fail-over.

• **Unnecessary updating of Institutional Data is discouraged.** – When the same Institutional Data elements exist in multiple Systems of Record, the official values must be kept synchronized. When feasible, manual updates of Institutional Data should be performed in one System of Record and then automatically copied to as few other additional data repositories as possible. This eliminates redundant processing, increases integrity, and provides better auditing capabilities.

• **Quality standards for Institutional Data shall be defined and monitored.** – Data quality standards shall be defined, published, communicated, managed, and applied according to the reliability and risk levels established by appropriate Data Stewards (defined below). Examples of data quality standards include: data validation rules, timeliness of updates, defined error rates, integrity monitoring processes, etc.
• **Institutional Metadata shall be recorded, managed, and utilized.** – Metadata will be used to model, define, and organize data in order to maximize the value of Institutional Data. Institutional Metadata will be published and communicated clearly and consistently.

• **Necessary maintenance of Institutional Data shall be defined.** – Maintenance of Institutional Data to ensure appropriate backup, retention, destruction, de-identification, etc. will be defined by appropriate Data Custodians and Information Technology Services and other system operators.

### VIII. Definitions

• **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.

• **Institutional Information** – “Institutional Information” is defined as a collection of Institutional Data which can be **contained** in any form, including but not limited to documents, databases, spreadsheets, email and websites; **represented** in any form, including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof; **communicated** in any form, including but not limited to handwriting, printing, photocopying, photographing, and web publishing; and **recorded** upon any form, including but not limited to papers, maps, films, prints, discs, drives, memory sticks, and other information systems.

• **Institutional Metadata** – “Institutional Metadata” is data collected, maintained, and used to describe and define the processes around the management of Institutional Data. Examples of Institutional Metadata include:
  - Definitions regarding the purpose, usage and context of Institutional Data
  - Identification of which system is the official system of record of Institutional Data
  - Who is responsible for management of Institutional Data
  - How Institutional Data is transferred, derived, and stored
  - What security and privacy practices are used to safeguard Institutional Data
  - Risk and compliance classifications for Institutional Data
  - Rules around retention of records and data

• **System of Record** – A “System of Record” is an information system that is designated by Data Steward (defined below) as holding **official values** of Institutional Information. 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.
- **Institutional Data Warehouses** – Institutional Data is often copied from Systems of Record into other systems, for ease of access, or to facilitate historical storage of data. UH’s Operational Data Store (ODS) is an example of this type of additional data repository. Since Systems of Record may purge Institutional Data on defined schedules, these types of additional data repositories may contain Institutional Data that survives beyond what the System of Record contains. They then become a System of Record holding official values of Institutional Data. These additional Institutional Data Warehouses are sanctioned by Data Stewards (defined below) and are subject to the same policies and procedures that govern the use of Institutional Data.

- **Departmental/Unit/Local Data Repositories** – Various UH academic and administrative departments or units copy Institutional Data from Systems of Record 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.

**IX. 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.

- **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.

- **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 delegated authority over centralized Institutional Data Warehouses, such as the student, financial, and human resources databases.

- **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.
• **Data Governance Committee (DGC)** – The Data Governance Committee is responsible for: 1) revising, recommending, and endorsing the policies and standards that govern the University’s data and information management practices; 2) defining clear and consistent structures and models, and establishing definitions to support systemwide coordination and collaboration, effective decision-support, and efficient operations; and, 3) providing guidance and recommendations concerning the University’s institutional data related to expanding access, improving quality, assuring security, and improving performance. The DGC also recommends solutions to UH leadership when disputes arise in the definition or usage of Institutional Data, promotes knowledge and awareness of the existence of data governance policies, standards, guidelines, and procedures. 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.

• **Institutional Research and Analysis Office (IRAO) Director** – A voting ex-officio 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 administrative data systems. The individual updates the DGC on data quality issues and is responsible for decisions around mediating and correcting inconsistencies in data definitions.

• **Information Technology (IT) Security Officer** – A voting ex-officio member of the DGC, the 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 IT Security Leads groups and updates the DGC on security and privacy issues.

• **Data Stewards** – Institutional Data shall have one or more designated stewards. Data stewards are typically senior administrators responsible for functional operations such as Finance, Human Resources, Student Services and other activities that involve institutional information processing. At the University of Hawai‘i, offices such as the Institutional Research and Analysis Office (IRAO) and Information Technology Services (ITS) also have stewardship responsibility for institutional information.

Data stewards ensure applicable federal, state and UH policies, standards, regulations and laws are met with regard to data in their respective areas. Data stewards are also responsible for minimizing the use, storage and exposure of
sensitive information, i.e., PII. They have responsibility to restrict the use and exposure of such information to those specific situations where it is essential and appropriate.

- **Data Custodians** – Data custodians are the managers and/or administrators of systems or media on which sensitive data 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. Any authorized individual who downloads or stores sensitive information onto a computer or storage device becomes a data custodian through that act.

Data custodians are responsible for implementing and administering controls over the resources according to policies and parameters provided by data stewards. Data custodians are responsible for the technical safeguarding of sensitive information, including ensuring security transmission and providing access control systems approved by data stewards to prevent inappropriate disclosure.

- **Users** – Users are any individuals who, in order to fulfill their job duties and responsibilities, require access to sensitive information as defined in Executive Policy E2.214, and are therefore granted access. Individuals must successfully complete training requirements as specified in Executive Policy E2.214 before access will be granted. Users are responsible for understanding and complying with all applicable University policies, procedures, and standards for dealing with sensitive information and its protection.

Specific questions about the appropriate handling or usage of a specific information resource should be directed to the data steward responsible for that area.