DATA MANAGEMENT POLICY **POLICY #**

Implementation Date: Date current P&P was approved by President, or effective date if different than approval date

Definition

Humboldt State University is committed to making decisions based on data. The quality of those decisions is directly linked to the consistency, integrity, and completeness of the data stored in HSU's enterprise systems. A solid governance foundation paves the way for users to trust and value institutional data and to leverage the data to its potential. Access to campus systems for the purpose of maintaining records within those systems or reporting the data within those systems should be granted to employees with a legitimate business need.

The purpose of this policy is replace (EM P09-02: HSU Policy to Implement the System wide Records/Information Retention and Disposition Schedule – Executive Order 1031) and update (UML 05-03: Student Records Access Policy) previous campus level policies in order to bring campus into alignment with the requirements of the CSU Information Security Policy (ICSUAM 8000.0), and developing an integrated list of roles and assignments for data managers at HSU. This Data Management Policy will also provide an ongoing mechanism by which that list is maintained, and clear definitions for the responsibilities associated with the various Data Management roles at Humboldt State University.

The list of employees assigned to specific roles is now maintained at http://www.humboldt.edu/its/security-data-management.

Authority

ICSUAM 8000.0 – System Wide Information Security Policy
CSU Executive Order 1031 – System Wide Records/Information Retention and Disposition Schedules Implementation

Scope

All HSU employees with access to Institutional Data, including employees in auxiliary and self-support units

Lisa A. Rossbacher, President — Approval Date

Noah Zerbe
Chair, University Senate — Approval Date

Implementation Date: Date current P&P was approved by President, or effective date if different than approval date

I. Policy Statement

University executives and managers who are assigned responsibility for areas of Institutional Data shall provide stewardship of those records by ensuring that only appropriate access is given, that the integrity of the records is maintained, and that records are disposed of following the CSU guidelines. All employees who are granted access to Institutional Data are expected to limit its use to the performance of their duties to the institution, to respect the privacy of students and employees who are represented by the data, and to treat the data and any analysis or reporting generated from the data with the highest ethical standards.

II. Definitions

A. Institutional Data

A data element qualifies as Institutional Data if it is:

- Relevant to planning, managing, operating, controlling, or auditing administrative functions of an administrative or academic unit of the University; or
- Generally referenced or required for use by more than one organizational unit; or
- Included in an official University administrative report; or
- Used to derive an element that meets one or more of the criteria above.

B. Data Classification

The California State University System defines three data classification categories. The complete Data Classification standard is available here which includes additional details and examples. The three levels are:

- Confidential
- Internal
- General

III. Roles and Responsibilities

A. Campus Manager

Senior-level employees of Humboldt State University (typically a VP or AVP) are responsible for:

- Ensuring that information assets under their control are managed in compliance with CSU and campus information security policies and standards;
- Ensuring that staff and other users of information assets under their control are informed of and comply with CSU and campus information security policies and standards.

1. Assignment of Campus Managers
   The President will review and approve Campus Manager assignments on an annual basis.

2. HSU Campus Managers have been identified and are listed at: http://www.humboldt.edu/its/security-data-management

B. Data Owner

A Data Owner is a senior-level employee of Humboldt State University (typically an MPP or executive) who oversees one or more sets of Institutional Data and is responsible for:

- Classifying each information asset for which the Data owner has ownership responsibility in accordance with CSU and campus policy/standards, or legal, regulatory or contractual requirements;
- Working with the Information Security Officer (ISO) to define controls for limiting access to and preserving the confidentiality, integrity, and availability of information assets that have been classified as requiring such controls;
- Authorizing access to the information asset by 1) serving as an Access Grantor themselves or 2) delegating an Access Grantor who will:
    - Authorize (or deny) Access Requests
    - Ensure that those who are granted access understand their responsibilities
    - Regularly review the list of those with access for continuing appropriateness
- Attending the semi-annual Data Managers meetings to:
    - Participate in conversations about important issues relevant to the integrity of Humboldt State University's data assets
    - Review this policy and associated procedures on a biennial basis
- Administering CSU Records/Information Retention and Disposition schedules, as defined below.

1. Assignment of Data Owners

   The initial list of Data Owners was reviewed and approved by the Campus Managers. Campus Managers will review and approve Data Owner assignments on an annual basis.

2. HSU Data Owners have been identified and are listed at: http://www.humboldt.edu/its/security-data-management

C. Access Grantor

An Access Grantor is an employee of the University who has been delegated day-to-day administrative responsibility for defining and monitoring access to Institutional Data, and is responsible for:

- Reviewing and approving security roles created in Enterprise Systems which structure how appropriate access is provided to the relevant set of data;

- Approving or denying requests to grant such roles and other access to individual employees or defined groups of employees.

    1. Assignment of Access Grantors
       Data Owners can delegate their day to day Access Granting responsibility to others in their unit, but must do so by submitting the Delegation by Data Owners form to the Information Security Officer. Data Owners will review and approve Access Grantor delegations on an annual basis.

    2. HSU Access Grantors have been identified and are listed at: http://www.humboldt.edu/its/security-data-management

    3. Requirements for Access to Institutional Data
        - Campus employees and volunteers who require access to Level 1 or Level 2 Institutional Records must obtain approval from an Access Grantor.
        - All individuals requesting access to Institutional Records are required to have a confidentiality agreement on file with the University.
        - Individual access requests must be made by a supervisor or administrator on behalf of the employee or volunteer for approval by the appropriate Access Grantor(s).
        - Employment groups may be assigned to an approved role based on classification or position (e.g., all faculty get the advisor role).
        - Access to these records must be removed when an individual is transferring positions or is separating from HSU (see Access Request Information).

D. Records Custodian

Records custodians are responsible for controlling the physical administration of records/information *in all media forms*, and are responsible for:

- Ensuring that their subject area is operating in compliance with the California State University Records/Information Retention and Disposition schedules (EO 1031) (http://www.calstate.edu/recordsretention/);
- Publishing their subject area Records/Information Retention and Disposition schedule to the campus
- Identifying records/information that may have historic or vital value for their subject area;
- Ensuring that the designation of a vital record/information is consistent with the campus' business continuity plans (per Executive Order 1014 www.calstate.edu/EO/EO-1014.html);
- Establishing procedures regarding the modification of retention and disposition schedules, as needed, to incorporate records unique to their subject area;

- Annually reviewing records/information as listed on the schedules to determine if they should be destroyed or maintained;
- Ensuring appropriate and timely disposal of records/information in accordance with retention and disposition schedule timeframes;
- Continuing to secure records/information in accordance with applicable campus and CSU policy;
- Certifying annually, by July 31, that their subject area Records/Information Retention and Disposition schedule is up to date and records are in compliance with the policy, by sending to the Director of Financial Services:
    - a copy of the subject area Records/Information Retention and Disposition Schedule
    - a signed copy of the Records/Information Retention and Disposition Schedule Certificate.

1. Assignment of Records Custodians
   Some Records Custodians are specified by EO-1031, while others can be delegated their responsibilities by the relevant Data Owner by submitting the Delegation by Data Owners form to the Information Security Officer. Data Owners will review and approve Records Custodian delegations on an annual basis.

2. HSU Records Custodians have been identified and are listed at http://www.humboldt.edu/its/security-data-management

E. Report Author

A Report Author is an employee of the University who has been given access to a set or multiple sets of Institutional Data for the purposes of analysis and reporting. Since the reports created by Report Authors can be distributed to others in the organization or posted publically without specific access review, each individual with this role has responsibilities for understanding data exposure risks. Responsibilities for Report Authors are:

- Reviewing, understanding and following applicable restrictions (CSU Data Classifications, State and Federal Law, FERPA, etc.) for the data sets in question;
- Safeguarding sensitive data to guarantee privacy and confidentiality;
- Using data in a manner consistent with the reason it was gathered;
- Reporting data accurately and without bias;
- Developing and reviewing with Data Owners an appropriate statistical model for aggregate reporting if public reporting is needed;
- Developing and reviewing a security role or set of roles with Access Grantors for report distribution.

1. Assignment of Report Authors
   Report Authors are assigned by job function.

F. Campus Data User

University employees who request or are granted access to campus information systems are Campus Data Users. The responsibilities of a Data User are:

- Understanding their responsibilities for collecting, using, and disposing Institutional Data in accordance with CSU and campus policies/standards, or legal, regulatory, or contractual requirements;
- Ensuring that any University information asset to which they have access is not put at risk through their actions;
- Working with the ISO, Data Owner, Access Grantor, and/or other authorized individuals during the investigation and mitigation of information security incidents affecting the information asset.

1. Assignment of Campus Data Users
   All individuals requesting access to Institutional Records are required to have a confidentiality agreement on file with the University. Campus employees and volunteers who require access to Level 1 or Level 2 Institutional Records must obtain approval from an Access Grantor.

Revised: date third revision was approved by President or effective date (if different than approval date): _____
Revised: date second revision was approved by President or effective date (if different than approval date): _____
Revised: date first revision was approved by President or effective date (if different than approval date): _____
Implemented initially: date P&P was first approved by President or effective date (if different than approval date):_____