I. **Purpose**

A. To describe the mandatory training and continuing education requirements for individuals with access to UH Institutional Data considered protected (i.e., data classified as restricted, sensitive, and regulated). These groups of individuals include:

1. Data Users who have been or will be granted login privileges to Institutional Data Systems as part of their job duties and responsibilities and therefore work with Institutional Data.

2. Individuals who are requesting access to Institutional Data through the Data Sharing Request Process. The request for access may be related to fulfilling an administrative or academic work-related requirement or for research projects.

Note the data may be accessed in any form, i.e., electronically, on paper, or other media. Electronic access is tied to login privileges to Institutional Data Systems or other UH or third party data systems that hold UH protected data.

B. To protect the privacy and security of Institutional Data under the University’s stewardship.

C. To ensure compliance with federal and state laws, rules, and regulations, including, but not limited to Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), Hawai‘i Revised Statutes, Chapter 487N - Security Breach of Personal Information, and Chapter 92F - Uniform Information Practices Act as well as all applicable University policies (e.g., Executive Policies EP 2.215 – Institutional Data Governance and EP 2.214 Institutional Data Classification Categories and Data Security Guidelines).
II. Definitions:

A. Data Users – All 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 EP 2.214, Institutional Data Classification Categories and Data Security Guidelines, and are therefore granted access. Data Users are responsible for understanding and complying with applicable UH policies and procedures and federal and state laws dealing with protected data. This administrative procedure applies to Data Users who are granted login privileges to Institutional Data Systems to access protected data.

B. 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, and how it is being managed and protected.

http://www.hawaii.edu/uhdatagov/

C. Executive Data Stewards – Executive Data Stewards exist at the system and campus levels. They are accountable for the use and management of Institutional Data at their respective campuses or within the Institutional Data Systems under their purview. Executive Data Stewards have the authority to grant and remove access privileges to Institutional Data Systems. For more information on Executive Data Stewards, refer to Executive Policy EP 2.215, Institutional Data Governance. A listing of Executive Data Stewards and associated System Executive Data Stewards is available at the following site.

http://www.hawaii.edu/uhdatagov/stewards.pdf

D. General Confidentiality Notice (GCN) – One of two mandatory training and continuing education requirements for Data Users. The GCN outlines the responsibilities of Data Users with access to protected information. A UH username is required to access the GCN.

http://www.hawaii.edu/its/acer/

A GCN for individuals who do not have UH usernames (third parties) is also available.

http://www.hawaii.edu/uhdatagov/nonuh_gcn.pdf

E. Information Security Awareness Training (SAT) – The second of two mandatory training and continuing education requirements for Data Users. Information Security Awareness Training covers the proper handling of protected information and related UH policies and procedures, and applicable federal and state laws and regulations.
https://www.hawaii.edu/infosec/training.html

F. Institutional Data Systems – UH systemwide repositories that collect and store data that are created, received, maintained and/or transmitted by the University of Hawai‘i in the course of meeting its administrative and academic requirements (e.g., Banner Student Information System, PeopleSoft, Kuali Financial System, STAR, Laulima, etc.).

A listing of Institutional Data Systems and associated System Executive Data Stewards is available at the following site. Note the list is not intended to be all-inclusive of the University’s Institutional Data Systems, but rather, represents Institutional Data Systems that most likely contain protected data.
http://www.hawaii.edu/uhdatagov/stewards.pdf

G. Legitimate educational interest – The basis for granting access to an education record, which is to perform an appropriate educational, research or administrative function of the University.

H. Protected data – Institutional Data that are subject to security and privacy considerations (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 Data Security Guidelines.

III. Administrative Procedure

A. APPLICABILITY

1. This administrative procedure is applicable to:

   a. Data Users who are requesting login privileges to Institutional Data Systems for the first time as part of their job duties and responsibilities;

   b. Data Users who require the continuation of login privileges to Institutional Data Systems as part of their job duties and responsibilities;

   c. Individuals who are requesting access to Institutional Data through the Data Sharing Request Process. The request for access may be related to fulfilling an administrative or academic work-related requirement or for research purposes. The Data Sharing Request Process applies to individuals who are requesting access to data that they do
not normally have access to and therefore need someone else to provide the data to them.

B. MANDATORY TRAINING AND CONTINUING EDUCATION REQUIREMENTS FOR DATA USERS

1. To be granted initial access to protected data, Data Users will need to complete the Information Security Awareness Training (SAT) and General Confidentiality Notice (GCN).

   a. Information Security Awareness Training (SAT)

      (1) Data Users with UH usernames must self-register and successfully complete the training modules. 
          www.hawaii.edu/infosec/training.html

      (2) Individuals who do not have UH usernames must contact the Data Governance Office to gain access to the training modules (datagov@hawaii.edu, 956-7487).

   b. General Confidentiality Notice (GCN)

      (1) Data Users with UH usernames must log in, read, and acknowledge the GCN. 
          www.hawaii.edu/its/acer

      (2) Individuals who do not have UH usernames must complete the Non-UH GCN version. 
          http://www.hawaii.edu/uhdatagov/nonuh_gcn.pdf

   c. Data Users requesting access privileges to a particular Institutional Data System for the first time may need to complete a request form for that particular Institutional Data System in addition to completing the SAT and GCN.

   d. Requests for access to protected data for research purposes will be granted on a case by case basis as part of the Data Sharing Request Process.

2. For continued access to protected data, Data Users will need to renew their training and education requirements.

   a. The SAT must be re-taken every two years.

   b. The GCN must be re-acknowledged annually.
c. An email notification from the System Executive Data Steward (or his or her designee) will be sent two months in advance to Data Users and their supervisors when an SAT renewal and/or GCN re-acknowledgement are required. A final reminder will be sent to both parties a week in advance.

d. Access will be removed upon failure to complete either requirement within the specified expiration date(s).

C. MANDATORY TRAINING AND CONTINUING EDUCATION REQUIREMENTS FOR DATA SHARING REQUESTS

1. Individuals who are requesting access to Institutional Data through the Data Sharing Request Process will need to complete the Information Security Awareness Training (SAT) and General Confidentiality Notice (GCN). The request for access may be related to fulfilling an administrative or academic work-related requirement or for research purposes. Data sharing requests may only be submitted by individuals with UH usernames.

   a. Information Security Awareness Training (SAT)

      Individuals must self-register and successfully complete the training modules.

      www.hawaii.edu/infosec/training.html

   b. General Confidentiality Notice (GCN)

      Data Users with UH usernames must log in, read, and acknowledge the GCN.

      www.hawaii.edu/its/acer

D. EXECUTIVE DATA STEWARD ROLES AND RESPONSIBILITIES

1. The Executive Data Steward has the authority to grant or remove access to Institutional Data under their purview. This includes granting or removing access privileges to an Institutional Data System. For more information on Executive Data Stewards, refer to Executive Policy EP 2.215, Institutional Data Governance. A listing of Institutional Data Systems and associated System Executive Data Stewards is available at the following site.

   http://www.hawaii.edu/uhdatagov/stewards.pdf

2. The System Executive Data Steward of an Institutional Data System (or his or her designee) is responsible for ensuring Data Users are current on their Information Security Awareness Training
and GCN requirements. This responsibility involves notifying Data Users to re-take the training or re-acknowledge the GCN. The System Executive Data Steward will receive a report that indicates the status of each Data User. The System Executive Data Steward may appoint a designee to manage this function.

IV. **Contact Information**

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

V. **References**

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, 45 CFR 160, 162, 164
Hawai‘i Revised Statutes 487N, Security Breach of Personal Information
Hawai‘i Revised Statutes 92F, Uniform Information Practices Act
Executive Policy EP 2.215, UH Institutional Data Governance
Executive Policy EP 2.214, Institutional Data Classification Categories and Data Security Guidelines

**Approved:**

David Lassner  
President