

A8.\_\_\_\_ Electronic Imaging of Documents and Electronic Signatures

I. PURPOSE:

This policy:

- A. Establishes the University of Hawai'i (University) requirements for the imaging of University records (storing and accessing digital images of documents instead of paper) and electronic signatures.
- B. Provides guidance to University employees in the creation, use, retention, storage and destruction of University electronic imaging records to ensure compliance with all applicable State and Federal retention laws and regulations.
- C. Provides policy on when an electronic signature may replace a written signature.

II. SCOPE:

This policy applies to all University departments, and governs all uses of electronic imaging and electronic signatures used to conduct the official business of the University.

III. RESPONSIBILITIES:

- A. Deans, Directors, Department Heads - Electronic records created through document imaging shall be managed by Deans, Directors and Department Heads in the same manner as all other public records with regard to retention and disposal as specified in the *General Record Schedule* published by Department of Accounting and General Services (DAGS). Programs that choose to implement document imaging for archiving official

University records shall comply with imaging program requirements specified in this policy.

- B. Owners (originators) of electronic records are responsible for effectively managing their electronic records including ensuring that back-ups of vital or permanent records are made and stored at an appropriate secured offsite facility.
- C. University personnel are responsible for ensuring their electronic records are managed properly.

#### IV. DEFINITIONS:

- A. *Archive* - the records created or received and accumulated by an institution or organization in the course of routine business and retained due to their continuing or enduring value.
- B. *Compact Disc* [sometimes spelled *disk*] (CD) – is a small, portable, round medium made of molded polymer for electronically recording, storing, and playing back audio, video, text, and other information in digital form.
- C. *Digital Versatile Disk (DVD)* – Optical disc technology that uses high density recording techniques in addition to layering and two-sided manufacturing to achieve very large disc capabilities. Able to hold video, audio and computer data.
- D. *Disaster Recovery* – See State of Hawaii Department of Accounting and General Services Comptroller’s Circular No. 2001-01, subject: Vital Records Protection Policy and Guidelines.
- E. *Electronic Record* – Includes numeric, graphic and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes but is not limited to, magnetic media, such as tapes and disks (hard and floppy), optical disks, and flash drives, etc.
- F. *Electronic Signature* – An electronic sound, symbol, or process (e.g., UH username and password authentication process) attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign a record or otherwise indicate responsibility for actions, transactions or information.
- G. *Format* – For electronic records, format refers to the computer file format described by a formal or vendor standard or specification. (See Imaging Document Architecture below for recommended format.)

Electronic documents stored in an imaging system are to be in standard image file formats. TIFF (Tagged Image File Format) file format is the preferred standard for documents submitted through a scanning system. Other industry standard file formats are acceptable, provided complete documentation is maintained.

If proprietary file formats are used, the application developer should provide technical documentation on how to manage and how to convert to a standard format the electronic records created and used by the system. This will ensure records that are not forward-compatible are migrated to a compatible technology format, e.g., a current .PDF format, well before it comes unreadable.

- H. *General Records Schedule* – Issued by the State Comptroller pursuant to Hawaii Revised Statutes, §94-3. The schedule describes the records series, the minimum time the record shall be retained, and provide authorization for its disposition.
- I. *Imaging System* – An electronic imaging system is a computer-based configuration of equipment and software that stores machine-readable document images and their associated character-coded index data for on-demand retrieval. Electronic images can be computer generated, or created through document scanning.
- J. *Long-term retention period* – Records with an authorized retention period of more than ten years.
- K. *Secure Offsite Storage* – May include on-line storage, or a facility that is not the agency's normal place of business, e.g., State Archives (Comptroller's Circular No. 2001-02, dated August 2, 2001). The facility should provide appropriate climate-control for the storage of digital media, should have adequate security measures in place to protect the information from access by unauthorized personnel, and should provide for dry fire suppression.
- L. *Permanent retention period* – Records with an authorized retention period of permanent (in perpetuity).
- M. *Record – Information*, regardless of medium, detailing academic and/or employment history, business transactions, etc. Records include all books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics.
- N. *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. Record management procedures are used

to achieve adequate and proper documentation of State and Federal policies and transactions.

- O. *Retention Period* – The length of time that a record must be kept before it can be destroyed.
- P. *Short-term retention period* – Records with an authorized retention period of ten years or less.
- Q. *Storage* – Space for non-active records. Can be digital, optical, or physical space.
- R. *WORM (Write Once, Read Many)* - Data storage technology that allows information to be written to a disc a single time and prevents the drive from erasing or changing the data. The discs are intentionally not rewritable, because they are especially intended to store data that the user does not want to erase accidentally.

V. DOCUMENT IMAGING REQUIREMENTS (Best Practices):

- A. The following shall be present in an imaging program to ensure the reliability, accuracy, security, and accessibility of the digital images it creates:
  - 1. Hardware and software that meet industry standards listed below, and procedures and practices that comply with best practices for managing digital imaging programs.
  - 2. System and procedural documentation that outlines system specifications and describes and defines the creation maintenance, use, and preservation of digital images within the systems.
  - 3. Training program for departmental users of the system.
  - 4. Adequate system controls that monitor the reliability, authenticity and security of scanned images.
- B. Implementation requirements.
  - 1. *Records Manager* - University offices planning imaging programs shall identify a person to be the Records Manager to establish, document, implement, authorize access and monitor records management procedures and ensure appropriate training of assigned personnel.
  - 2. *Procedures* - Specific procedures shall be created and documented for: scanning and entering data; ensuring that all information within

images is readable and that the accuracy of index terms is verified; revising, updating and deleting images; backing up disks; establishing and implementing security measures; ensuring appropriate access; and implementing disposition.

3. *Compliance* - Procedures established shall be in compliance with pertinent, laws, regulations, and statements of best practice.
4. *Audit Trails* – Digital imaging programs shall provide and maintain a full audit trail of when and by whom scanned images have been created, revised, accessed or deleted.
5. *Training* – All staff members using an imaging system shall be required to undergo training on the system before they may add or dispose of official records.

#### C. Imaging System Architecture

1. The system must be able to cross-reference with other record keeping systems and software. Non-proprietary hardware and software components, open system architecture, or a requirement that vendors provide a bridge to any system with non-proprietary configurations is required. The flexibility of open systems architecture helps enable long-term records to be accessed and transferred from one hardware or software platform to another. Examples are systems where scanned images are stored as non-proprietary TIFF (Tagged Image File Format) or ASCII (American Standard Code for Information Interchange) formats.
2. Image Resolution
  - a. When determining document scanning resolution, UH programs shall consider data storage requirements, document scanning rates, and the accurate reproduction of the image.
  - b. Good quality images generally require a minimum scanning density of 200-300 dpi. For text documents that must be retained indefinitely, a minimum scanning density of 600 dpi is recommended.
3. Image Authenticity/Integrity
  - a. The imaging system shall ensure that scanned images are protected from accidental or intentional deletion or modification.

- b. To safeguard data integrity and longevity, UH digital imaging programs shall use a recording media that is **not rewritable**, referred to as WORM (Write Once Read Many).
4. Image Metadata - Metadata describing the content, sensitivity, and structure of the digital image shall be included within the digital image or linked to it. Examples of sensitive Information are the Family Educational Righrivacy Act (FERPA), Health Insurance Portability Accountability Act (HIPAA), personal identity information, etc.
5. Image Security
  - a. The department shall establish and document procedures for ensuring that only authorized personnel create, copy, modify, or use scanned images within the system. Records, which contain confidential and/or proprietary information, will be maintained in a secure environment, which ensures no unauthorized access.
  - b. The department shall develop and document backup procedures designed to create backup copies of scanned images and their related indexes. Backup copies should be stored in a Secure Offsite Storage facility.
6. Image Access - The imaging program shall use an indexing system that provides for efficient retrieval and printing, ease of use, and up-to-date information on the scanned images stored in the system.
7. Image Storage
  - a. Digital images should be saved in **non-proprietary** file formats, e.g., ASCII for text or Tagged Image File Format (TIFF) for images. If proprietary file formats are used, the application developer should provide technical documentation on how to manage and migrate the electronic records created and used by the system. This will ensure records not forward compatible are migrated to a compatible technology format, e.g., a current .PDF format, well before it comes unreadable.
  - b. Scanned documents shall be preserved without loss of vital information for as long as required by law, policy and best practice.
  - c. Both the working and backup copies of the disks and indexes are either migrated and converted if optical systems are upgraded or changed in a way that prevents access to the context of the disk created by the old system; or

- d. Electronic storage media should be periodically tested (e.g., conduct annual statistical sampling to identify any loss of data) to ensure data records are intact and recopied to new media if necessary or at least every eight to ten years. Use a recording media that is not rewritable.

#### D. Destruction

1. Electronic record shall comply with records-related laws, regulations, and authorized records retention and disposition schedules. Retention concepts for electronic records are the same as those for non-electronic records. (See Comptroller's Circular No. 2001-02, dated August 2, 2001)
2. When records have satisfied their required period of retention, they shall be destroyed in an appropriate manner as prescribed in APM A8.450.
3. Records not covered by an approved records retention schedule will not be destroyed without the prior approval of the State Comptroller. (See APM A8.450)
4. Records covered by the State General Records Schedules should be destroyed without further concurrence from the State Comptroller as long as the minimum retention periods set forth in the schedules have been met. (See APM A8.450, para 7, Records Disposition Procedures)
5. Original paper documents should be destroyed once the electronic documents have been successfully backedup and the imaging system meets the requirements of this APM.

#### IV. USE OF AN ELECTRONIC SIGNATURE

##### A. Signature required by University policy

1. Where a University policy requires that a record or electronic document have the signature of a responsible person, that requirement is met when the electronic record has associated with it a digital signature or an electronic signature generated through a software application or a process for electronic authentication maintained by University of Hawaii Information Technology Services (ITS).
2. ~~Where a University policy requires a written document, that requirement is met when an electronic record has associated with an~~

~~electronic signature generated through a software application or a process for electronic authentication maintained by University of Hawai'i Information Technology Services (ITS).~~

3. Electronic authentication occurs when an electronic document is associated with a digital 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).

B. Electronic signatures must 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 must 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.

C. Approval of other Electronic signature methods

1. The approval of electronic signature methods which are generated through software applications not maintained by ITS will be by the Vice President from Administration after a review of the electronic signature method by ITS.
2. The approval of an electronic signature method can limit the use of that method to specified electronic records or specific University organizations. An electronic signature used outside of its limitations will not be considered valid by the University.

D. Unauthorized use

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

## **REFERENCES:**

Department of Defense (DoD) 5015.2-STD, Design Criteria Standards for Electronic Records Management Software Applications, June 2002.  
([http://www.dtic.mil/whs/directives/corres/pdf/50152std\\_061902/p50152s.pdf](http://www.dtic.mil/whs/directives/corres/pdf/50152std_061902/p50152s.pdf))

Electronic Signatures in Global and National Commerce Act (ESIGN Act), October 2000. (<http://www.ftc.gov/os/2001/06/esign7.htm>)

National Archives and Records Administration (NARA), 36 Code of Federal Records (CFR), Part 1234 – Electronic Records Management, May 2001.  
(<http://www.archives.gov/about/regulations/part-1234.html>)

State of Hawaii Comptroller's Circular No. 2001-02, Policy and Guidelines Relating to Electronic Records Retention and Disposition, August 2001.  
(<http://www.hawaii.gov/dags/archives/records-management/records-retention-and-disposition-schedules>)

State of Hawai'i, Department of Accounting and General Services, General Records Schedules 2002 – Revised through May 2006,  
(<http://www.hawaii.gov/dags/archives/records-management/records-retention-and-disposition-schedules/?searchterm=archives%202002>)

State of Hawaii House Bill 515 SD-1, Relating to Government Records, June 2005.  
(<http://www.capitol.hawaii.gov/sessioncurrent/status/HB515.asp>)

Uniform Electronic Transactions Act (1999).  
(<http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm>)

University of Hawaii Administrative Procedures Manual (APM) A8.450, Records Management, August 2002. (<http://www.hawaii.edu/svpa/apm/a8450.html>)