RECORDS MANAGEMENT POLICY #9.0 - Rev. Nov. 2013

GUIDELINES FOR ELECTRONIC RECORDS

PURPOSE: The purpose of this guideline is to establish a records management policy under which the courts and offices of the New York State Unified Court System can, with reasonable certainty, certify records maintained in electronic formats within the useable life of that system.

Unlike records created in "sight" medium formats such as paper and film, records created in electronic formats have a short term life expectancy due to ever changing technology. Ever changing technology makes records more accessible for those who use these types of systems. This, however, creates special challenges for addressing retention and preservation issues.

POLICY STATEMENT: This guideline applies to all electronic records created, used and maintained by courts and administrative offices. Records on electronic systems should be managed uniformly and efficiently; should be accurate and reliable so their integrity is not questioned; should be accessible when needed; should be protected from unauthorized access under confidential and sealing statutes; and should be maintained/destroyed in accordance with the records retention and disposition schedules adopted pursuant to 22NYCRR §104.

A. SYSTEMS DOCUMENTATION AND RECORDS MANAGEMENT

1. **Document all processes and protocols for records created in the normal course of business. This includes court records and records which document the business processes and history of the courts.**

2. **Create up-to-date and adequate system documentation to describe and understand the purpose(s) and function(s) of the system. It should be available in electronic format and backed up either on a hard copy print format or in secure digital format; that preserves the original system documentation. The documentation should include the System Metadata file required to interpret the records as well as technical components and characteristics necessary for reading, processing, accessing, using, and processing of records; disaster, recovery and contingency operation plans; retention of records; disposing of records; auditing procedures for internal controls; quality control procedures; training and system maintenance.**

3. **Maintain equipment hardware along with documentation of any service resulting from an event impacting a disruption in service.**

4. **Establish error tolerance standards for service.**

5. **Document software systems (operating, application, communication, etc.) detailing all system problems and resolutions, updates, upgrades and conversions, and software modifications.**

6. **If proprietary hardware or software is used, the system developer must provide technical documentation on how to manage and migrate the electronic records created and used by the system.**

7. **Electronic files and records, indices, documentation, and any other related material must be inventoried and appraised for retention requirements. Records Retention and Disposition Schedules and guidelines apply to all records regardless of format.**

B. SYSTEM SECURITY AND ACCESS REQUIREMENTS

1. **Only authorized personnel should have access to electronic records. Security levels need to be correlated to individual levels of access requirements. Tapes, disks and other media housing records accessible to the public should not contain confidential, sealed or expunged records.**

2. **E-commerce and electronic signatures processes/protocols must contain all security and access protocols to protect UCS and users on the system. The process/protocols should be in compliance with New York State and Federal regulations and must assure that any unauthorized use of information is prohibited.**

3. **Communication and exchange mechanisms of information/documents via electronic means between outside computer systems and/or portable media (disks, tapes, CD's, etc.) should be provided so that the UCS information stored on the system is not breached.**

4. **Disaster Planning and Recovery Plans must be in place, tested for viability, and documented to protect records against information loss.**

5. **Electronic records must be backed-up on a regular schedule to safeguard against the loss of information due to equipment malfunctions or human error. Maintain backup and disaster recovery copies of electronic records in separate off-site storage areas. The off-site storage area must meet security standards for unauthorized access and use, environmental storage standards, and fire prevention and suppression standards for electronic records found in Records Management Offsite Storage Policy #1.**

6. **All types of electronic storage media (including backup and disaster recovery copies) utilized to store records must be tested, verified, and stored per ANSI/NISO industry standards.**

7. **Ensure that electronic records are in compliance with confidential and sealing requirements as found in New York State and Federal statues and rules. Magnetic recording media previously used for electronic records containing vital, confidential and/or sealed and proprietary information should not be reused if the previously recorded information can be compromised by reuse in any way. Procedures should be established and documented to restore all confidential and sealed electronic records to their original state if the record is unsealed.**

8. **System integrity should be maintained by adhering to routine operating procedures and maintaining an audit trail. Establish audit trail procedures for data entry and track when and what alterations were made and by whom.**

C. FILE INTEGRITY

1. **Implement procedures to ensure that file integrity is maintained. Identify how the documents/records, will be created, stored, retrieved, transmitted, displayed, printed, processed, reported, migrated, and disposed. Identify the workflow process of the computer system, users, and outside sources coming into the system. Identify the location, manner and media in which electronic records will be maintained and stored to meet operational and retention period requirements and the maximum time span that records remain on each storage medium, and the procedures needed to dispose of the electronic records.**

2. **Establish quality control procedures for areas of system design, implementation, operation, conversion and administration. Quality control should be conducted for all records that will serve as the certifying record copy and should include a review for legibility and accuracy. It should be certified by the court and/or office of the New York State Unified Court System that all data is true and correct. Those quality control measures should include, but not be limited to:**

    (a) a verification, no more than six months prior to use, that the magnetic media used to store permanent or archival electronic records are free of permanent errors and are in compliance with ANSI/NISO Standards;

(b) an annual test of a three percent statistical sample of all volumes, or 10 volumes of each type, of magnetic media, whichever is larger, to identify any loss of data and to discover and correct the causes of data loss;

(c) rewind, under controlled tension, all tapes and cartridges at least every two years; where applicable

(d) copy immediately, onto new media, any permanent or archival electronic records stored on media with 10 or more permanent errors per volume and, where possible, lost data must be restored. Any error correction resulting in the re-creation of data must be documented;

(e) prepare external labels which provide a unique identifier for each volume, the name of the organizational unit responsible, and the permanent or archival electronic records title.

3. If converting record copies of records to electronic format and the electronic system will be used as the official certifying record, the electronic system must meet all design requirements and conditions (as set forth in Section A of this Guideline) to serve as the new official certified record, be audited and certified by the appropriate UCS departments.

4. If creating original records directly in electronic format (including electronic filing, indexes and docket books) and the electronic system will be used as the official certifying record, the electronic system must meet all design requirements and conditions (as set forth in Section A of this Guideline) to serve as the new official certified record, be audited and certified by the appropriate UCS departments. The system must meet all criteria in this guideline to ensure migration of the information on to new systems.

5. File integrity must be maintained for all records in the electronic system. Where the standards rendered herein are not able to be complied with, records that have a long term or permanent retention must also be maintained in an alternate medium such as paper or microfilm that comply with archival standards as required by the Rules of the Chief Administrator §104.

6. All electronic records, including backup and disaster recovery copies, that have reached the date for destruction, must be destroyed pursuant to retention designations in the Records Retention and Disposition Schedules and following the requirements established by the Rules of the Chief Administrator §104. A searchable list must be maintained detailing what records and copies were destroyed, the date, by what method and who conducted the disposal.

7. **If the storage media contains records with varying retention dates, the media should not be destroyed until all destruction dates have passed. Where the system does not address this, it is advisable to put records containing the same destruction dates and security protocols on the same storage media.**

8. **A migration strategy should be established and implemented for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorized life cycle. Migration needs to maintain the content of the records and any associated metadata required to interpret the records. This should include record format or layout and contextual elements, and the data's relationship to other data. Document how the data on the current hardware and software will be transferred. All records not yet completing their retention and disposition requirements must be converted to the most recent software and hardware versions in use. Changing technology, media deterioration and migration should not result in lost information. If, for any reason, normal migrations and backups are not able to be maintained, electronic records must be backed up in a sight medium format such as paper or microfilm in order to insure the long term integrity of the records.**

D. COMPLIANCE

1. **Ensure compliance with all applicable UCS policies, procedures and standards.**

2. **Review electronic records systems at regularly scheduled intervals for conformance with established UCS procedures, standards and policies. The review should determine if the records have been properly identified and described, and whether the schedule descriptions and retention periods reflect the current informational content and use.**

3. **Designate an employee who will attest to the integrity of the system, including hardware and software components and all operational and administrative procedures and activities relating to the creation and disposition of the record, so if called upon can do so in a judicial/legal/administrative context.**

APPENDIX: DEFINITIONS

Access - **The process and procedure by which records are made available for use.**

ANSI - **American National Standards Institute**

Audit Trail - **Data about the activities of data: creation, updates, deletion. Examples of audit trail data are a date and time stamp of when the change occurred and who changed the data.**

Data File - **An original collection of related data, usually arranged into logical records that are stored together and treated as a unit.**

Data - **Symbols or representations of facts or ideas that can be communicated, interpreted, or processed by manual or automated means. Often associated with electronic data or with statistics or measurements.**

Deletion - **The obliteration of the record or data from an Electronic Record System. The record is deleted and no longer exists. Used synonymously with erasure and expungement**.

Electronic Record - **Records stored in a form only a computer can process. Also called machine-readable records or EDP (Electronic Data Processing) records.**

Electronic Record System - **Record system that produces, manipulates, or stores auditable records of transactions by using a computer.**

Erasure - **The obliteration of the record from an Electronic Record System. The record is deleted and no longer exists. Used synonymously with deletion and expungement.**

Error tolerance standards - **Established maximum standard of measurement allowed for errors in electronic computer equipment or its function.**

Expungement - **Removing and deleting records or information from an Electronic Record System. Used synonymously with deletion and erasure.**

Information System - **The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Also known as a record system.**

Long Term or Permanent Retention - **Check with Records Staff for appropriate designation.**

Metadata - **Information about the data. Includes the attributes and information about each piece of data, such as a business definition, size, format, or location. Provides the context that transforms the data into meaningful business information.**

Migration - **Moving data from one electronic computer information system to another electronic information system.**

NISO - **National Information Standards Organization**

Permanent Records - **Appraised records with enduring value which are designated for permanent retention on the Records Retention and Disposition Schedules.**

Record - **Any book, paper, map, photograph, microphotograph, machine-readable material, or other documentary material, regardless of physical form or characteristics, made or received by a court or administrative office in connection with the transaction of public business or the exercise of its functions and responsibilities.**

Record Copy - **This is the official copy of the record.**

Record-Keeping System also known as Records System - **A set of policies and procedures for organizing and identifying documents/files to speed their retrieval, use, disposition and to provide adequate documentation of functions and transactions.**

Reformatting - **Migrating information from one information system to another in a different media. For example migrating paper or electronic records to microfilm, or migrating paper to an electronic system.**

Short Term Retention - Check with Records Staff for appropriate designation.

System Documentation - **Written explanations of functions and procedures related to all aspects of an electronic information system.**

Volume - A fixed amount of storage on a disk or tape.