Executive Policy, EP 2.214
Institutional Data Classification
Categories and Technical Guidelines

Executive Policy Chapter 2, Administration
Effective Date: February 2017
Dates Amended: October 2014
October 2014
October 2014
October 2014

Responsible Office: Office of the Vice President for Academic Planning and Policy and Information Technology/Chief Information Officer
Governing Board of Regents Policy: RP 2.202, Duties of the President
Review Date: February 2020
August 2017

I. Purpose

The objective of this executive policy is to organize UH Institutional Data into data classification categories based on different levels of security risk and penalties that may result from the inadvertent exposure and inappropriate disclosure of those data. To provide the framework for specific practices and procedures associated with systems and files that contain sensitive, personal, and confidential information (hereinafter referred to as "sensitive information") within the University of Hawai‘i System.

II. Definitions

A. Institutional Data – Data elements/data records which are created, received, maintained and/or transmitted by the University of Hawai‘i in the course of meeting its administrative and academic requirements.

B. Personally Identifiable Information (PII) – Data or information, or a combination of data or information that when considered together, would identify an individual. The level of security risk when managing PII varies from none to very high, depending on the data elements involved.

C. Physically Secured – The storage of electronic media or paper containing Institutional Data in a non-public, controlled area such as an area accessible only to a trusted, known group of individuals or in a locked room or file cabinet when there is no authorized individual present. Classrooms and lab areas are considered public locations.
D. **Protected Data — Institutional Data that are subject to security and privacy considerations that range from moderate to very high. In other words, all Institutional Data that are not considered public. Within the UH Institutional Data Classification Categories, protected data encompasses those that fall under the “restricted,” “sensitive,” and “regulated” categories. See section III-B for category descriptions.**

Selected data elements/data records that fall under the sensitive or regulated categories may be subject to federal, state, and local regulations or industry standards such as FERPA, HIPAA, PCI-DSS (Payment Card Industry Data Security Standard), National Industrial Security Program (NISPOM), and the Bioterrorism Special Agent Program. This policy is not intended to supercede those regulations, but to promote and reinforce them. Should a provision in this policy conflict with applicable state, federal, or local regulations, the applicable regulation takes precedence and will govern.

No policy-specific or unique definitions apply.

---

**III. Executive Policy**

A. **POLICY STATEMENT A. Philosophy**

B. **The University of Hawai‘i is committed to protecting the privacy and security of Institutional Data, one of its most valuable institutional assets.**

The University of Hawai‘i makes substantial use of personal and confidential information in achieving its mission. In the wrong hands, such information can be abused for improper and illegal activities. Identity theft provides the most visible but not the only example of how sensitive personal information can be misused. The University is committed to handle all sensitive information carefully and responsibly. The first tenet of the University’s philosophy is to limit the use of, storage of and access to sensitive information to situations where it is absolutely required for the operations of the institution. When balancing convenience of operations against the risk associated with unnecessary storage of sensitive information, the policy of the University shall be to limit any unnecessary storage to protect the interests of the individuals who have entrusted their information to the institution. Where sensitive information is absolutely required for the University’s operations, it must be adequately protected from improper exposure inside and outside the institution.
These tenets apply to information that may be used in any aspect of the University’s mission of teaching, learning, research, service and administration.

C. **DATA CLASSIFICATION CATEGORIES**

**B. Purpose**

1. This policy is intended to provide the framework for specific practices and procedures associated with systems and files that contain sensitive, personal and confidential information (hereinafter referred to as “sensitive information”) within the University of Hawaii System. The scope of this policy includes categorization, provision of access, storage, handling and destruction of such information. This specific policy does not address issues related to public information that may need to be protected from modification, corruption or loss, and does not address issues related to information that may be classified by governmental agencies through programs such as the National Industrial Security Program (NISPOM), or the Biotechnology Special Agent Program, which have their own requirements. This policy applies to all University departments regardless of funding, including RCUH service-ordered projects.

2. 

3. Nothing in this policy is intended to constrain open and direct communication by the University Community, including through electronic means. Such communications may include the exchange of sensitive information about an individual to that individual or others as may be necessary for institutional purposes and in compliance with applicable privacy regulations.

4. 

5. **C. Data Categorization**

6. 

7. For purposes of this policy, data is simply categorized in two ways.

8. 

9. 1. Public Information

10.
11. Public information is any information to which access is not restricted.

13. **Sensitive Information**

15. Sensitive information is information that is subject to privacy considerations or has been classified to as confidential and subject to protection from public access or inappropriate disclosure.

17. Examples of Sensitive Information include but are not limited to:

19. a. Student records, including anything protected by the Family Educational Rights and Privacy Act (FERPA)

20. b. Health information, including anything covered by the Health Insurance Portability and Accountability Act (HIPAA)

21. c. Personal financial information such as credit card information, bank account information, debit card information, etc.

22. d. Job applicant records (names, transcripts, etc.)

23. e. Social Security Numbers

24. f. Dates of birth

25. g. Private home addresses and phone numbers

26. h. Driver license numbers and State ID Card numbers

27. i. Access codes, passwords and PINs for online information systems

28. j. Answers to "security questions" such as "what is the name of your favorite pet?"

29. k. Confidential information subject to attorney-client privilege
30. Detailed information about security systems (physical and/or network)

31. Confidential salary information

32. Information made confidential by a collective bargaining agreement

33. Public – Institutional Data where access is not restricted and is subject to open records requests.

This category includes: 1) student directory information as defined in UH's Administrative Procedure, AP7.022, Procedures Relating to Protection of the Educational Rights and Privacy of Students; and, 2) public employee information as defined in Hawai'i Revised Statutes (HRS) 92F-12 under the Uniform Information Practices Act. See Attachment 1 for examples.

34. Restricted – Institutional Data used for UH business only. Restricted data will not be distributed to external parties except under the terms of a written memorandum of agreement or contract. Data is maintained in a physically secured location. See Attachment 1 for examples.

35. Sensitive – Institutional Data subject to privacy or security considerations or any Institutional Data not designated as public, restricted, or regulated. Data is maintained in a physically secured location. See Attachment 1 for examples.

36. Regulated – Institutional Data where inadvertent disclosure or inappropriate access requires a breach notification in accordance with HRS §487N or is subject to financial fines. Social Security Number (SSN) and personal financial information fall within this category. Data is maintained in a physically secured location. See Attachment 1 for examples. For breach notification procedures, refer to UH Administrative Procedure 2.xxx (forthcoming).

Attachment 1 is not intended to be an exhaustive list but is an attempt to capture the more common data elements/data records used by the University to conduct its daily business. Institutional Data that are not listed shall be considered sensitive until otherwise determined. For guidance on Institutional Data not listed in Attachment 1, email datagov@hawaii.edu.
D. DATA MANAGEMENT GUIDELINES AND BEST PRACTICES

1. The Social Security Number (SSN) may will not be used as an identifier in any University information system and its use as an identifier shall be phased out in all existing systems. This includes use of the SSN as an optional identifier in legacy systems, which is similarly prohibited. The SSN may be included as a data element in an information system only where it is required for financial processing (e.g., payroll or student tax reporting) or other uses consistent with federal and state law. For example, the University may require the use of the SSN as part of the essential process of identifying when a person has contact with the university using different names, or to distinguish between individuals who have the same name. In situations such as these, the SSN may be used only as a data element and not as an identifier. The SSN must be purged from all other information systems.

2. Documents or records that contain Institutional Data from multiple classification categories will be managed according to the highest level of classification.

37. Individuals with access to protected data must complete mandatory training and continuing education requirements. Refer to UH Administrative Procedure 2.xxx for details (forthcoming).

38. Lists of student directory data (which are categorized as public) shall not be released to third parties except under the terms of a contract or memorandum of agreement. Refer to UH Administrative Procedure AP7 022, Procedures Relating to Protection of the Educational Rights and Privacy of Students which is UH’s interpretation of the federal Family Educational Rights and Privacy Act.

39. When displaying protected data in aggregate (i.e., not on an individualized basis), appropriate care must be taken to protect the identities of the individuals such that a person cannot identify any of the individuals with reasonable certainty. Note that data elements may not be personally identifiable when considered alone. However, when considered in combination with other data elements, they may reveal the identity of an individual. For example, average GPA by major may be reported. But if ethnicity is added, and there is only one individual within an ethnicity category, the identity of the individual and his/her GPA may be revealed.
Therefore, appropriate consideration and measures must be taken when considering the mix of data elements being shared and highest level of data classification category involved. Guidelines and best practices on the reporting of Institutional Data, such as managing small cell sizes, are available at www.hawaii.edu/uhdatagov/ (forthcoming).

40. Notwithstanding any records retention policies, paper and electronic transaction records containing regulated data, such as SSN or personal financial information, will be redacted or removed/destroyed when considered nonessential.

E. DATA SECURITY MEASURES

1. Technical guidelines for each data classification category shall be followed to prevent the inadvertent exposure and inappropriate disclosure of Institutional Data that are considered protected data. Technical guidelines by type of storage device are available at www.hawaii.edu/infosec/techguidelines (forthcoming). These technical guidelines are part of the UH Information Security Program which is administered by the Information Technology Services Information Security Team.

   Information Technology Services shall have full authority to require that all servers be registered and to implement standard measures, such as network and server scanning, to identify security weaknesses in any University information system or network that may compromise sensitive information or the operations and availability of institutional services.

2. Information Technology Services shall have authority to take such technical measures as are necessary to ensure the protection of sensitive information stored or transmitted, whether intentionally or unintentionally, on University systems and networks, including but not limited to immediate disconnection of compromised systems from the University network. As stated in Executive Policy EP2.215, Information Technology Services (ITS) has the full power to enforce technical measures to ensure the security and confidentiality of protected data that are stored or transmitted, whether intentionally or unintentionally, on University systems and networks, including but not limited to immediate disconnection of compromised systems and devices from the University network.
3. require that all servers operating on the University network servers be registered in the server registration database and regularly scanned for sensitive information and vulnerabilities. All servers shall be protected with standard measures. ITS has the authority to conduct network and device scanning and to implement standard measures, such as network and server scanning, to identify security weaknesses in any University information system, device, or network that may compromise sensitive information or the operations and availability of institutional services.

ITS also has the authority to require all servers operating on the University network be regularly scanned for sensitive information vulnerabilities and be protected in accordance with appropriate data security guidelines based on data classification categories. ITS also has the authority to enforce technical measures to ensure the protection of protected data that are stored or transmitted, whether intentionally or unintentionally, on University systems and networks, including but not limited to immediate disconnection of compromised systems and devices from the University network.

4. To better protect the University's Institutional Data, ITS may require departments/units/programs to periodically report on the data element/records that they manage. Reporting requirements administered by ITS include PII and Health Insurance Portability and Accountability Act (HIPAA) surveys and server registrations.

The PII survey is part of an HRS §487N-7 requirement where Under Hawaii Revised Statutes §487N-7 UH, the University must annually prepare a report describing the all information systems that contain personal information. UHITS is responsible for Information Technology Services has been designated as the submitter of this report and maintains a secure online system for units to report all such systems. Chancellors and Vice Presidents are responsible to ensure that all units under their purview report all systems containing sensitive protected data information and update the information at least annually.

5. Chancellors and Vice Presidents should also designate an individual in their organization who will be responsible on their behalf for the units personal information protection and compliance program which includes ensuring that the PII the survey is completed accurately and assuractively for the elimination
ofing all unnecessary storage of personal information, and for implementing appropriate security measures for systems under their purview that must retain sensitive information for essential University operations. This individual's name and contact information shall be sent to the Vice President of Information Technology and the Chief Information Officer/Chief Information Security Officer. These designated individuals will form the systemwide Data Security Leadership Council.

D. Sensitive Information of Special Concern

1.

2. Social Security Number

3.

4. The Social Security Number (SSN) may not be used as an identifier in any University information system and its use as an identifier shall be phased out in all existing systems. This includes use of the SSN as an optional identifier in legacy systems, which is similarly prohibited. The SSN may be included as a data element in an information system only where it is required for financial processing (e.g., payroll or student tax reporting) or other uses consistent with federal and state law. For example, the University may require the use of the SSN as part of the essential process of identifying when a person has contact with the university using different names, or to distinguish between individuals who have the same name. In situations such as these, the SSN may be used only as a data element and not as an identifier. The SSN must be purged from all other information systems.

5.

6. The UH Number is the University’s unique identifier and should be used as the identifier in all University information systems.

7.

8. Personal Financial Information

9.
10. In order to protect the personal financial information of those with whom the University does business, the University has adopted administrative procedures that apply to all paper-based and electronic credit card transactions.

12. Administrative Procedure A3.711 “Credit Card Program” applies to all processing of credit card transactions by University programs.

14. In addition, Administrative Procedure A3.711 “Electronic Payments via University Websites” must be followed for all electronic transaction processing (eCommerce). To provide a secure eCommerce environment, the University has implemented a PCI-DSS compliant, hosted eCommerce management system that supports a payment processing service for a variety of eCommerce applications. Campuses and departments that want to accept online payments are required to process all sales transactions through this eCommerce management system. Exceptions may be granted to only those departments that provide evidence to the Bursar or his/her designee, that the University’s eCommerce management system cannot meet the department’s business needs, and that the alternate system complies with University and PCI-DSS requirements for security.

16. Notwithstanding any records retention policies, paper and electronic transaction records shall be redacted of personal financial information as defined in this policy.

18. E-Roles & Responsibilities in Information Security
22. Institutional information resources shall have one or more designated stewards. Institutional information resource 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 & Analysis Office (IRAO) and Information Technology Services (ITS) also have stewardship responsibility for institutional information. Producers and collectors of original data, e.g., researchers, are considered the stewards of those information resources.

23.

24. Information resource stewards are responsible for classification of their data consistent with applicable federal, state and UH policies, standards, regulations and laws. Information resource stewards are also responsible for minimizing the use, storage and exposure of sensitive information, especially the Social Security Number. They shall restrict the use and exposure of such information to those specific situations where it is essential and appropriate.

25.

26. Information resource stewards may have multiple responsibilities if they also serve as data custodians.

27.

28. 2. Data Custodians

29.

30. 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 individual who downloads or stores sensitive information onto a computer or storage device becomes a data custodian through that act.

31.
32. Data custodians are responsible for implementing and administering controls over the resources according to policies and parameters provided by the information resource stewards. Data custodians are responsible for the technical safeguarding of sensitive information, including ensuring security transmission and providing access control systems approved by the information resource steward to prevent inappropriate disclosure.

33. 

34. All data custodians for sensitive information are required to sign the UH General Confidentiality Notice (see Attachment I).

35. 

36. 3. Users

37. 

38. Users are any individuals who are granted access to sensitive information as required to perform their professional responsibilities.

39. 

40. All individuals who are provided with access to sensitive information must be briefed on their responsibilities and agree to accept these responsibilities. Users are responsible for understanding and complying with all applicable University policies, procedures, and standards for dealing with sensitive information and its protection.

41. 

42. Specific questions about the appropriate handling or usage of a specific information resource should be directed to the information resource steward.

43. 

44. All users granted access to sensitive information are required to sign the UH General Confidentiality Notice (see Attachment I).

45. 

46. F. Collection of Sensitive Information
47.

48. Sensitive information is only collected and stored when essential to the functions and operations of the institution. Information resource stewards shall minimize the use of sensitive information in the systems and services for which they are responsible. When balancing convenience of operations against the risks associated with unnecessary storage of sensitive information, the policy of the University shall be to protect the interests of the individuals by limiting the collection and storage of sensitive information.

49.

50. G. Mandatory Reporting of All Information Systems with Sensitive Information

51.

52. Under Hawai‘i Revised Statutes §487N-7, the University must annually prepare a report describing all information systems that contain personal information. UH Information Technology Services has been designated as the submitter of this report and maintains a secure online system for units to report all such systems. Chancellors and Vice Presidents are responsible to ensure that all units under their purview report all systems containing sensitive information and update the information at least annually. Chancellors and Vice Presidents may also designate an individual in their organization who will be responsible on their behalf for the survey’s completion and accuracy, for eliminating all unnecessary storage of personal information, and for implementing appropriate security measures for systems under their purview that must retain sensitive information for essential University operations.

53.

54. H. Access to Sensitive Information

55.

56. 1. Granting of Access

57.
58. Individuals may only be granted access to sensitive information by an information resource steward or their designee in support of necessary functions or operations. Access to sensitive information is granted by stewards on a "need-to-know" basis to as limited a portion of sensitive information as is feasible to allow individuals to be effective and efficient in their activities.

59.

60. 2. Access Procedures

61.

62. For multi-user systems, access procedures must be implemented by information resource stewards and data custodians before access is granted to others. Access procedures must address:

63.

64. a. How access is requested by a prospective user or their supervisor;

65. b. Types of access available including read, write, copy and extend access to third parties;

66. c. How access requests are reviewed and approved;

67. d. How those who are granted access are advised of their responsibilities and agree to accept them

68. (Attachment I, UH General Confidentiality Notice;

70. may be used for this purpose);

71. e. How mandatory information security training will be provided to all users, minimally, at the time they are granted access to sensitive information;

72. f. How the system will ensure the use of "strong" passwords, idle-time logout, and other best practices to ensure security;

73. g. Whether or how access is limited only to the portions of sensitive information required by the individual;
h. How access is revoked in a timely manner when no longer required;

i. How access is reviewed on a regular basis, and

j. Availability of audit trails for when, how and to whom access was granted.

Access by third parties to sensitive information may only be granted by the information resource steward, not by other users. Access by third parties must be granted through contracts or memoranda of agreement that include appropriate language to ensure protection of UH-sensitive information by the third party. The third parties shall agree to comply with all applicable federal, state and local laws, regulations and ordinances, and University policies pertaining to information designated as private, protected, sensitive or confidential by law or by the University, including, but not limited to, E2.210 (Use and Management of Information Technology Resources), E2.214 (Security and Protection of Sensitive Information), A7.022 (Procedures Relating to Protection of the Educational Rights and Privacy of Students), Hawaii Revised Statutes (HRS) §487J (Social Security Number Protection), HRS §487N (Security Breach of Personal Information), HRS §487R (Destruction of Personal Information Records), and Act 10, Part V, 2009 Special Session, Session Laws of Hawaii. Please see http://www.hawaii.edu/infosec/a2.214-techguide.html for suggested contract or memorandum language.

I. Transmission of Sensitive Information

Whenever sensitive information is transmitted the sender must take care to protect that information and inform the recipient(s), including those involved in the delivery process, that the transmission contains sensitive information and must be protected.
1. Security of Paper Transmissions

When transmitting sensitive information on paper (via hardcopy), the sender shall mark the envelope as "CONFIDENTIAL" as appropriate to minimize the chance of unnecessary exposure and shall similarly mark the documents as "CONFIDENTIAL" when feasible and appropriate.

2. Security of Digital Transmissions

Sensitive information shall be strongly encrypted whenever transmitted over public networks or carriers in digital form. This includes the transmittal of sensitive information via email, file transfers (SFTP), web transactions (HTTPS), instant messaging or terminal login sessions. The UH "fileDrop" service provides a secure mechanism for exchange of sensitive information.

3. Security of Fax Transmissions

When transmitting sensitive information by facsimile (fax), the sender shall ensure that the information is promptly retrieved and properly protected at both the sending and receiving locations, with telephone/email confirmation as appropriate.

4. Email and Sensitive Information

Given the very real possibility of an email message going astray due to human error or otherwise, transmission of sensitive information by email is strongly discouraged unless protected by-
strong personal end-to-end encryption (such as PGP, GPG or similar tools). Exchange of sensitive information over networks can instead be done using a secure file exchange service, such as the UH "filedrop" utility, which enables the exchange of information using strong end-to-end encryption to or from members of the UH community.

104. When it is necessary to transmit sensitive information by standard email, the sender shall absolutely minimize the inclusion of sensitive information and take special care to ensure that the information is only received by authorized users. Both sender and receiver shall delete all copies of the sensitive information as soon as practicable, and the sender shall include a notice informing any recipient that the message contains sensitive information and requesting appropriate handling. A sample is provided as Attachment II. Similar language shall be used when transmitting any sensitive information via the "filedrop" service or other means.

105.

106. J. Use and Storage of Sensitive Information

107.

108. 4. Limited Use and Storage

109.

110. Sensitive information should be stored only where it is specifically required and in as few systems as possible.

111.

112. 2. Security of Systems with Sensitive Information

113.

114. Systems on which sensitive information is stored must minimally comply with all basic computer security standards, including diligent attention to application of all available security patches to operating systems and software, maintenance of up-to-date antivirus protection, implementation of secure password controls, etc.
Standard logs must be maintained, minimally of all access to files, with a retention period not less than one year.

115.

116. Unencrypted sensitive information shall be stored only on systems that are housed in secure and controlled environments. Where desktop systems can access sensitive information, they must not be set to login automatically without entry of a password, must not be left logged in on an unattended basis, and must not be available for casual perusal by unauthorized individuals.

117.

118. 3. Encryption and Physical Security of Sensitive Data in Mobile Formats and Storage in Cloud Environments

119.

120. Sensitive information stored on any environment, system or media that is subject to loss or theft—including laptops, USB drives, diskettes, CDs/DVDs, personal computers, departmental servers, and cloud environments—must be encrypted whenever not in active use.

121. Encryption is highly recommended for all other systems as well, whenever feasible. Systems susceptible to theft should also be physically secured, e.g., with use of secure laptop cables, whenever possible.

122.

123. 4. Decoupling of Personal Information

124.

125. Whenever possible, such as for any research studies, sensitive data must be de-coupled from all personally identifiable information. If it is necessary to maintain such linkages, a unique identifier should be used to “crosswalk” sensitive research information back to personal identities and the crosswalk table itself shall be protected as sensitive information and encrypted separately from the data.

126.
5. Security of Non-Electronic Information

Paper documents and files containing sensitive information must be secured at all times. Such documents shall not be left in open view on desks and when not in use must be stored in secured areas or locked files with access limited to authorized users.

K. General Purpose Servers

General purpose servers used by faculty, staff and students may represent a risk to the protection of sensitive information since sensitive information may be inadvertently or unintentionally stored in a manner that allows unauthorized access. For this reason, all servers on University networks must be registered and regularly scanned for sensitive information and vulnerabilities. Information Technology Services shall be responsible to create and maintain a registration database and services to support the protection of all servers from misuse that may endanger sensitive information.

L. Disposal of Media Containing Sensitive Data

When disposing of media containing sensitive information the custodian must ensure that information is unrecoverable.

M. Erasable Media

Electronic and magnetic media such as hard drives, diskettes, magnetic tapes and optical tapes must be erased using secure deletion tools before transfer or disposal.
2. Unerasable or Unerased Media

Media that are not or cannot be securely erased, such as USB-drives, CDs and DVDs, must be physically destroyed before disposal.

3. Paper

Paper documents and printouts containing sensitive information must be shredded before disposal, ideally using a crosscut shredder.

4. Contracting for Disposal

These requirements may be fulfilled by contracting with a professional disposal firm engaged in the business of record destruction using methods consistent with this policy, provided that the data custodian conducts appropriate due diligence on the company. State law (Hawaii Revised Statutes §487R-2) provides that such due diligence may include: reviewing an independent audit of the company; checking references and requiring independent certification; or reviewing the company’s policies and procedures.

M. Multi-Function Printers, Copiers, Scanners and Fax Machines

Modern printers, copiers, scanners and fax machines generally utilize digital storage and communications capabilities that can present security vulnerabilities when not properly and actively managed.
158.

159. 1. Settings

160.

161. Whenever possible, devices shall be configured to encrypt all data.

162.

163. Security settings shall be configured and maintained to restrict access to the smallest practicable set of users and network locations to prevent intrusions and compromise.

164.

165. 2. New Devices:

166.

167. All new devices shall be purchased/leased with disk encryption and secure data overwriting capabilities.

168.

169. 3. Disposal

170.

171. Disposing of a printer, copier, scanner or fax machine that has ever been used with sensitive information shall be treated like disposal of a computer with a hard drive. The hard drive must be securely wiped before you give the device away or sell it. Or if the device’s hard drive is removable, remove the drive entirely and have it securely destroyed.

172.

173. 4. Use of Public Devices:

174.

175. Public or unsecured/unknown printers/copiers/scanners/faxes shall not be used for documents containing sensitive information.
177. N. Personnel Issues & Violations

179. 1. Termination

181. In case of employer-initiated termination of employment of personnel with access to sensitive information, such access may, as circumstances warrant, be revoked immediately at the time of notification, or as soon as may be consistent with an applicable collective bargaining agreement. In all other cases, upon termination of employment of personnel with access to sensitive information, such access shall be revoked at the time of separation. The appointing authority shall be responsible for initiating the revocation of employee access to all sensitive information when it is no longer required.

183. 2. Violations

185. Violation of this policy may result in disciplinary action up to and including discharge in accordance with University policies and procedures and applicable collective bargaining agreements. Violators may also be subject to applicable civil and/or criminal penalties.

187. 3. Personnel Background Checks

189. Prior to granting an employee access to sensitive information, an appropriate background check should be performed by the appointing authority in accord with applicable policies and procedures.
191. O—Notice and Reporting of Security Breaches

192.

193. In accordance with state law, the University shall notify all affected individuals in the event of a security breach involving personal information and must also report the breach to the Legislature. Preparation and transmission of notices and reports and responding to all inquiries and concerns from affected individuals is the responsibility of the Chancellor or Vice President with purview over the breached information system, including responsibility for all associated costs.

194.

195. 1—Definition of Personal Information

196.

197. In accordance with Hawaii Revised Statutes §487N-1, personal information means an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver’s license number or Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual’s financial account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

198.

199. 2—Definition of Security Breach

200.

201. In accordance with Hawaii Revised Statutes §487N-1, a security breach means an incident of unauthorized access to and acquisition of unencrypted or unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur and creates a risk of harm to a person, or an incident of unauthorized access to and—
acquisition of encrypted records or data containing personal information along with the confidential process or key.

202.

203. 3. Timely Notice

204.

205. Notices to affected individuals shall be made without unreasonable delay, subject to any delays requested by law enforcement agencies to support legal investigations or broader security concerns and consistent with any immediate need to restore and ensure the integrity of any breached information system(s).

206.

207. 4. Contents of Notice

208.

209. In accordance with Hawai‘i Revised Statutes §487N-2, notices shall be clear and conspicuous and shall include a description of the following: (1) The incident in general terms; (2) The type of personal information that was subject to the unauthorized access and acquisition;

210. (3) How the personal information will be protected from further unauthorized disclosure; (4) A telephone number and email address that can be called for further information and assistance; and (5) General advice on protection against identity theft that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports. Sample notices are available from the UH Information Security Officer in ITS. Notices should be reviewed before distribution by both the UH Office of General Counsel and the Information Security Officer. UH Means of Notice

211.

212. In accordance with Hawai‘i Revised Statutes §487N-2, notice may be provided by any or all of: (1) Written notice to the last available address the University has on record; (2) Electronic mail notice, for those persons for whom the University has a valid electronic mail-
address and who have agreed to receive communications electronically after being given notice of their rights and options as provided by law. (3) Telephonic notice, provided that contact is made directly with the affected persons. Substitute notice may be provided if the cost of providing notice would exceed $100,000 or the number of persons to be notified exceeds two hundred thousand, or if the University does not have sufficient contact information or consent to satisfy options (1), (2), or (3) above. Substitute notice shall consist of all the following: (a) Electronic mail notice when the University has an electronic mail address for the subject persons (even if consent has not been provided); (b) Conspicuous posting of the notice on the University website; and (c) Notification to major statewide media.

5. Legislative Reporting Requirements

In accordance with Hawai‘i Revised Statutes §487N-4, the University must also submit a written report to the legislature within twenty days after discovery of a security breach at the University. This report must detail information relating to the nature of the breach, the number of individuals affected by the breach, a copy of the notice of security breach that was issued, the number of individuals to whom the notice was sent, whether the notice was delayed due to law enforcement considerations, and any procedures that have been implemented to prevent the breach from reoccurring. This report must be prepared in draft form by the unit that experienced the breach and submitted to the UH Information Security Officer in ITS for review. The UH Information Security Officer can also provide sample reports. Final reports are transmitted by the UH Office of External Affairs and University Relations.

6. Breaches Involving Credit Card Information
221. Any breach that involves credit card information must also be immediately reported to the UH Treasury Office, which may have additional reporting requirements. Any resultant fines shall be the responsibility of the Chancellor or Vice President with purview over the breached information system.

222.

223. 7. Breaches Involving Student Information

224.

225. Any breach of student information must be reported to the campus FERPA official or designee in order to ensure that all U.S. Department of Education guidelines and reporting requirements pertaining to protection of educational records are followed.

226.

227. The U.S. Department of Education’s Recommendations for Safeguarding Education Records specifies that an educational institution should consider the following when there is an unauthorized release of education records:

228.

229. a. Report the incident to law enforcement authorities.

230. b. Determine exactly what information was compromised, i.e., names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.

231. c. Take steps immediately to retrieve data and prevent any further disclosures.

232. d. Identify all affected records and students.

233. e. Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.

234. f. Determine whether institutional policies and procedures were breached, including organizational requirements governing access.
(user-names, passwords, PINS, etc.); storage; transmission; and destruction of information from education records.

235. (1.) Determine whether the incident occurred because of a lack of monitoring and oversight.

236. (2.) Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.

237. (3.) Notify students that the Department's Office of Inspector General maintains a website describing steps students may take if they suspect they are a victim of identity theft at:

238. http://www.ed.gov/about/offices/list/oig/misuse

239. didtheft.html; and

240. http://www.ed.gov/about/offices/list/oig/misuse

241. victim.html.

242.

243. P. Technical Guidance

244.

245. Information Technology Services shall provide technical guidance on recommended means of protecting digital information as required to comply with this policy including but not limited to:

246.

247. • Password selection and protection

248.

249. • Securing personal computers and servers that run commonly used computer operating systems

250.

251. • Exchanging files securely between members of the UH community
252.

253. Secure protocols for login, file transfer and web transactions

254.

255. Encrypting sensitive information stored on systems that run uncommonly used personal computer operating systems

256.

257. Erasing hard disks on personal computers prior to transfer or disposal

258.

259. Securing network-connected multi-function printers and related devices

260.

261. Protection of servers that contain sensitive information including secure login practices, log practices, encryption and/or firewalls

262.

263. This guidance shall be provided on a UH system web site and updated regularly with currently feasible best practices.

264.

265. Q. Technical Protections and Enforcement

266.

267. Information Technology Services shall have full authority to require that all servers be registered and to implement standard measures, such as network and server scanning, to identify security weaknesses in any University information system or network that may compromise sensitive information or the operations and availability of institutional services.

268.
269. Information Technology Services shall have full authority to take such technical measures as are necessary to ensure the protection of sensitive information stored or transmitted, whether intentionally or unintentionally, on University systems and networks, including but not limited to immediate disconnection of compromised systems from the University network.

270.


272.

6. The UH Board of Regents approved a Federal Trade Commission (FTC) Red Flags Rule Identity Theft Prevention Program for UH. The program falls under pursuant to the FTC’s Red Flags Rule, 16 CFR Part 681, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. The purpose of the Identity Theft Prevention Program is to detect, prevent and mitigate identity theft in connection with a “covered account” which involves the University extending credit to an individual to obtain goods or services, or accepting a deposit from the individual, and involves multiple payments or transactions. See this is incorporated herein as Attachment II for details.

7. Personnel related actions

a. Terminations

In the case of an employer-initiated termination of employment of personnel with access to protected information, such access may, as circumstances warrant, be revoked immediately at the time of notification, or as soon as may be consistent with an applicable collective bargaining agreement. In all other cases, upon termination of employment of personnel with access to protected information, such access shall be revoked at the time of separation. The appointing authority shall be responsible for initiating the revocation of employee access to protected information when it is no longer required.

b. Violations
Actions that result in the inadvertent exposure or inappropriate disclosure of protected data may result in disciplinary action up to, and including, discharge in accordance with University policies and procedures and applicable collective bargaining agreements. Violators may also be subject to applicable civil and/or criminal penalties.

c. Personnel Background Checks

Prior to granting an employee access to protected data, an appropriate background check may be performed by the appointing authority in accord with applicable policies and procedures.

IV.

V.

VI. S.-Precedence of State and Federal Law

VII.

VIII. To the extent that any provision in this policy conflicts with applicable state or federal laws, the applicable laws take precedence and will govern.

IX.

X.

XI. Delegation of Authority

There is no policy-specific delegation of authority.

XII. Contact Information

Offices of the Vice President for Academic Planning and Policy and Information Technology/Chief Information Officer
Sandra Furuto, 956-7487, yano@hawaii.edu
Office of the Vice President for Information Technology/Chief Information Officer
telephone number: 808-956-2800 or email ssmith28@hawaii.edu
XIII. References

Executive Policy EP2.215, Institutional Data Governance, provides the overall structure for the University's data governance program. It describes the fundamental principles and best practices governing the management and use of Institutional Data and stewardship roles and responsibilities. Executive Policy EP2.214 is a supporting policy on data governance and security.

Other University of Hawai'i executive policies, State of Hawai'i Revised Statutes, and external regulations that relate to data governance and Institutional Data classification categories are available at: www.hawaii.edu/infosec/policies.html

A. Link to superseded Executive Policies in old format
   https://www.hawaii.edu/policy/archives/ep/

B. Link to Administrative Procedures in old format

Approved:

_________________________ October 31, 2014
David Lassner Date
President