

Prepared by the Office of the Vice President for Budget and Finance and Chief Financial Officer. This is a new procedure.

E2.216 Institutional Records Management and Electronic Approvals/Signatures

**I. PURPOSE AND POLICY**

To establish institutional requirements for the responsible management of University records.

To establish institutional requirements for the acceptability of electronic approvals/signatures.

The University is committed to effective institutional records management to meet legal and institutional requirements, optimize space usage and minimize the cost of record retention.

**II. SCOPE**

This policy applies to all University employees and governs the management of records used in the conduct of official business of the University.

This policy applies to records in any form and to records however or by whoever created that belong to the University or were created by University employees, as part of their work for the University.

Records produced or received by any University unit in the transaction of University business are the property of the University of Hawai'i.

This policy does not apply to records under the jurisdiction of the University Legal Affairs and General Counsel Office.

**III. RESPONSIBILITIES**

Each University unit has primary responsibility to:

- A. Manage and store records in a manner that facilitates timely and accurate retrieval;
- B. Ensure records are stored in secure locations with stable physical or electronic environments;
- C. Allow only those with proper authority to access records;
- D. Comply with UH policies and external laws and regulations that affect the management and disposition of its records.

To meet this responsibility each University unit shall designate a functional data steward as defined in E2.215 - Institutional Data Governance <<http://www.hawaii.edu/apis/ep/e2/e2215.pdf>>. Functional data stewards are responsible for the proper care and management of data and records for its unit.

#### IV. DEFINITIONS

- A. Disposition - Destruction or transfer to another state agency or to the State of Hawai'i Archives. Records with Personally Identifiable Information (PII) shall be securely disposed of per E2.214 <<http://www.hawaii.edu/apis/ep/e2/e2214.pdf>>.
- B. Electronic Signature - An electronic signature is an electronic sound, symbol, or process, attached to or logically associated with an electronic record (agreement, email, or other electronic record) and executed or adopted by a person with the intent to sign the record. For purposes of this policy, electronic signature and digital signature mean the same thing.
- C. Executive Data Steward - Vice Presidents, Chancellors, Vice Chancellors or appropriate administrators responsible for the major functional areas within a campus including, but not limited to, student affairs, research, academic affairs, and administration. These positions have the authority to govern the use of institutional data and records within their respective unit.

- D. Functional Data Steward - Functional Data Stewards are responsible for the day-to-day use and management and distribution of institutional data and records. Functional Data Stewards exist among all levels and across all units within the University. Registrars, financial aid officers, fiscal administrators, human resources specialists, and institutional researchers are among those considered Functional Data Stewards.
- E. General Records Schedule (GRS) - Issued by the State Comptroller pursuant to HRS §94-3, <<http://ags.hawaii.gov/wp-content/uploads/2012/09/GRS-2002-revised-5-06.pdf>>. The GRS provides retention and disposition standards for records common to several or all state executive and legislative agencies.
- F. Institutional Record - Institutional records are official business records, and may not be destroyed without an official retention period as specified in A8.450 <<http://www.hawaii.edu/svpa/apm/recmgmt/a8450.pdf>>.
- Institutional records, regardless of medium or characteristics, are created, received or maintained by a University unit in connection with its transaction of University affairs and/or in meeting its duties and responsibilities for the University. Such records would include both original documents and record copies. A record copy is a reproduction of the contents of an original document which is prepared either simultaneously or separately and can be identified by a particular function or by method of creation. (hereinafter "Records")
- G. Litigation Hold - An act by a University unit to preserve records relevant to a lawsuit or government investigation. University units shall take steps to prevent spoliation, destruction or alteration of records needed for on-going or pending legal actions and /or audits until the legal actions and / or audits are completed, even if they exceed the retention requirements listed in an approved retention schedule.

- H. Records Management - The planning, controlling, directing, organizing, training, promoting, and other managerial activities involving the life cycle of information, including creation, maintenance (use, storage, retrieval), and disposal, regardless of media. Records management procedures are used to ensure adequate and proper documentation of State and Federal policies and transactions.
- I. Records Retention Schedule - The list of records by name or type that authorize the retention and disposition of records. The retention schedule applies to all record formats.
- J. Retention Period - The minimum length of time which records shall be maintained by the University unit for operational, legal, or institutional purposes. Retention periods are based on legal and institutional requirements, standard practices; and the administrative, fiscal, legal and institutional value of the content.
- K. University Unit - For purposes of this policy, University unit means any campus, college, school, department, or unit of the University of Hawai'i.

**V. RECORDS STORAGE**

- A. University units shall:
  - 1. Determine the confidentiality and privacy status of all their records.
  - 2. Ensure that their records storage security measures meet the confidentiality and privacy needs of their records.
  - 3. Store records in a safe, stable and secure manner that supports timely and accurate retrieval, establishes appropriate controls on accessibility, and adheres to applicable federal regulations for specific records.
  - 4. Know the location of all their records.

5. Periodically check the stability and security of their physical and electronic storage environments.
  6. Ensure that their physical and electronic records storage areas are secure and maintain control of access to their physical and electronic storage areas and adheres to applicable federal regulations for specific records.
  7. Periodically review their physical and electronic records storage security measures.
  8. Document their records organization system, storage locations and security procedures.
  9. Protect records from accidental or intentional alteration and from destruction while the records still have value.
  10. When creating an electronic version of an original paper document, ensure that the electronic version accurately reflects the information set forth in the original paper document.
- B. The electronic version of an original paper document, once scanned shall be recognized by the University as an official business record. The electronic copy shall be deemed to be an original record for all purposes, pursuant to (HRS §92-30).
- C. Original paper documents shall be retained for one year from the scan date. Original paper documents shall be destroyed after the one year period provided the imaged document has been verified as accurate, readable and retrievable for later reference.
- D. Original documents deemed to contain intrinsic value by the University archivist or the State Archives Division may need to be retained in its original format.

VI. RECORDS RETENTION AND DISPOSITION

- A. Records shall be retrievable and accessible in a timely manner throughout their retention period.
- B. Retention concepts for electronic records are the same as those for non-electronic records. (Comptroller's Circular No. 2001-02, dated August 2, 2001).
- C. When records have satisfied their required period of retention, they shall be disposed of in an appropriate manner as prescribed in A8.450 - Records Management Guidelines and Procedures <<http://www.hawaii.edu/apis/apm/a8450.php>>.
- D. Records not covered by an approved records retention schedule will not be disposed of without the prior approval of the State Comptroller as prescribed in A8.450.
- E. Records covered by the State General Records Schedules shall be disposed of without further concurrence from the State Comptroller as long as the minimum retention periods set forth in the schedules have been met as prescribed in A8.450.
- F. Records to be transferred to other state agencies or the State Archives shall be transferred in accordance with procedures in A8.450.
- G. Records with a litigation hold shall not be destroyed until the legal action or audit is completed.
- H. Record retention for extramurally financed research and training programs/activities shall be in accordance with A8.926 <<http://www.hawaii.edu/apis/apm/congrant/a8926.pdf>>.
- I. University units shall annually update the State of Hawai'i Records Report System (RRS) administered by the State of Hawai'i Office of Information Practices (OIP) in accordance with HRS 92F-18(b).

**VII. ELECTRONIC APPROVAL/SIGNATURE**

- A. Pursuant to HRS 489E-7, a record or signature shall not be denied legal effect or enforceability solely because it is in electronic form.
- B. Where a University policy requires that a record or electronic document have the approval/signature of a responsible person, that requirement is met when the electronic record has associated with it an electronic signature.

Electronic authentication occurs when an electronic document is associated with an electronic signature or when a record is associated with a unique identifier such as a UH Username. Electronic authentication is required for establishing nonrepudiation (a guarantee that the owner of the signature cannot deny responsibility for the activity).

- C. Electronic signatures shall meet the following requirements:
  - 1. Unique to person using the electronic signature, i.e., Personal Digital Certificate or Login ID/Password.
  - 2. Capable of verification (Part of record's data structure).
  - 3. Under the sole control of person using the electronic signature.
  - 4. Sufficient controls shall be in place to provide an audit trail and to ensure that the electronic signature and their link to the respective record cannot be removed, copied, or otherwise manipulated to falsify an electronic record.
- D. An electronic signature used outside of its limitations will not be considered valid by the University.

- E. Any individual that makes inappropriate or illegal use of electronic signatures and/or records shall be subject to sanctions as provided by applicable law, rule, policy, or collective bargaining agreement.

**VIII. CONFIDENTIALITY AND PUBLIC INSPECTION OF UNIVERSITY RECORDS**

- A. Issues relating to the required disclosure or nondisclosure of University records are governed by Chapter 92F, Hawai'i Revised Statutes (Uniform Information Practices Act), and certain federal laws and regulations. Requests from University departments regarding these matters should be directed to the Office of the Vice President for Legal Affairs and University General Counsel.
- B. The State Office of Information Practices, (OIP) may be contacted for assistance in determining whether a record is public information.
- C. Records shall be subject to a litigation hold when the University is aware of a pending or threatened litigation by a member of the public for access to or a copy of a record. Records shall not be destroyed, even if that destruction is authorized by law. University functional data stewards are responsible for ensuring litigation holds are imposed and appropriate action is taken to prevent spoliation, destruction or alteration of records.

**IX. RETENTION OF PERSONALLY IDENTIFIABLE INFORMATION**

Nothing in this Procedure shall require, promote or support the retention of sensitive personally identifiable information (PII) such as credit card information and social security numbers in University records. In accord with Executive Policy E2.214 (Security and Protection of Sensitive Information), PII may be collected only when necessary to meet specific institutional requirements and shall be maintained in secured areas with access limited to authorized users. All PII shall be removed or redacted from University records once the requirements for having collected that information have been met.



**X. REFERENCES**

Hawai'i Revised Statutes Chapter 489E Uniform Electronic Transactions Act <<http://ags.hawaii.gov/wp-content/uploads/2012/09/Shortcuts-to-laws-on-records.pdf>>