Union County

Electronic Records and Document Imaging Policy

Adopted by the Union County Board of Commissioners
December 2, 2013

Table of Contents

1. Purpose 3
2. Responsible Parties 3
3. Availability of Information Systems and Electronic Records for Outside Inspection 5
4. Maintenance of Trustworthy Electronic Records 6
5. Components of Information Technology Systems 7
6. Documentation of Information Technology Systems 8
7. Digital Document Imaging Program Documentation and Procedures 8
8. Request for Disposal of Original Records Duplicated by Electronic Means 11
9. Other Electronic Records Management Practices 13
10. Compliance and Electronic Records Self-Warranty 14
11. Commencement Date of Policy 14

1. Purpose

The purpose of this policy is to provide standards for the efficient safeguarding of all of Union County's electronic records, including records that fall under the document imaging policies described herein. The records covered by this policy are in the custody of Union County (the "County") and are maintained for the benefit of County use in delivering services and in documenting County operations. This Electronic Records and Document Imaging Policy reflects guidelines set forth by the North Carolina Department of Cultural Resources (the "DCR"). Complying with this policy will increase the reliability and accuracy of records stored in the County's information technology systems, and will ensure that these records remain accessible over time. Exhibiting compliance with this policy will enhance records' admissibility and acceptance by the judicial system as being trustworthy.

All public records as defined by N.C.G.S. § 132-1 are covered by this policy. This includes permanent and non-permanent records, and confidential and non-confidential records. These classifications may warrant different treatments when processing the records. This policy serves as basic documentation of the procedures followed by the County in imaging, indexing, auditing, backing up, and purging electronic records in accordance with the applicable retention and disposition schedules, and in handling the original paper records, if applicable. More detailed procedures and documentation is also available, or developed, in accordance with this policy.

This policy also serves to protect those records digitized and stored in the County's electronic records and document imaging systems, which reduces required storage space for original documents as the County transitions toward a more "paperless" digital system, and provides instant and simultaneous access to documents as needed.

The form provided in Section 8 of this policy, *Request for Disposal of Original Records Duplicated by Electronic Means*, or any similar successor document produced by the DCR, is completed and submitted to the DCR whenever the County wishes to obtain the DCR's permission to destroy a new series of paper records that have been digitized through document imaging and the implementation of this policy.

This policy will supersede any electronic records system and/or document imaging policy previously adopted by the County; provided, however, (i) that this policy will not supersede such polic(ies) adopted by the Union County Sheriff, unless the Sheriff expressly consents in writing, and (ii) that this policy will supersede the polic(ies) adopted by the Division of Social Services only at such time established by the County Manager as the implementation date pursuant to Section 11. This policy will be reevaluated at a minimum of every five years, or upon the implementation of a new information technology system that affects the electronic records and document imaging systems described herein, and will be updated as needed. A copy of this policy, as well as any amendments hereto, will be sent to the DCR for its files.

2. Responsible Parties

County Manager/Executive Directors/ Division Managers

Responsibilities include:

1. Determining access rights to the electronic records and document imaging systems;
2. Approving applicable information systems as configured by the IT Division; and
3. Performing quality assurance checks of documents imaged under this policy by sampling applicable imaged documents for audit before the original documents are destroyed pursuant to this policy and applicable law.

IT Division

Responsibilities include:

1. Installing and maintaining all information technology systems and their equipment and software, particularly the electronic records and document imaging systems;
2. Configuring electronic records and document imaging systems according to County needs, including creating and testing applications and indexes;
3. Controlling access rights to the electronic records and document imaging systems, in accordance with the determinations and direction of County management;
4. Maintaining documentation of the electronic records and document imaging systems' hardware and software;
5. Establishing audit trails that document actions taken on records stored by the electronic records and document imaging systems;
6. Providing backups for electronic records and recovering deleted electronic records when necessary, as provided herein;
7. Completing disaster recovery backup of electronic records and document imaging systems at least once every two years;
8. Establishing and providing training on electronic records and document imaging processes and systems equipment and software, documenting such training, and providing remedial training as needed; and
9. Creating and updating detailed procedural manuals describing the document imaging process and document imaging system equipment.

Record Creators

Responsibilities include:

1. Attending and signing off on acknowledgement of electronic records (and document imaging, if applicable) training conducted by IT Division staff or by the DCR;
2. Creating passwords for computers containing, or with access to, electronic records that are long, complex, and frequently changed;
3. Creating and managing electronic records in the record creator's purview in accordance with this policy, guidance issued by the DCR, County IT Division policies and procedures, and all applicable law;
4. Reviewing the electronic records system records annually and purging records in accordance with the applicable retention and disposition schedules;

5. Carrying out day-to-day processes associated with the County's document imaging program, as assigned to particular persons by County management, which may include the following:
    - Designating records to be entered into the document imaging system
    - Noting confidential information or otherwise protected records and fields
    - Removing transient records
    - Completing an indexing guide form for each record being scanned
    - Reviewing and indexing imaged documents for quality assurance
    - Naming and storing the scanned image documents in designated folders
    - Once approved by the DCR, destroying or otherwise disposing of original records in accordance with guidance issued by the DCR.
    - Conducting any necessary batch conversions or batch renaming of imaged records; and
6. County employees who have been approved to telecommute or use mobile computing devices must:

    - Comply with all applicable County policies relating to telecommuting or mobile computing, as well as all other applicable law and policies governing public records
    - Back up information stored on the mobile computing device daily to ensure proper recovery and restoration of data files
    - Keep the backup medium separate from the mobile computing device when a mobile computing device is outside of a secure area.

3. Availability of Information Systems and Electronic Records for Outside Inspection

The County recognizes that the judicial system may request pretrial discovery of the information technology systems used to produce electronic records, as well as related materials. County personnel will honor requests for outside inspection of such information systems and testing of data by opposing parties, a court of competent jurisdiction, and government representatives, as required by law. Electronic records will be available for inspection and audit by a government representative for the full period required by law and approved records retention and disposition schedules, regardless of the life expectancy of the media on which such records are stored, to the extent that such inspections or audits are required by law. Electronic records related to any litigation, government investigation, or audit must continue to exist when such litigation, government investigation, or audit is pending, imminent, or if a court order may prohibit specified records from being destroyed or otherwise rendered unavailable.

In order to lay a proper foundation for the purposes of admitting the County's electronic records into evidence, the County will be able to provide up-to-date, detailed documentation that describes the procedural controls employed in producing records; procedures for input control (including tests used to assure accuracy and reliability of relevant information systems); and evidence of the records' chain of custody. In addition to this policy as documentation, such documentation includes the following documentation that will be prepared by the IT Division:

- Information systems procedural manuals

- Information systems documentation
- Electronic records and document imaging training documentation
- Electronic records and document imaging audit documentation
- Electronic records and document imaging audit trails

The County will also honor inspection and copy requests of electronic records pursuant to applicable law. The County will produce electronic records pursuant to a public records request, as required by applicable law, in the format in which they were created, unless otherwise specified by the requesting party. However, the County shall produce the records in any medium it is capable of producing such records, if asked by the requesting party. The County may assess different fees for different media as prescribed by law. If it is necessary to separate confidential from non-confidential information in order to permit the inspection or copying of records pursuant to a public records request, the County will bear the cost of such separation.

4. Maintenance of Trustworthy Electronic Records

Electronic Records Produced by Methods that Ensure Accuracy

All systems used by the County to create and manage electronic records, including any email clients, social media platforms, and cloud computing platforms, conform with all applicable DCR policies, as well as any applicable IT Division security policies.

Electronic records files are named in accordance with the *Best Practices for File-Naming,* published by the DCR, or any successor document.

Electronic records files are saved in formats that comply with the DCR's *File Format Guidelines for Management and Long-Term Retention of Electronic Records,* or any successor document. This document is currently available at the following web address: (http://www.records.ncdcr.gov/guides/file_formats_in-house_preservation_20120910.pdf).

File formats used by the County are adopted as standard by the state, and are well supported, are backwards compatible, and have robust metadata support.

Electronic Records Maintained in a Secure Environment

Security of the electronic records and document imaging systems, and access to the records they hold, are maintained in the following ways:

- Access rights are managed by the IT Division, as determined by County management, to prevent unauthorized viewing of documents.
- The electronic records and document imaging systems are able to separate confidential from non-confidential information; or record creators otherwise organize and name file to reflect confidentiality of documents stored within.
- Confidential material is redacted before it is shared or otherwise made available to public records requestors. Documents, including metadata, tags, and other information, are assessed to ensure the effectiveness of redaction of any confidential information.

- Confidential information is stored on off-network storage systems, and folders with confidential information are restricted.
- Physical access to computers, disks, and external hard drives is appropriately restricted.
- Duplicate copies of digital media and system backup copies are stored in offsite facilities.
- All information systems' password and operating procedure manuals are kept in secure offsite storage.

Electronic Records are Associated and Linked with Appropriate Metadata
Metadata is maintained alongside electronic records as appropriate. At a minimum, metadata retained in electronic records will include file creator, creation date, title (stored as the file name), and when appropriate, cell formulae and email header information fields. Information on the access of records will also be retained as part of the metadata for electronic records. County employees are instructed to not create metadata, other than metadata that is essential for a file's current use and/or retention.

Electronic Records are Stored on Media that is Regularly Assessed and Refreshed
Data is converted to new usable file types as old file types become obsolete or otherwise deteriorate. The following steps are taken to ensure the continued accessibility of records kept in electronic formats:

- Data is audited and assessed yearly.
- Media is refreshed every three to five years, as appropriate. County staff documents when and how records are transferred from one storage medium to another.
- Records are periodically converted to new file types, particularly when a new information technology system requires that they be brought forward in order to properly render the file.
- Metadata is maintained during media migration.
- Records are verified through hash algorithms before and after migration of records to new media to ensure that the records did not change during such a conversion.
- Storage media is maintained in a manner and in an environment that promotes bit-level preservation. Humidity does not exceed 50% and should not fall below 30%. Room temperature is set between 65° F to 75° F. The County adheres to the media manufacturer's recommendations for specific environmental conditions in which the media should be stored.
- Media used to store imaged data is clearly labeled with enough information such that its contents can be determined.

5. Components of Information Technology Systems

Training Programs
The IT Division will conduct training for information systems use for electronic record creation and electronic records management, using material published by the DCR when appropriate. All employees who create or maintain electronic records will be made aware of

information systems procedures and policies and will be trained on such policies. After such employees complete this training, the employees will confirm their acknowledgement of the policies and training by their signature. When appropriate, County employees will also attend trainings offered by the DCR on the maintenance of electronic records. Documentation will be maintained for the distribution of written procedures, attendance of individuals at training sessions, refresher training programs, as well as other relevant information.

Audit Trails

A log of activities on the electronic records system is maintained. This log includes information on who accessed the system, how and by whom electronic records were created and modified, and whether standard procedures were followed.

Audits

Audits are designed to evaluate the electronic records process and system's accuracy, timeliness of procedures, adequacy of procedures, training provided, and the existence of audit trails. Internal audits are conducted regularly by the County's IT Division. The County may also request periodic independent, external audits of its electronic records systems and electronic records policies, procedures, and training, if appropriate. Records are kept of the result of any such audits for the time period required by law and this policy.

6. Documentation of Information Technology Systems

Content of Systems Documentation

The County maintains information systems documentation that describes systems procedures and actual practices, systems software and hardware, systems environment (in terms of the organizational structure, functions and responsibilities), and systems processes. This documentation explains how the systems operate from a functional user, as well as data processing, point of view. Documentation is reviewed and updated yearly, or upon implementation of a new information technology system, by IT Division staff. Such documentation maintained by the County includes:

- Information systems procedural manuals
- Information systems documentation
- Security backup and disaster recovery procedures as a part of the Continuity of Operations Plan
- Agreements or purchase orders (as appropriate) for contracted information technology services

Retention of Systems Documentation

One set of all information systems documentation will be maintained during the period for which the records produced by the processes or systems could likely be subject to court review, and until all data created by every system instance has been destroyed or transferred to a new operating environment. The time period for the retention of such documentation shall be at least three years.

7. Digital Document Imaging Program Documentation and Procedures

System and Procedural Documentation

The IT Division is responsible for preparing and updating detailed procedures that describe the process followed to create and re-create electronic records. This documentation will include a description of the document imaging system hardware and software. A current procedural manual will be maintained to assure the most current steps are followed and to assure reliable system documentation will be available for judicial review or similar proceedings.

Each workstation designated as a document imaging station will have, at a minimum, the following hardware and software, unless the scanner is collocated by means of a network interface:

- Document/image scanner authorized by the IT Division. This is currently the Fujitsu fi-6130Z model, but such model may be changed as deemed appropriate by the IT Division.
- Driver software for scanner
- Laserfiche imaging software, or other software as deemed appropriate by the IT Division
- Instructions manual, maintained by IT Division staff, describing in detail the steps required to get from the beginning to the end of the document imaging process. This manual will also define:
    - The resolution of scanned images, as well as any compression standard used;
    - The file formats of scanned images;
    - The file naming conventions to be used for scanned images;
    - A determination of when batch conversion or batch file re-naming will be necessary, and what tool should be used for such conversions;
    - How the scanned images will be stored in the document imaging system; and
    - Image enhancement techniques, if any, that should be conducted after document imaging.

Training

Only designated staff that have been formally trained by IT Division staff on the use of the document imaging system software and equipment, and who have signed documentation noting their attendance at, and acknowledgement of, such training, will be allowed to use the document imaging system. The IT Division shall keep records regarding this training, as well as the attendance of employees at such training sessions. Original records will be scanned and filed in the document imaging system as part of an ongoing regularly conducted business activity, as such scheduling and activity is determined by County management and the IT Division. Components of the training will include basic techniques for image capture, indexing, quality control, security configuration, auditing, use of equipment, and general system maintenance. Rights to image and index records will not be assigned until a user has been trained. If it is found that a user improperly indexes or scans a document, an auditor, or other appropriate County staff, will address this occurrence with the user and remedial training will be performed as necessary.

Indexing and Metadata

All imaged records must be indexed in order to facilitate efficient retrieval, ease of use, and up-to-date information about the imaged documents stored in the document imaging and electronic records systems. This index should capture the content, structure, and context of the imaged documents. The index will be developed by IT Division staff, working with other County management staff as appropriate, prior to the implementation of any County-wide document imaging system. Imaged records should also be indexed according to guidelines set by the DCR.

Auditing and Audit Trails

Employees authorized to image records will conduct a quality control audit following the imaging of a record to ensure that the following features of the imaged record are legible:

- Individual letters, numbers, and symbols;
- Combinations of letters, numbers, and symbols forming words or sentences;
- Graphics such as signatures, logos, and pictures; and
- Other features of records such as color, shape, texture, etc., that relate to the content of the information.

Appropriate managerial staff for the various service areas/divisions of the County, as assigned by County management, will also periodically audit imaged records for accuracy, readability, and reproduction capabilities. Audits will be conducted on a sampling of documents from a particular record set that are converted from original paper record form into electronic records before the destruction of any original records from that particular record set. A written audit report will be prepared indicating the sampling of records produced and what remedial procedures were followed if the expected level of accuracy was not achieved.

Audit trails built into the document imaging system will automatically document which user creates, duplicates, modifies, or otherwise prepares records, and what procedures were taken related to those records. Audit trails include the success or failure, date, time, and user of the following events:

- Add/Edit electronic document
- Assign index template
- Copy document
- Copy pages
- Create document/folder
- Delete entry
- Delete pages
- Delete volume
- Edit image
- Email document
- Export document
- Index creation/deletion/modification
- Insert page
- Log in/out
- Move document
- Move pages

- Print document

Retention of Original and Duplicate Records

To obtain permission to destroy original records following the document imaging process, the appropriate county staff will complete the form found in Section 8 of this policy, *Request for Disposal of Original Records Duplicated by Electronic Means*, or any successor form issued by the DCR. Once each new record series is imaged into the document imaging and electronic records systems, the DCR must approve the destruction of the original records. Permanent records may be also imaged for ease of access, but the original records may not be destroyed unless an analog copy exists prior to the records' destruction, as provided by applicable law and DCR policies.

Destruction of original records is allowed only after quality assurance has been conducted on the imaged records, necessary corrections have been made, auditing procedures have been conducted by the appropriate County staff, and the destruction of such records is approved by the DCR. Such original records will be destroyed in a manner allowed by applicable law.

The imaged electronic document records will be maintained for the specified retention periods according to the County's records retention and disposition schedules. The retention period is considered to have begun when the original document was created, not when the electronic document reproduction of the original document was created.

Electronic and digital images of scanned records in the document imaging and electronic records systems will be considered the "official" County record once the original records are destroyed in accordance with applicable law and this policy. Any hard copy generated from such imaged electronic records will be considered the County's duplicate "working" record.

A copy of any purchase order or detailed service-level agreement with any third-party providing services related to the document imaging process will be maintained as required by applicable law and records retention and disposition schedules.

8. Request for Disposal of Original Records Duplicated by Electronic Means

The form in this section, or a successor form issued by the DCR for the same purpose, is used to request approval from the DCR to dispose of non-permanent paper records which have been imaged into the County's information systems, or otherwise duplicated through digital document imaging or other conversion to a digital environment. This form will only be submitted by County staff once all of the applicable procedures in Section 7 of this policy have been followed. This form does not apply to records which have been microfilmed or photocopied, or to records requiring permanent retention. The most-up-to-date version of the Request for Disposal of Original Records by Electronic Means can be found at www.ncdcr.gov/archives, or any successor place designated by the DCR.

STATE ARCHIVES of NORTH CAROLINA

GOVERNMENT RECORDS SECTION
STATE RECORDS CENTER

www.ncdcr.gov/archives 4615 Mail Service Drive, Raleigh, NC 27699 919-807-7350

Request for Disposal of Original Records Duplicated by Electronic Means

If you have questions, call (919) 807-7350 and ask for the Records Management Analyst assigned to your agency.

This form is used to request approval from the Department of Cultural Resources to dispose of non-permanent paper records which have been scanned, entered into databases, or otherwise duplicated through digital imaging or other conversion to a digital environment. This form does not apply to records which have been microfilmed or photocopied, or to records with a permanent retention.

Agency Contact Name:	**Date (MM-DD-YYYY):**
Phone (area code):	**Email:**
County/Municipality:	**Office:**
Mailing address:	

Record Series Title A group of records as listed in records retention schedule	**Description of Records** Specific records as referred to in-office	**Inclusive Dates** (1987-1989; 2005-present)	**Approx. Volume of Records** (e.g. "1 file cabinet," "5 boxes")	**Retention Period** As listed in records retention schedule

Requested by: _____ Signature, _____ Requestor, _____ Date

Approved by: _____ Signature, _____ Requestor's Supervisor, _____ Date

Concurred by: _____ Signature, _____ Assistant Records Administrator, State Archives of North Carolina, _____ Date

Physical Address
215 N Blount St
Raleigh, NC 27601

State Courier 51-81-20
Facsimile (919) 715-3627
records@ncdcr.gov

9. Other Electronic Records Management Practices

System Planning

The County uses traditional paper media, electronic systems, or microfilm, for the creation and storage of records, based upon which media best serves the records retention requirements of unique records groups, as well as the administrative needs of the County. Any document that is considered to be a permanent record must be kept either as paper media or microfilm. Permanent records may be scanned and become a part of the document imaging and electronic records systems to provide for greater efficiency; however, they will still be maintained in either a paper media or microfilm form. The County monitors all computing resources and information systems for performance, storage, and supportability. Those systems identified as requiring upgrading or additional resources, are part of the annual budgeting process within the County.

Electronic Records Management

Information systems documentation, systems access records, digitized and scanned records, metadata, and other information maintained by the relevant information systems, are listed for the required amount of time according to approved records retention and disposition schedules, prior to their destruction or other disposition. All records produced by the County are retained for the period of time required by applicable local records retention and disposition schedules, regardless of format. Any permanent records maintained in electronic form also exist as a paper or microfilm preservation duplicate copy in compliance with the DCR's *Human Readable Preservation Duplicates* policy, or any similar successor policy.

Database Indexing

N.C.G.S**.** §132-6.1 requires that databases be indexed with certain fields, as also required by the DCR. Indexes shall contain at least the following data fields:

- Description of the format or record layout;
- Frequency with which the database is updated;
- List of all data fields;
- List of any data fields to which public access is restricted;
- Description of each form in which the database can be copied or reproduced using the County's computer facilities; and
- Schedule of fees for the production of copies in each available form.

Security and Disaster Backup and Restoration

The County has a disaster recovery plan for its electronic data in place, which includes contact information for data recovery vendors and information about backups of all data. Security backups to protect against data loss are generated for all but the most transitory of files. Routine backups are conducted daily. Backups are stored on a VTL, and the server volumes are also replicated to a disaster recovery SAN located off-site also.

Security backups of all imaged documents will be generated and maintained off-site. Imaged documents will be synchronized to a secured offsite location upon document changes or upon document scanning. A backup copy of the scanned data and imaged

documents and index database is created on a nightly basis for the purpose of document recovery.

10. Compliance and Electronic Records Self-Warranty

The completion of the form below (beginning on page 15 of this policy) by applicable records custodians signals that all employees of the service area/division under which the records custodian has the jurisdiction of particular records will adhere to the rules set forth in this policy. Furthermore, this section is to be used as a self-evaluation tool to ensure that electronic records produced by the County are created, reproduced, and otherwise managed in accordance with guidelines for electronic public records published by the DCR. The self-warranting of records in itself does *not* authorize the destruction of records, originals or copies, *nor* does it change current records retention and disposition scheduling procedures.

The government agency producing electronic records and/or reproductions is responsible for ensuring the records' authenticity and accuracy. The DCR is not responsible for certifying the authenticity or accuracy of any records, whether originals or reproductions, produced by the originating agency.

11. Commencement Date of Policy

This policy will become effective upon adoption, but because it will require changes to current practices that will necessitate extensive training of employees, the requirements of this policy will be deferred until such implementation date determined by the County Manager to be feasible, provided that such date will not be earlier than approval of this policy by DCR nor later than June 30, 2014.

Records Custodian

The records custodian is the person responsible for creating records or managing the staff who creates records. The records custodian certifies that:

_____ The records created or duplicated by electronic means in this office are prepared in accordance with these guidelines as indicated by the following statements:

- Quality - Records are legible, accurate, and complete.
- The records are produced or reproduced as part of a regularly conducted activity.
- The records conform to DCR guidance regarding file formats, file naming, and if applicable digital preservation guidance produced by DCR.
- Detailed, documented procedures are in place and followed when the records are created, copied, modified, or duplicated.
- The person(s) who creates, copies, modifies, or duplicates the records receives formal training on detailed system procedures prior to records preparation.
- Details of the training received are adequately documented through written policies and procedures.
- Training records are signed by employee after receiving training.

_____ This agency will comply with the best practices and standards established by the Department of Cultural Resources as published on its website.

_____ This agency will submit to the Department of Cultural Resources Section 8 of this policy, *Request for Disposal of Original Records Duplicated by Electronic Means*, to seek approval for the destruction of original records that have been converted from paper to electronic record.

Approved by: _____ Date: _____

Title : _____

Signature: _____

IT Professional or other Project Supervisor

The IT Professional is the person responsible for providing technical support to the records custodians and who may be involved in infrastructure and system maintenance. In the absence of an IT department, the supervisor of the records custodian should verify the following items. The IT Professional certifies that:

_____ Audit trails document the identity of the individual(s) who creates, duplicates, modifies, or otherwise prepares the records, what actions are taken by the individual during the course of the process, when these actions are taken, and what the results of these actions are.

_____ Audits:

_____

- are performed periodically to confirm that the process or system produces accurate results.
- confirm that procedures actually followed are in accordance with procedure stated in the system's documentation.
- are performed routinely on documents to ensure no information has been lost.
- are performed by an independent source (i.e., persons other than those who create the records or persons without an interest in the content of the records. Acceptable source may include different department or authorized auditing authority).
- are adequately documented.

_____ The process or system hardware and software are adequately documented

_____ Permanent records conform to all file format, file naming, and digital preservation guidance produced by the Department of Cultural Resources.

_____ Back up procedures are in place and comply with best practices, as established by the Department of Cultural Resources.

_____ Successful disaster recovery back up is completed at least once every two years.

Approved by: _____ Date:_____

Title: _____

Signature: _____

FOR DEPARTMENT OF CULTURAL RESOURCES USE

Approved by: _____ Date:_____

Title: _____

Signature: _____