David Lassner
President

UNIVERSITY of HAWAI'I® SYSTEM

DEPT. COMM. NO. 314

February 17, 2017

The Honorable Ronald D. Kouchi,
President and Members of the Senate
Twenty-Ninth State Legislature
Honolulu, Hawai'i 96813

The Honorable Joseph Souki, Speaker
and Members of the House of Representatives
Twenty-Ninth State Legislature
Honolulu, Hawai'i 96813

Dear President Kouchi, Speaker Souki, and Members of the Legislature:

For your information and consideration, the University of Hawai'i is transmitting one copy of the Report to the Legislature on the Security Breach at Kapi'olani Community College, University of Hawai'i (Section 487N-4, Hawai'i Revised Statutes) as requested by the Legislature.

In accordance with Section 93-16, Hawai'i Revised Statutes, this report may be viewed electronically at: http://www.hawaii.edu/offices/government-relations/2017-legislative-reports/.

Should you have any questions about this report, please do not hesitate to contact Stephanie Kim at 956-4250, or via e-mail at scskim@hawaii.edu.

Sincerely,

David Lassner
President

Enclosure

2444 Dole Street, Bachman Hall
Honolulu, Hawai'i 96822
Telephone: (808) 956-8207
Fax: (808) 956-5286
An Equal Opportunity/Affirmative Action Institution

UNIVERSITY OF HAWAIʻI SYSTEM REPORT

REPORT TO THE 2017 LEGISLATURE

Report on Security Breach
at the University of Hawaiʻi, Kapiʻolani Community College

HRS 487N-4

February 17, 2017

SELF-REPORT ON
INFORMATION SECURITY INCIDENT

DISCOVERY	February 01, 2017
LOCATION	University of Hawai‘i, Kapi‘olani Community College (KCC)
NATURE	Paper-based W-2 with Sensitive Information

INCIDENT DESCRIPTION

On February 01, 2017, an employee (custodian of W-2) from the Health Science Department self-reported to KCC a possible breach of ninety-two (92) employee paper copies of W-2 that contained sensitive information.

An internal investigation was immediately commenced, and initial determinations were made that the missing W-2 were left on a typewriter in the departmental workroom Monday mid-morning, January 30, 2017. The files were discovered missing on Tuesday morning, January 31, 2017.

The departmental workroom is located in the Health Science Department office that is accessible by the Health Science faculty, staff, and student help during normal working hours (8:00am-5:00pm Monday-Friday) and by the Health Science faculty and staff during after hours. The door to the office is locked when the main office is not occupied. The files went missing between approximately 10:30am Monday, January 30, 2017 – 9:00am Tuesday, January 31, 2017. KCC was unable to identify which faculty, staff or student help accessed the departmental workroom during this time.

While the University's investigation is ongoing, interviews of all relevant faculty and staff have been completed. Aside from the employee who made the copies (apparently for the convenience of employees who might lose their original W-2) and inadvertently left the W-2 copies on the typewriter, no one had seen the files on the typewriter, or recalls any strangers walking through the area during the relevant timeframe. Multiple intensive searches did not recover the missing documents.

In total, ninety-two (92) individuals have been identified as being "at-risk" because the combination of their full name and Social Security Number was contained in the missing documents. All 92 individuals are currently employed by KCC, and were notified in writing on February 8, 2017. A copy of the notification letter is included as Attachment A. At this time, the University has no evidence or confirmation that the information has been exposed, that illegal use of the personal information has occurred, or that the personal information was acquired for illegitimate purpose.

The University's policies are clear that "sensitive" information (including social security numbers) is to be protected, and unnecessary duplication and unsecured

storage of sensitive information violate Section III of UH Executive Policy 2.214 (Attachment B), which states in relevant part:

> F. Collection of Sensitive Information
>
> Sensitive information is only collected and stored when essential to the functions and operations of the institution. . . . 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.
>
> *****
>
> J. Use and Storage of Sensitive Information
>
> *****
>
> 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.

KCC provides workshops at least twice a semester that cover this policy on collecting sensitive information. Training on collecting sensitive information is also provided during new employee orientation at the beginning of every semester.

In addition, in circulating W-2 forms annually, the University provides clear instructions regarding the due diligence expected in safeguarding sensitive information. See Attachment C.

Again, written notification has been sent to all 92 individuals at their US postal mailing address on record, and all are being provided two (2) years of credit monitoring services through Experian.

KCC has developed an Action Plan to prevent further recurrence of these types of incidents that includes refresher notifications to all custodians of W-2 about existing State law and University policies regarding such sensitive documents. A summary of this plan, including an implementation timeline, is included as Attachment D.

ATTACHMENT A

Office of the Chancellor

UNIVERSITY of HAWAI'I®
KAPI'OLANI
COMMUNITY COLLEGE

February 7, 2017

First Name, Last Name
Mailing Address
City, State, Zip Code

Dear _____,

We are contacting you to inform you of a recent incident that may put you at risk for identity theft or fraud and to provide guidance on steps we are taking and how you can protect yourself from financial harm associated with this and other potential risks.

On February 1, 2017, Kapi'olani Community College was notified by an employee from the Health Science Department of a possible exposure of W-2 forms that contained sensitive information including your name and social security number. A thorough search and interviews of all relevant faculty and staff were conducted. As of this writing, the paper documents have not been located.

While the University's internal investigation is ongoing, we are providing this notice to all individuals whose personal information may have been exposed. At this time, the College has no evidence or confirmation that the information has been exposed, that illegal use of the personal information has occurred, or that the personal information was acquired for illegitimate purpose.

To help protect you in the event your information falls into the wrong hands, we will provide you with two years of credit monitoring at no cost to you through Experian. Instructions to activate your Experian credit monitoring service are included with this letter.

We also urge you to carefully monitor your credit card statements and to take heightened protective measures including:

- Review your bank and credit card statements regularly and look for unusual or suspicious activities.
- Obtain and carefully review your credit reports. You can order free credit reports from all three credit agencies at https://www.annualcreditreport.com
- Contact appropriate financial institutions immediately if you notice any irregularity in your credit report or any account. If your accounts or identity have been compromised, you may take immediate actions such as requesting refunds, closing accounts, placing your credit reports in a state of "fraud alert" or "freeze", and filing a police report.

Kapi'olani Community College is implementing additional security measures to ensure that a similar incident does not recur. The College is reviewing whether applicable policies or procedures were violated and will strengthen training of staff in secure record keeping and data management practices. We will also be minimizing the creation and use of paper copies of sensitive information.

We apologize for any inconvenience this incident has caused or may cause in the future. If you have any questions or need additional information, you may call (808) 734-9569 or email ohaganp@hawaii.edu

Sincerely,

Louise Pagotto
Interim Chancellor

4303 Diamond Head Road
Honolulu, Hawai'i 96816
Telephone: (808) 734-9565
Facsimile: (808) 734-9162
Website: www.kapiolani.hawaii.edu

ATTACHMENT A

Office of the Chancellor

UNIVERSITY of HAWAI'I®
KAPI'OLANI
COMMUNITY COLLEGE

Date

First Name, Last Name
Mailing Address
City, State, Zip Code

RE: Important Security and Protection Notification
Please read this entire letter.

Dear ____,

We are contacting you regarding a data security incident that we were informed about on February 1, 2017 at Kapi'olani Community College. This incident involved your name, address, and social security number. As a result, your personal information may have been potentially exposed to others. Please be assured that we have taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that fraud resolution support is needed then an Experian Fraud Resolution agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for two-years from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.experian.com/fraudresolution. You will also find self-help tips and information about identity protection at this site.

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through ProtectMyID® Alert as a complimentary two-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

Ensure that you **enroll by**: **02/16/19** (Your code will not work after this date.)
Visit the ProtectMyID website to enroll: **www.protectmyid.com/redeem**
Provide your **activation code**: **[code]**

4303 Diamond Head Road
Honolulu, Hawai'i 96816
Telephone: (808) 734-9565
Facsimile: (808) 734-9162
Website: www.kapiolani.hawaii.edu

If you have questions about the incident, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-371-7902 by **02/16/19**. Be prepared to provide engagement number **PCXXXXX** as proof of eligibility for the fraud resolution services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH PROTECTMYID MEMBERSHIP:

A credit card is **not** required for enrollment in ProtectMyID.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.experian.com/fraudresolution for this information.

We sincerely apologize for this incident and regret any inconvenience it may cause you.

Sincerely,

Louise Pagotto
Interim Chancellor

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ATTACHMENT B

Viewing Policy EP 2.214

Title

Security and Protection of Sensitive Information

Header

Executive Policy Chapter 2, Administration
Executive Policy EP 2.214, Security and Protection of Sensitive Information
Effective Date: October 2014
Dates Amended: April 2012, April 2009
Responsible Office: Office of the Vice President for Information Technology/Chief Information Officer
Governing Board of Regents Policy: RP 2.202, Duties of the President
Review Date: August 2017

I. Purpose

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

No policy specific or unique definitions apply.

III. Executive Policy

A. Philosophy

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.

B. Purpose

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 Hawai'i 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 Bioterrorism Special Agent Program, which have their own requirements. This policy applies to all University departments regardless of funding, including RCUH service ordered projects.

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.

C. Data Categorization

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

1. Public information

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

2. Sensitive Information

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

Examples of Sensitive Information include but are not limited to:

a. Student records, including anything protected by the Family Educational Rights and Privacy Act (FERPA)
b. Health information, including anything covered by the Health Insurance Portability and Accountability Act (HIPAA)
c. Personal financial information such as credit card information bank account information, debit card information, etc.
d. Job applicant records (names, transcripts, etc.)
e. Social Security Numbers
f. Dates of birth
g. Private home addresses and phone numbers
h. Driver license numbers and State ID Card numbers
i. Access codes, passwords and PINs for online information systems
j. Answers to "security questions" such as "what is the name of your favorite pet?"
k. Confidential information subject to attorney-client privilege
l. Detailed information about security systems (physical and/or network)
m. Confidential salary information
n. Information made confidential by a collective bargaining agreement

D. Sensitive Information of Special Concern

1. Social Security Number

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.

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

2. Personal Financial Information

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.

Administrative Procedure A8.710 "Credit Card Program" applies to all processing of credit card transactions by University programs.

In addition, Administrative Procedure A8.711 "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 ePayments are required to process all sales transactions through this eCommerce management system. Exceptions may be granted to only to 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.

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

E. Roles & Responsibilities in Information Security

1. Information Resource Stewards (may also be referred to as Data Stewards)

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.

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.

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

2. Data Custodians

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.

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.

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

3. Users

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

responsibilities.

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.

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

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

F. Collection of Sensitive Information

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.

G. Mandatory Reporting of All Information Systems with Sensitive Information

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.

H. Access to Sensitive Information

1. Granting of Access

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.

2. Access Procedures

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:

a. How access is requested by a prospective user or their supervisor;
b. Types of access available including read, write, copy and extend access to third parties;
c. How access requests are reviewed and approved;
d. How those who are granted access are advised of their responsibilities and agree to accept them (Attachment I, UH General Confidentiality Notice, may be used for this purpose);
e. How mandatory information security training will be provided to all users, minimally, at the time they are granted access to sensitive information;
f. How the system will ensure the use of “strong” passwords, idle-time logout, and other best practices to ensure security;

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), Hawai'i 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, 2008 Special Session, Session Laws of Hawai'i. Please see http://www.hawaii.edu/infosec/e2.214-techguide.html for suggested contract or memoranda 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.

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.

J. Use and Storage of Sensitive Information

1. Limited Use and Storage

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

2. Security of Systems with Sensitive Information

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 anti-virus 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.

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.

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

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.
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.

4. Decoupling of Personal Information

Wherever 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.

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.

1. 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 (Hawai'i 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.

1. Settings

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

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.

2. New Devices:

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

3. Disposal

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.

4. Use of Public Devices:

Public or unsecured/unknown printers/copiers/scanners/ faxes shall not be used for documents containing sensitive information.

N. Personnel Issues & Violations

1. Termination

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.

2. Violations

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.

3. Personnel Background Checks

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.

O. Notice and Reporting of Security Breaches

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.

1. Definition of Personal Information

In accordance with Hawai‘i Revised Statutes §487N-1, personal information means an individual's first name or first initial and last name in combination with anyone 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 Hawai‘i 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.

2. Definition of Security Breach

In accordance with Hawai‘i 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.

3. Timely Notice

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).

4. Contents of Notice

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;
(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

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

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.

7. Breaches Involving Student Information

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

The US 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:

a. Report the incident to law enforcement authorities.
b. Determine exactly what information was compromised, i.e.,names, addresses, SSNs, ID numbers, credit card numbers, grades, and the like.
c. Take steps immediately to retrieve data and prevent any further disclosures.
d. Identify all affected records and students.
e. Determine how the incident occurred, including which school officials had control of and responsibility for the information that was compromised.
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.
(1.) Determine whether the incident occurred because of a lack of monitoring and oversight.
(2.) Conduct a risk assessment and identify appropriate physical, technological, and administrative measures to prevent similar incidents in the future.

(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:
http://www.ed.gov/about/offices/list/oig/misuse
d/idtheft.html; and
http://www.ed.gov/about/offices/list/oig/misuse
d/victim.html.

P. Technical Guidance

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:

- Password selection and protection
- Securing personal computers and servers that run commonly used computer operating systems
- Exchanging files securely between members of the UH community
- Secure protocols for login, file transfer and web transactions
- Encrypting sensitive information stored on systems that run commonly used personal computer operating systems
- Erasing hard disks on personal computers prior to transfer or disposal,
- Securing network-connected multi-function printers and related devices
- Protection of servers that contain sensitive information including secure login practices, log practices, encryption and/or firewalls

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

Q. Technical Protections and Enforcement

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.

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.

R. Federal Trade Commission Red Flags Rule Identity Theft Prevention Program

The UH Board of Regents approved a Federal Trade Commission (FTC) Red Flags Rule Identity Theft Prevention Program 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. This is incorporated herein as Attachment III.

S. Precedence of State and Federal Law

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

IV. Delegation of Authority

There is no policy specific delegation of authority.

V. Contact Information

Subject Matter Experts
Steven Smith
steven.smith@hawaii.edu
956-2808

Office of the Vice President for Information Technology/Chief Information Officer telephone number: 808-956-2808 or email ssmith28@hawaii.edu.

VI. References

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

B. Link to Administrative Procedures in old format https://www.hawaii.edu/policy/archives/apm/sysap.php

VII. Exhibits and Appendices

No Exhibits and Appendices found

Approved

Signed	October 31, 2014
David Lassner	Date
President	

ATTACHMENT C

UNIVERSITY of HAWAI'I SYSTEM

Disbursing and Payroll Office

January 19, 2017

TO: Fiscal Administrators/Personnel Officers

FROM: James R. Kashiwamura, Director

SUBJECT: **FORM W-2 WAGE AND TAX STATEMENTS FOR 2016**

Employees' Wage and Tax Statements (Form W-2) for the calendar year 2016 will be distributed on Friday, January 27, 2017. W-2 forms for ALL EMPLOYEES can be picked up at the Financial Management Office (FMO) Conference Room, 1402 Lower Campus Road, Building H, Room 37 from 8:00am. Ensure that your runner knows the pick-up (PU) # and is authorized to pick-up your W2s. The authorization is the same as payroll pick-up.

There are no format revisions to this year's Wage and Tax Statement. Employees will continue to receive only one (1) set of the Form W-2. Statements will be laser-printed on two (2) separate sheets of paper.

Each year the UH Payroll Office receives numerous requests for duplicate Form W-2s because of careless or improper handling of the forms. Employees requesting duplicate W-2s may be required to wait at least 2-3 weeks for the Department of Accounting and General Services (DAGS) to act on the request.

We are required by DAGS to assess a $10.00 fee to the employee for a duplicate statement.

The procedures listed below should be followed to minimize requests for duplicate statements that have been lost or otherwise not received by employees:

1. Distribute each W-2 as directly as possible to the employee. With the increase in identity theft, please exercise due diligence in safeguarding an employee's record containing confidential information. Be sure the chain of responsibility for delivery can be traced in the event the employee claims non-receipt.

2. IF THE STATEMENT IS MAILED, MAKE EVERY EFFORT TO ADDRESS IT TO THE EMPLOYEE'S **CURRENT ADDRESS.** Because the payroll files may not contain the employee's mailing address, some of the statements will be printed with a University of Hawaii default address; do **not** mail the W-2 to this address.

   All W-2s must be issued no later than January 31, 2017. A Form W-2 should not be held for future mailing, but should be immediately sent to the current/last address of record.

   For Departments located on Manoa Campus: Campus Mailroom has requested that W2s reach the mailroom by **1:00pm** in order for W2s to be processed and sent out that day. Reminder that mail needs to be brought in with barcodes and sorted into international or domestic mail. Campus Mailroom will have a special incoming bin designated to receive the W2s.

3. It is important the return address on the mailing envelope be the specific address of the office in your department that is responsible for distributing the form.

1402 Lower Campus Road, Room 26 Honolulu, Hawai'i 96822
Telephone: (808) 956-8575 Fax: (808) 956-9143

It is especially important the return address on your mailing envelope be followed by the endorsement **"RETURN SERVICE REQUESTED"** so that any undelivered statement will be returned to you with either an address correction or the reason for non-delivery. There must be a ¼-inch clear space both above and below the endorsement.

4. Advise your employees who received payroll payments from more than one State of Hawaii agency that all their earnings for the year will be included on one statement. If your employee worked in two or more university or state departments, only one W2 will be issued to the employee. If your employee's W-2 is not with your department, have your employee check with their other university or state department(s) in which they worked.

5. Urge your employees to protect their statements from being misplaced or lost. There will be a $10.00 fee assessed to the employee for each duplicate statement.

   We have been advised by DAGS that if a personal check is accepted from the employee and if it subsequently bounces, the employing agency will be required to immediately reimburse DAGS the $10.00 duplicate W-2 fee and the $25.00 bounced check fee.

6. Make all requests for duplicate W-2s to the UH Payroll Office in writing. All requests must include the following information pertaining to the employee:

   a. Employee's name

   b. Social security number

   c. Payroll number and warrant distribution code

   d. The specific year of the W-2 (e.g. 2016)

   e. The reason for the request

   f. The $10.00 duplicate W-2 fee. (Checks should be made payable to the "Director of Finance".)

7. Any returned form W-2 must be retained in your office until April 13, 2017 so that all employee inquiries on non-receipt can be efficiently screened against those returned forms.

   Return all undeliverable W-2 forms and the envelopes in which they were mailed in to the UH Payroll Office after April 13, 2017.

Your assistance in forwarding these instructions to the responsible personnel in your department and to ensure that the instructions are followed is appreciated.

ATTACHMENT D

KAPIʻOLANI COMMUNITY COLLEGE ACTION PLAN SUMMARY

In addition to the notification of affected individuals and providing them with two years of credit monitoring through Experian, Kapiʻolani Community College has taken or will take the following actions:

1. A review of all data management practices in the programs involved with this incident was completed on February 13, 2017. A reminder notification of State law and university policies was done.

2. Twenty-four (24) additional custodians of W-2 were contacted by February 13, 2017. These custodians were also given a reminder notification of State law and university policies.

3. Communicate HRS 487N, UH Executive Policy E2.214 and other information security policies to all employees on a regular basis. Additional training will be provided as part of new employee orientation sessions, department chair/unit head training, faculty and staff professional development programs and training for program directors and other custodians of student records. Additional training will commence with the employees in the program involved with this incident in Spring 2017 and continue in the next academic year with other programs. The College will hold four (4) trainings per year at minimum.

4. Evaluate data management practices across all campus programs and institute changes as needed to ensure compliance with State law and University policies. Standardize practices across campus to the fullest possible extent. Comprehensive evaluation of data management practices will commence with selective admissions programs in April 2017 and continue through all academic programs and other offices across campus with a target completion date of December 2017. The campus will implement a schedule of annual evaluations.

5. An annual mandatory training program will be implemented for Academic Year 2017-2018 and communicated to all campus employees by Summer 2017. Training will be coordinated by the Center for Excellence in Learning, Teaching and Technology and the University of Hawaiʻi's Information Security team.