Administrative Procedure, AP 2.215
Mandatory Training and Continuing Education
Requirements on Data Privacy and Security

Page 1 of 5

Administrative Procedure Chapter 2, Administration
Administrative Procedure AP 2.215, Mandatory Training on Data Privacy and Security
Effective Date: xxx 2021
Prior Dates Amended: N/A
Responsible Office: Office of the Vice President for Information Technology and Chief Information Officer
Governing Board of Regents Policy: RP 2.202 Duties of the President
Review Date: xxx 2022

I.   **Purpose**

A.   To establish a mandatory training (see exemptions to this policy in Section III.A. below) program that increases the knowledge and awareness of the University community in managing and protecting data subject to security and privacy considerations (referred to as "Protected Data"). The goal is to reduce the risk of inadvertent exposures or inappropriate disclosures of Protected Data under the University's stewardship.

B.   To ensure compliance with federal and state laws, rules, regulations, and industry standards (see list below) 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 Information Security Guidelines).

1. Family Educational Rights and Privacy Act (FERPA)

2. Higher Education Act (HEA)

3. Gramm-Leach-Bliley Act (GLBA)

4. Health Insurance Portability and Accountability Act (HIPAA)

5. General Data Protection Regulation (GDPR)

6. Hawaiʻi Revised Statutes, Chapter 487N – Security Breach of Personal Information

7. Chapter 92F – Uniform Information Practices Act

8. PCI-DSS (Payment Card Industry Data Security Standard)

9. NIST SP 800-171 (National Institute of Standards and Technology Special Programs)

10. National Industrial Security Program (NISPOM)

11. Bioterrorism Special Agent Program

II. Definitions:

A. "General Confidentiality Notice" ("GCN") – The GCN is completed as part of the onboarding process for new UH employees and outlines the responsibilities of Data Users with access to Protected Data. http://www.hawaii.edu/its/acer/

B. "Information Security Awareness Training" ("ISAT") – The ISAT covers best practices for protecting the privacy and security of Protected Data and applicable federal and state laws and regulations and related UH policies and procedures. http://www.hawaii.edu/its/acer/

C. "Institutional Data Systems" – They are 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. https://drive.google.com/file/d/13cmIaXofKhdymo1RKeHxMr_2hrPJtrug/view (update URL)

D. "Protected Data" – These are data that are subject to security and privacy considerations (i.e., all non-public data). They 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.

III. Administrative Procedure

A. APPLICABILITY

Mandatory training requirements consist of acknowledging the General Confidentiality Notice (GCN) and completing the Information Security Awareness Training (ISAT).

These training requirements apply to all UH employees except for employees who meet all three criteria below:

1. Their duties are not office- or classroom-based;

2. Their duties do not involve working with Protected Data; and,

3. They have limited access to technology at work.

Supervisors are responsible for determining whether the employees within the department/unit are exempt and should consult with their departmental HR office if they need guidance and/or assistance.

B. TRAINING AND CONTINUING EDUCATION REQUIREMENTS BY EMPLOYEE TYPE

1. UH New Hires

a. As part of the onboarding process, all newly hired UH employees, including student employees and graduate assistants, and excluding exempt employees (refer to section A), are required to acknowledge the GCN and complete the ISAT within the first two weeks of employment.

A UH username and password are required to access the GCN and ISAT at www.hawaii.edu/its/acer.

b. If a UH employee transfers to another unit within UH, the employee is not required to re-acknowledge the GCN and will not need to re-take the ISAT (i.e., the ISAT annual renewal date will remain unchanged).

c. Completion of the GCN and ISAT will be required before access privileges to Institutional Data Systems are granted.

2. Current UH Employees

a. All UH employees are required to re-take the ISAT annually, based on the anniversary date the ISAT was last completed.

b. An email notification will be sent 60, 30, 14, and 7 days in advance to employees when an ISAT renewal is required.

c. A valid ISAT must be maintained for continued access privileges to Institutional Data Systems.

3. UH Affiliates

a. Research Corporation of the University of Hawaiʻi (RCUH) employees whose responsibilities involve working with UH principal investigators are required to comply with the same requirements as UH employees.

b. All UH Foundation (UHF) employees are required to comply with the same requirements as UH employees.

C. TRACKING / MANAGING COMPLIANCE

1. Each department/unit will designate an individual to monitor compliance in meeting the mandatory training and continuing education requirements. This includes the acknowledgement of the GCN and completion of the ISAT within the first two weeks of employment. The ISAT will be completed annually thereafter.

2. Individuals responsible for monitoring compliance for their department/unit will have access to a web application that will provide them with GCN and ISAT completion statuses and reports.

3. Employees designated as exempt from the training by their supervisors should not be included in the web application that tracks GCN and ISAT compliance.

4. Compliance requirements for student employees and graduate assistants will be monitored by the department/unit where they are employed.

5. Failure to complete the requirements by the specified due date will be reported to the supervisor. Extenuating circumstances affecting an employee's ability to complete the requirements on time shall be taken into consideration by the supervisor. A reasonable timeframe to complete the requirements will be set by the supervisor and communicated to the employee.

6. Repeated non-compliance of mandatory training and continuing education requirements will follow University policies and procedures as well as applicable collective bargaining agreements, and may be subject to disciplinary actions up to, and including, termination.

IV. **Contact Information**

Office of the Vice President for Information Technology and Chief Information Officer
Sandra Furuto, 956-7487, yano@hawaii.edu

V.   **References**

The following site lists the University of Hawaiʻi executive policies, State of Hawaiʻi Revised Statutes, and external regulations that relate to data governance and have information security implications.

https://www.hawaii.edu/infosec/policies/

Approved:

_____   _____
David Lassner   Date
President