Electronic Records and Imaging Policy and Procedures

City of Winston-Salem

City of Winston-Salem

April 2024
Version 1.0

Winston-Salem

NC DEPARTMENT
OF NATURAL AND
CULTURAL RESOURCES

This policy is modeled after the Department of Natural and Cultural Resources guidance document *Guidelines for Managing Trustworthy Digital Public Records*[1]. This policy applies to both born-digital electronic records and electronic records generated by imaging systems. Elements specific to state or local agencies are noted and should be adopted accordingly. This policy should be tailored by the party responsible for the custodianship of an agency's or department's electronic records to the agency's specific electronic records management practices wherever applicable and should provide as much detail as possible. This policy incorporates two additional forms, the *Electronic Records Self-Warranty* form and the *Request for Disposal of Original Records Duplicated by Electronic Means* form.

The North Carolina Department of Natural and Cultural Resources requires that any agency that images its records as part of its records retention practices sign this policy after tailoring it to meet agency needs. This policy is also a requirement for agencies maintaining electronic records that have retention periods of ten or more years.

Subject: ____________________ Policy Number: ____________________
Effective date: ____________________ Modified date: ____________________

Type of Government Office: □ County □ Municipal □ State Agency □ Other*
For Other, enter name of "parent" agency
unless unassigned: ____________________
County/Municipality/Agency: ____________________
Name of Office: ____________________
Office Address: ____________________
Phone: ____________ Fax: ____________ Email: ____________

*Includes assigned and unassigned offices (authorities, boards, bureaus, commissions, councils, private/public hybrid entities, etc.)

[1] https://archives.ncdcr.gov/documents/guidelines-managing-trustworthy-digital-public-records

Table of Contents

1. Purpose

The Purpose of this Policy is to protect all records including those that are permanent. The records covered by this policy are in the custody of employees of the City of Winston-Salem and are maintained for the benefit of agency use in delivering services and in documenting agency operations. This electronic records policy reflects guidelines established in the North Carolina Department of Natural and Cultural Resources publication *Guidelines for Managing Trustworthy Digital Public Records.*[2] Complying with this policy will increase the reliability and accuracy of records stored in information technology systems and will ensure that they 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 North Carolina G.S. § 132-1 are covered by this policy. This includes permanent and non-permanent records, including both 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 department in imaging, indexing, auditing, backing up, and purging electronic records in accordance with the disposition schedule, and in handling the original paper records, if applicable.

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

The form provided in Section 9 of this document, *Request for Disposal of Original Records Duplicated by Electronic Means*, is completed and submitted to the Department of Natural and Cultural Resources whenever this agency wishes to dispose of a series of paper records that have been digitized.

This policy will supersede any electronic records system policy previously adopted. This policy will be reevaluated at a minimum of every five years, or upon the implementation of a new information technology system, and will be updated as required. A copy of this policy will remain on file at the Department of Natural and Cultural Resources.

2. Responsible Parties

- Managerial Staff
- Information Systems Department
- Records Creators

Managerial Staff

Responsibilities include:

1. Determining access rights to the system
2. Approving system as configured by the Information Systems Department

[2] https://archives.ncdcr.gov/documents/guidelines-managing-trustworthy-digital-public-records

Information Systems Department

Responsibilities include:

1. Installing and maintaining equipment and software
2. Configuring the system according to agency needs, including creating and testing applications and indexes
3. Controlling permission rights to the system
4. Maintaining documentation of system hardware and software
5. Establishing audit trails that document actions taken on records stored by the information technology system
6. Providing backups for system records and recovering deleted imaged records when necessary
7. Completing a disaster recovery backup at least once every two years
8. Establishing and providing training on equipment and software, documenting such training, and providing remedial training as needed. Such training includes, but is not limited to, training on the imaging system.
9. Creating and updating detailed procedural manuals describing the imaging process and equipment
10. Conducting any necessary batch conversions or batch renaming of imaged records

Records Creators

Responsibilities include:

1. Participate in training conducted by appropriate staff
2. Creating passwords for computers that are long, complex, and frequently changed
3. Creating and managing electronic records in their purview in accordance with the policies and other guidance issued by the Department of Natural and Cultural Resources and complying with all Information Systems Department security policies
4. Reviewing system records annually and purging records in accordance with the retention schedule
5. Guaranteeing that records, regardless of format, be retained for the period of time required by local records retention schedules
6. Carrying out day-to-day processes associated with the agency's imaging program, including:
    - Designating records to be entered into the imaging system
    - Noting confidential information or otherwise protected records and fields
    - Removing transitory records from the scanning queue
    - Completing indexing guide form for each record being scanned
    - Reviewing images and indexing for quality assurance
    - Naming and storing the scanned images in designated folders
    - Once approved, destroying or otherwise disposing of original records in accordance with guidance issued by the Department of Natural and Cultural Resources
7. Public employees who have been approved to telecommute or use mobile computing devices must:
    - Comply with all information technology security policies, including the agency and statewide acceptable use policies, as well as all statutes and policies governing public records
    - Back up information stored on the mobile device daily to ensure proper recovery and restoration of data files
    - Keep the backup medium separate from the mobile computer when a mobile computer is outside a secure area

3. Availability of System and Records for Outside Inspection

This agency recognizes that the judicial system may request pretrial discovery of the information technology system used to produce records and related materials. Agency personnel will honor requests for outside inspection of the system and testing of data by opposing parties, the court, and government representatives. Records must be available for inspection and audit by a government representative for the full period required by law and approved records retention schedules, regardless of the life expectancy of the media on which the records are stored. Records must continue to exist when litigation, government investigation, or audit is pending or 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 agency's electronic records into evidence, the agency 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; and evidence of the records' chain of custody. In addition to this policy, such documentation includes:

- Procedural manuals
- System documentation
- Training documentation
- Audit documentation
- Audit trails documenting access permission to records

The agency will also honor inspection and copy requests pursuant to N.C. G.S. § 132. The agency should produce the records created and used in the course of business, maintaining established folder structure as applicable. The agency should produce records in any format it is capable of producing if asked by the requesting party; however, the agency is not required to create or compile a record that does not already exist. If it is necessary to separate confidential from non-confidential information in order to permit the inspection or copying of the public records, the public agency will bear the cost of such separation.

4. Maintenance of Trustworthy Electronic Records

- Produced by Methods that Ensure Accuracy
- Maintained in a Secure Environment
- Associated and Linked with Appropriate Metadata
- Stored on Media that are Regularly Assessed and Refreshed

Produced by Methods that Ensure Accuracy

All platforms used by the agency to create and manage electronic records, including e-mail clients, social media platforms, and cloud computing platforms, conform with all Department of Natural and Cultural Resources policies and all applicable Information Systems Department security policies.

Electronic files are saved in formats that comply with DNCR's *File Format Guidelines for Management and Long-Term Retention of Electronic Records.*[3] File formats used by the agency are identified as standard by DNCR and are well-supported and have robust metadata support.

[3] http://archives.ncdcr.gov/documents/file-format-guidelines-management-and-long-term-term-retention-electronic-records

Maintained in a Secure Environment

Security of the system and the records it holds is maintained in the following ways:

- Access rights are managed by the Information Systems Department and/or business unit are approved by a supervising authority to prevent unauthorized viewing of documents.
- Either the information technology system is able to separate confidential from non-confidential information, or data creators must organize and name file systems in such a way to identify confidentiality of the documents.
- Folders with confidential information are restricted, and access rights to confidential data are carefully managed. Confidential material is redacted before it is shared or otherwise made available.
- Physical access to computers, disks, and external hard drives is restricted.
- All system password and operating procedure manuals are kept in secure off-site storage.

Associated and Linked with Appropriate Metadata

Metadata that is essential for a file's current user and/or retention is maintained alongside the record[4]. At a minimum, metadata retained includes file creator, date created, file name, and when appropriate, cell formulae and e-mail header information.

Stored on Media that are Regularly Assessed and Refreshed

Data is converted to new usable file types as old ones become obsolete. The following steps are taken to ensure the continued accessibility of records kept in electronic formats:

- Data is audited and assessed annually. If there is evidence of file corruption, data should be migrated to new media.
- Records are periodically verified through hash algorithms. This is required before and after transfer to new media to ensure the records were not altered.
- Media is refreshed every three to five years. The agency documents when and how records are transferred from one storage medium to another. Once the new media has been sampled to assure the quality of the transfer, the original media may be destroyed according to the guidelines of 07 NCAC 04M .0510.
- Records are periodically migrated to new file types, particularly when a new information technology system requires that they be brought forward in order to render the file properly.
- Metadata is maintained during transfers and migrations.
- Storage media are maintained in a manner and in an environment that promotes bit-level preservation. The agency adheres to the media manufacturer's recommendations for specific environmental conditions in which the media should be stored.
- Whatever media is used to store data is clearly labeled with enough information that its contents can be determined (e.g., optical media should have a physical label; data stored on a server should be indexed).

[4] For more information, see DNCR's guidance document *Metadata as a Public Record in North Carolina: Best Practices Guidelines for Its Retention and Disposition* (https://archives.ncdcr.gov/Portals/3/PDF/guidelines/Metadata_guideliens.pdf)

5. Components of Information Technology Systems

- Training Programs
- Audit Trails
- Audits

Training Programs

The Information Systems Department will conduct training for system use and electronic records management, using material published by the Department of Natural and Cultural Resources when appropriate. All employees will be made aware of system procedures and policies and trained on them; employees will acknowledge by initialization or signature that they are aware of the policies and have received training on them. When appropriate, employees will also attend trainings offered by the Department of Natural and Cultural Resources on the maintenance of electronic records. Documentation will be maintained for the distribution of written procedures, attendance of individuals at training sessions and refresher training programs, and other relevant information.

Audit Trails

At a minimum, the Information Systems Department will maintain documentation on who has read and/or write permission to files maintained by the agency. Ideally, a log of activities on the system is maintained, which shows who accessed the system, how and by whom records were created and modified, and whether standard procedures were followed.

Audits

Audits are designed to evaluate the process or system's accuracy, timeliness, adequacy of procedures, training provided, and the existence of audit trails. Internal audits are conducted regularly by agency Information Systems Department staff, at least annually.

6. Documentation of Information Technology System

- System Design
- Retention of System Documentation

System Design

The agency maintains documentation that describes system procedures, practices, and workflows. This documentation also identifies system software and hardware and captures the system environment in terms of the organizational structure, functions and responsibilities, and system processes. It explains how the system operates from a functional user and data processing point of view. Documentation is reviewed and updated by Information Systems Department staff as required for compliance or upon implementation of a new information technology system. Such documentation maintained by the agency includes:

- Procedural manuals
- System documentation
- Security backup and disaster recovery procedures as a part of the Continuity of Operations Plan
- Service level agreements for contracted information technology services

Retention of System Documentation

All system documentation will be maintained during the period for which the records produced by the process or system 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. All such documentation is listed in the City of Winston-Salem's records retention schedule.

7. Digital Imaging Program Documentation and Procedures

- System and Procedural Documentation
- Training
- Indexing and Metadata
- Auditing and Audit Trails
- Retention of Original and Duplicate Records

System and Procedural Documentation

The Information Systems Department is responsible for preparing and updating detailed procedures that describe the process followed to create and manage imaged electronic records. This documentation will include a description of the system hardware and software. A current procedural manual will be maintained to ensure the most current steps are followed and to ensure reliable system documentation will be available for judicial or similar proceedings.

Each workstation designated as a scanning station will have, at a minimum, the following hardware and software, unless the scanner is collocated by means of a network interface:[5]

- Document/image scanner authorized by the Information Systems Department
- Driver software for scanner
- Imaging software
- Instructions manual, maintained by Information Systems Department staff, describing in detail the steps required in the scanning 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 used for scanned images
    - Whether batch conversion or batch file re-naming will be necessary, and what tool is used for such conversions
    - Whether any image enhancement techniques should be conducted after imaging

Training

Only designated staff that have been formally trained on the use of the imaging software and equipment will be allowed to scan records.

[5] If your scanner is networked, you will only have one response to each of the first three items. If you have separate workstations throughout your agency, we recommend an inventory that specifies the equipment and software used at each workstation.

Components of the training will include basic techniques for image capture, indexing, quality control, security configuration, auditing, use of equipment, and general system maintenance. Permissions to image and index records will not be assigned until the user has been trained. If a user improperly indexes or scans a document, an auditor will address this occurrence with the user, and remedial training will be required.

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 images stored. This index should capture the content, structure, and context of the imaged records and will be developed by Information Systems Department staff prior to the implementation of any imaging system. Metadata will be maintained in accordance with the guidelines provided in Section 4, *Maintenance of Trustworthy Electronic Records*.

Auditing and Audit Trails

Staff trained to conduct imaging 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
- Other features of records such as color, shape, texture, etc., that relate to the content of the information

Managerial staff for the various units of the agency will also periodically audit imaged records for accuracy, readability, and reproduction capabilities. Written quality control documentation will be prepared indicating the sampling of records and what remedial procedures were followed if the expected level of accuracy was not achieved.

For contracted imaging systems, audit trails should be built into the imaging system that will automatically document who creates, duplicates, modifies, or otherwise accesses records and what procedures were taken. 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
- E-mail 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 imaging, this agency will complete Section 9 of this document, *Request for Disposal of Original Records Duplicated by Electronic Means*. For each records series identified for scanning, the Department of Natural and Cultural Resources must approve the destruction of the original records. Permanent records may be imaged for ease of access, but the original documents may not be destroyed unless a digital copy exists prior to the records' destruction.[6]

Destruction of original records is allowed only after quality assurance has been conducted on the imaged records, necessary corrections have been made, the electronic records system is audited for accuracy, and the destruction of records has been approved.

If digital images replace the original records and assume all legal authorities, these scanned records will be considered the record copy and must be maintained for the specified retention period defined in the appropriate records retention and disposition schedule.[7] The retention period is considered to have begun when the original document was created, not when the electronic version was produced. Any hard copy generated from the imaged records will be considered the agency's duplicate "working" record or reference copy.

For any outsourced scanning, a copy of the purchase order and a detailed service level agreement will be maintained. See Section 8 of this policy, *Other Electronic Records Management Practices,* for more information on contracting out electronic records management services.

8. Other Electronic Records Management Practices

- Shared Drive Management
- Security and Disaster Backup and Restoration
- Vendor-Provided Services/Hosted Solutions

Shared Drive Management

Employees use shared storage for collaboration and access. Procedures for the use of this shared storage comply with DNCR's guidance document *Global Shared Storage Guidelines*.[8]

Security and Disaster Backup and Restoration

The agency 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 in real-time and/or daily and are stored in secure

[6] Any permanent records maintained in electronic form must also exist as a paper or microfilm preservation duplicate copy in compliance with the Department of Natural and Cultural Resources *Human-Readable Preservation Duplicates* policy.

[7] The Society of American Archivists *Glossary of Archival and Records Terminology* defines record copy as "the single copy of a document, often the original, that is designated as the official copy for reference and preservation." Available at http://www2.archivists.org/glossary/terms/r/record-copy.

[8] https://archives.ncdcr.gov/documents/global-shared-storage-guidelines

off-site storage. **See *Security Backup Files as Public Records in North Carolina: Guidelines for the Recycling, Destruction, Erasure, and Re-use of Security Backup Files* for guidance on the appropriate retention and destruction of backup files.**[9] Imaged documents will be synchronized to a secured offsite location immediately upon document changes or upon document scanning.

Vendor-Provided Services/Hosted Solutions

The terms of the service level agreement with **all third-party contractors shall include:**

- File formats
- Plan for converting files to a new format
- File naming practices
- Access rights/security mechanisms
- Backups (specify frequency and location)
- Mechanism for destructions
- Audits (data should be audited at least annually to test accessibility and assess need for refresh or migration)
- Frequency of refreshing of media (should be at least every 3-5 years)
- Frequency of checksum validation (should be at least at every migration)
- Environmental conditions where media is stored (humidity 30-50%, temperature 65-75°F)
- Training program
- Disaster recovery procedures
- System documentation/procedural manual – a copy should be provided to the agency that specifies what hardware and software are provided by the vendor
- System for indexing records
- Quality control procedures
- Mechanism for document production due to litigation, audit, or public records request
- Mechanism for avoiding spoliation of evidence
- Costs for:
  - Uploading records
  - Downloading records
  - Migrating records
  - Service termination
  - Proprietary software necessary to access records (if applicable)
- Performance/availability (e.g., planned and unplanned downtime)
- Ownership of data
- Procedure for exporting records (including images as well as metadata) at end of contract period and/or when vendor ceases operation

[9] https://archives.ncdcr.gov/documents/security-backup-files-public-records-north-carolina

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

This form is used to request approval from the Department of Natural and Cultural Resources to dispose of **non-permanent** paper records that 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 that have been microfilmed or photocopied.[10]

[10] Please contact a Records Analyst with any questions about the destruction of original paper records.

NC DEPARTMENT OF
NATURAL AND CULTURAL RESOURCES

GOVERNMENT RECORDS SECTION
STATE RECORDS CENTER

archives.ncdcr.gov   4615 Mail Service Center, Raleigh NC 27699-4165   919-814-6900

Request for Disposal of Original Records Duplicated by Electronic Means

If you have questions, call (919) 814-6900 and ask for a Records Management Analyst.

This form is used to request approval from the Department of Natural and Cultural Resources to dispose of non-permanent paper records that 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 that 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:	

Records 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   Title   Date

Approved by:

Signature   Requestor’s Supervisor   Date

Concurred by:

Signature   Assistant Records Administrator
State Archives of North Carolina   Date