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. Hawai'i 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)

Deleted: for
Deleted: Users
Deleted: and Continuing Education Requirements for Data Users
Deleted: February 2018
Deleted: 0
Deleted: Academic Planning and Policy
Deleted: February
Deleted: 1
Deleted: To describe the mandatory training and continuing education requirements for UH employees, students, and affiliates who are considered Data Users.¶ To protect the privacy and security of Institutional Data under the University's stewardship.¶
Deleted: and
Deleted: ,

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

Deleted: <#>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/¶ Data Users – All UH employees, students, and affiliates who, in order to fulfill their job duties and responsibilities, require access to UH Institutional Data. Data Users are responsible for understanding and complying with applicable UH policies and procedures and federal and state laws dealing with Protected Data.¶ 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¶ ¶

Deleted: <#>

Deleted: <#>One of two mandatory training and continuing education requirements for Data Users.

Deleted: <#>protected information

Deleted: <#>. A UH username is required to access the GCN

Deleted: A GCN for individuals who do not have UH usernames (third parties) is also available. ¶ http://www.hawaii.edu/uhdatagov/nonuh_gcn.pdf¶ ¶

Deleted: The second of two mandatory training and continuing education requirements for Data Users. ISAT

Deleted: the

Deleted: proper

Deleted: handling

Deleted: protected information

Deleted: related UH policies and procedures, and

Deleted: https://www.hawaii.edu/infosec/training.html¶

Deleted: p

Deleted: d

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

Deleted: ¶ Legitimate educational interest – The basis for granting access to an education record, which involves performing an ... [1]

Deleted: Institutional

Deleted: D

Deleted: se data

Deleted: APPLICABILITY ¶ This administrative procedure is applicable to:¶ ... [2]

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.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, … + Start at: 1 + Alignment: Left + Aligned at: 1" + Indent at: 1.25"

Formatted: Font color: Auto

Formatted: Normal, Indent: Left: 1", No bullets or numbering

Formatted: Indent: Left: 1", Hanging: 0.25"

Formatted: Heading 4

Formatted: Not Highlight

Deleted: Completion of the GCN and ISAT will be required before access to IT systems is granted.

Formatted: Heading 4, Indent: Left: 1.75"

Moved (insertion) [1]

Deleted: General Confidentiality Notice (GCN)¶

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

Deleted:

Formatted: Heading 4

Formatted: Heading 3, Indent: Left: 1", Hanging: 0.25"

Deleted: ¶

Deleted: <#>Individuals who do not have UH usernames must complete the Non-UH GCN version. http://www.hawaii.edu/uhdatagov/nonuh_gcn.pdf ¶ MANDATORY TRAINING AND CONTINUING EDUCATION REQUIREMENTS ¶

Formatted: Heading 4, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 1.5" + Indent at: 1.75"

Deleted: <#>Complete the Information Security Awareness Training (ISAT) before being granted access to Protected Data.Data Users will need to complete the Information Security Awareness Training (ISAT) and General Confidentiality Notice (GCN) before being granted access to protected data. ¶
Data Users with UH usernames must self-register and successfully complete the training modules. www.hawaii.edu/infosec/training.htmlInformation Security Awareness Training (ISAT)¶
Data Users with UH usernames must self-register and successfully complete the training modules. www.hawaii.edu/infosec/training.html ¶
Individuals who do not have UH usernames must contact the Data Governance Program to gain access to the training modules (datagov@hawaii.edu, 956-7487).¶ … [3]

Moved (insertion) [3]

Moved up [3]: <#>Data Users with UH usernames and successfully complete the training modules.

Moved down [2]: <#>Individuals who do not have contact the Data Governance Program to gain

Moved up [1]: <#>General Confidentiality Notice

Moved (insertion) [2]

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 Hawai'i (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

Deleted: ¶
The ISAT must be re-taken every two years.¶
The GCN must be re-acknowledged annually.¶
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 ISAT renewal and/or GCN re-acknowledgement are required. A final reminder will be sent to both parties a week in advance.¶
Access will be removed upon failure to complete either requirement within the specified expiration date(s).

Formatted: Heading 3, Indent: Left: 1", Hanging: 0.25"

Formatted: Heading 4, Numbered + Level: 1 + Numbering Style: a, b, c, … + Start at: 1 + Alignment: Left + Aligned at: 1.5" + Indent at: 1.75"

Deleted: [When app is ready, add details on how users will get access.]

Formatted: Heading 3

Deleted: <#>EXECUTIVE DATA STEWARD ROLES AND RESPONSIBILITIES¶
System and Campus Executive Data Stewards have 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 ¶
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 ISAT 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.¶
¶

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

Deleted: Academic Planning and Policy

V. References

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

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

Formatted: Indent: Left: 0", First line: 0.5"

Deleted: ¶

Formatted: Indent: First line: 0.5"

Approved:

_____ _____
David Lassner Date
President

Page 2: [1] Deleted	**Gordon**	**10/1/20 5:51:00 AM**
Page 2: [2] Deleted	**Gordon**	**9/14/20 8:49:00 AM**
Page 3: [3] Deleted	**Gordon**	**9/14/20 9:46:00 AM**

a.