Prepared by Office of Vice President for Information Technology & CIO, the Office of Vice President for Legal Affairs and University General Counsel & the Office of Vice President for Student Affairs
This is a REVISED Executive Policy, replacing E2.214 dated November 2007.

E2.214 Security and Protection of Sensitive Information

I. 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 best 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 required for the operations of the institution. In such cases, the University must provide appropriate guidance and controls to protect the information it uses in its pursuit of teaching, learning, research, service and administration.

II. 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 such as the National Industrial Security Program or the Bioterrorism Special Agent Program, which have their own requirements.

Nothing in this policy is intended to constrain open and direct communication, 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.

III. Data Categorization

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

A. Public information

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

B. Sensitive Information

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

Examples of Sensitive Information include but are not limited to:

1) Student records, including anything protected by the Family Educational Rights and Privacy Act (FERPA)
2) Health information, including anything covered by the Health Insurance Portability and Accountability Act (HIPAA)
3) Personal financial information such as credit card numbers, bank account information, debit card numbers, etc.
4) Job applicant records (names, transcripts, etc.)
5) Social Security Numbers
6) Dates of birth

7) Private home addresses and phone numbers
8) Driver license numbers and State ID Card numbers
9) Access codes, passwords and PINs for online information systems
10) Answers to "security questions" such as "what is the name of your favorite pet?"
11) Confidential information subject to attorney-client privilege
12) Detailed information about security systems (physical and/or network)
13) Confidential salary information
14) Information made confidential by a collective bargaining agreement

IV. Social Security Number

The Social Security Number (SSN) may not be used as an identifier in any new University information system, and its use as an identifier shall be phased out in all existing systems. 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 State and Federal law and its inclusion shall be phased out in all other systems. 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.

V. Roles & Responsibilities

A. Information Resource 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 Office (IRO) 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.

B. 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**).

C. 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.

VI. Collection of Sensitive Information

Sensitive information is only collected and stored when essential to the functions and operations of the institution. Information resource stewards should minimize the use of sensitive information in the systems and services for which they are responsible.

VII. Access to Sensitive Information

A. 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 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.

B. Access Procedures

For multi-user systems, access procedures that are approved by the information resource steward must be in place before access is granted to others. Access procedures should address:

1) how access is requested by a prospective user or their supervisor
2) types of access available including read, write, copy and extend access to 3rd parties
3) how access requests are reviewed and approved
4) 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.)
5) what authentication and authorization processes are in place to ensure that only authorized users have access;
6) whether or how access is limited only to the portions of sensitive information required by the individual
7) how access is revoked in a timely manner when no longer required
8) how access is reviewed on a regular basis
9) how confidentiality is managed in cases whereby access granted may permit extension to 3rd parties
10) availability of audit trails for when, how and to whom access was granted

VIII. 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.

A. Security of Paper Transmissions

When transmitting sensitive information on paper (via hardcopy), the sender should mark the envelope as "CONFIDENTIAL" as appropriate to minimize the chance

of unnecessary exposure.

B. Security of Digital Transmissions

Sensitive information should be strongly encrypted whenever transmitted over public networks or carriers in digital form. This includes the transmittal of sensitive information via email, file transfers (FTP), web transactions, instant messaging or terminal login sessions.

C. Security of Fax Transmissions

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

D. 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 should 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 should delete all copies of the sensitive information as soon as practicable, and the sender should 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 should be used

when transmitting any sensitive information via the "filedrop" service or other means.

IX. Use and Storage of Sensitive Information

A. Limited Use and Storage

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

B. Security of System with Sensitive Information

Systems on which sensitive information is stored must minimally comply with all basic computer security standards (patch management, anti-virus protection, password controls, etc.).

Unencrypted sensitive information should be stored only on systems that are housed in secure and controlled environments. Where desktop systems access sensitive information, they must not be left logged in on an unattended basis or be available for casual perusal by unauthorized individuals.

C. Encryption and Physical Security of Sensitive Data in Mobile Formats

Sensitive information stored on any system or media that is subject to loss or theft -- including laptops, USB drives, diskettes, CD/DVDs, personal computers, departmental servers -- must be encrypted whenever not in active use. Systems susceptible to theft should be physically secured, e.g. with use of secure laptop cables, whenever possible.

D. Decoupling of Personal Information

Wherever possible (e.g. for any research studies), sensitive data should 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 should be protected as sensitive information.

E. Security of Non-Electronic Information

Paper documents and files containing sensitive information must be secured at all times. Such documents should 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.

X. Disposal of Media Containing Sensitive Data

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

A. Erasable Media

Electronic and magnetic media such as hard drives, diskettes, magnetic tapes and optical tapes should be erased using secure deletion tools before transfer or disposal.

B. Unerasable or Unerased Media

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

C. Paper

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

D. 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 suggests 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.

XI. 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 sensitive personal information and must report on them to the Legislature.

A. Definition of Security Breach

Under Hawai'i Revised Statutes, 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.

B. Timely Notice

Such notices 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).

C. Contents of Notice

Such 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 disclosed; (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.

D. Means of Notice

Such 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; (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.

E. Reporting Requirements

In accordance with State Law, the University must also submit a written report to the legislature within twenty days after discovery of a security breach. 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. In addition, in the event notice is provided to more than one thousand persons at one time pursuant to this section, the University must notify in writing, without unreasonable delay, the State of Hawai'i

Office of Consumer Protection and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

XII. Personnel Issues & Violations

A. Termination

In case of employer-initiated termination of employment of personnel with access to sensitive information, such access must be revoked immediately at the time of notification, or as soon as may be consistent with an applicable collective bargaining agreement.

B. 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.

XIII. 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 that run commonly used personal 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

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

On April 16, 2009, the UH Board of Regents approved the 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 (see **ATTACHMENT III**).

Attachment I

University of Hawai'i
General Confidentiality Notice

I understand that to fulfill the duties and responsibilities of my job, I may need to access personally identifiable information (PII) which is sensitive and/or confidential in nature. Such information may include, but is not limited to:

- Social Security Number, Home and mailing address, Home phone number, Date of Birth/Age, Ethnicity, etc.
- Admission and academic records
- Job applicant records (Names, transcripts, etc.)
- Employment and payroll records
- UH Usernames, passwords, "secret questions and answers" or other ID/password combinations for applications that contain or use personally identifiable information
- Credit card, debit card or credit-related information
- Bank account information

I understand that confidentiality of PII is protected by Chapter 92F (Uniform Information Practices Act) of the Hawai'i State Revised Statutes, the Federal Privacy Act of 1974, Federal Family Educational Rights and Privacy Act (FERPA), and other applicable state and federal laws and University of Hawai'i policies.

I understand the confidential nature of private information regarding our students, faculty, staff, and other members of the University of Hawai'i community and understand that it is my responsibility to respect and protect the confidentiality of this information.

I understand that accessing or seeking to gain access to PII except in the course of fulfilling my job responsibilities is prohibited. I further understand that disclosing, using or altering any such information without proper authorization is also prohibited. If I have any questions regarding access, use, or disclosure of such information, I understand that it is my responsibility to consult with my supervisor prior to taking any action.

I understand that it is my responsibility to keep my own UH Username and password confidential and that I am not to allow others to use my active sessions other than to resolve specific problems. I also understand that using another person's UH Username and password is prohibited unless given explicit permission to do so to resolve a reported problem. It is my responsibility to keep my Username/password combination(s) for all electronic applications confidential and sharing or transferring it to any other person is not allowed. I understand that it is my responsibility to notify my supervisor and/or the UH Information Security Officer (with Information Technology Services) if my Username and Password, PII data, or personal computer have been compromised.

I understand that electronic transactions on UH information systems may be automatically logged and that the logs of my actions may be routinely reviewed as part of the University's information security assurance program.

I have read and understand my responsibilities under UH Executive Policy: E2.210 "Use and Management of Information Technology Resources" (http://www.hawaii.edu/infotech/policies/itpolicy.html) and E2.214 "Security and Protection of Sensitive Information".

I understand that if I store any PII on any personal computer or server that it is my responsibility to ensure that the computer is secured and managed in accordance with applicable University policies and procedures.

I understand that failure to abide by this notice may result in disciplinary action in accordance with University policies and procedures, State and federal laws, and applicable collective bargaining agreement up to and including dismissal.

Signature: _____ Date: _____

Name (print): _____

UH Username: _____

Attachment II

CONFIDENTIALITY NOTICE: The contents of this email message and any attachments are intended solely for the addressee(s) and may contain confidential and/or privileged information and may be legally protected from disclosure. If you are not the intended recipient of this message or their agent, or if this message has been addressed to you in error, please immediately alert the sender by reply email and then delete this message and any attachments. If you are not the intended recipient, you are hereby notified that any use, dissemination, copying, or storage of this message or its attachments is strictly prohibited.

Attachment III

University of Hawai'i FTC Red Flags Rule Identity Theft Prevention Program
Creation Approved by the UH Board of Regents on April 16, 2009

I. Program Adoption

The University of Hawai'i ("UH" or "University") developed this FTC Red Flags Rule Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule, 16 CFR Part 681 ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the University of Hawai'i Board of Regents. After consideration of the size and complexity of the UH System and the nature and scope of its activities, the Board determined that this Program was appropriate for the UH System, and therefore approved the creation of this Program on April 16, 2009. This Program shall apply to all campuses and activities of the UH System.

II. Purpose and Elements

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account and to provide for continued administration of the Program. This Program should be carried out in conjunction with the existing UH Executive Policy, E2.214 on the Security and Protection of Sensitive Information, which provides comprehensive guidelines for information security. This Program supplements the existing Executive Policy to comply with the Red Flags Rule, which requires the University to adopt an Identity Theft Protection Program containing specific elements. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts offered or maintained by the University and incorporate those red flags into the Program;
2. Detect red flags that have been incorporated into the Program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students and other holders of covered accounts and the safety and soundness of the University from identity theft.

The Program shall, as appropriate, incorporate other existing policies and procedures that control reasonably foreseeable risks.

III. Definitions

"Identity Theft" is a fraud committed or attempted using the identifying information of another person without authority.

"Red Flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

"Covered Account" is a continuing relationship established by an individual with the University in which the University extends credit to the individual to obtain goods or services, or accepts a deposit from the individual, primarily for personal, family or household purposes, and that involves or is designed to permit multiple payments or transactions.

"Committee" means an Identity Theft Program Committee comprised of the Vice President for Budget & Finance/ Chief Financial Officer, the Vice President for Information Technology Services/Chief Information Officer, the Vice President for Student Affairs, and the Vice President for Administration, or their respective designees

IV. Covered Accounts

The University has identified three types of Covered Accounts:

1. Tuition and Mandatory Student Fees Installment Payment Plan;
2. Student Loans;
3. Services, Rentals, and Miscellaneous Fees, such as medical services, childcare services, facility rentals and use, parking, faculty housing rents, etc.

The University shall periodically review this list and identify any other Covered Accounts offered by the University, which shall be incorporated into this Program.

V. Identification of Relevant Red Flags

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The University will take reasonable steps to identify all persons seeking to open or use a Covered Account, such as requiring a photo ID card, requesting a service in writing, etc., as appropriate based on the nature of the transaction.

The University identifies the following Red Flags:

1. Suspicious Documents, i.e., identification documents appear to have been altered or forged or identification documents or card on which a person's photograph, signature or physical description is not consistent with the person presenting the document.
2. Suspicious Personal Identifying Information, i.e., identifying information presented in inconsistent with other information the student provides or with other sources of information; Social Security Number presented is the same as one given by another person; or an address or phone number presented is the same as that of another person.
3. Suspicious Covered Account Activity or Unusual Use of Account, i.e., change of address for an account followed by a request to change the student's name; payments stop on an otherwise consistently up-to-date account; or account used in a way that is not consistent with prior use.
4. Alerts from Others, i.e., report of fraud accompanying a credit report; notice to the UH System from another student, identity theft victim, law enforcement agent or others that the UH System is maintaining a fraudulent account for a person engaged in identity theft.

VI. Response to Detected Red Flags

The Program shall provide for appropriate response to detected red flags to prevent and mitigate identity theft commensurate with the degree of risk posed. In determining an appropriate response, the University shall consider any aggravating factors that may heighten the risk of identity theft. Appropriate responses to the relevant red flags include, but are not limited to the following:

1. Deny access to the Covered Account until other information is available to eliminate the red flag;
2. Monitor a Covered Account for evidence of identity theft;
3. Contact the affected student, staff member, faculty member, or other individual;
4. Change any passwords, security codes or other security devices that permit access to a Covered Account;
5. Prevent the opening of a new Covered Account;
6. Not attempt to collect on a Covered Account that is determined to have been fraudulently established;
7. Notify law enforcement; or
8. Determine no response is warranted under the particular circumstances.