REQUEST FOR BOARD ACTION

HENDERSON COUNTY

BOARD OF COMMISSIONERS

MEETING DATE: **21 September 2016**

SUBJECT: **Digital public records retention policy**

PRESENTER: **Charles Russell Burrell**
Becky Snyder

ATTACHMENT(S): **Proposed policy**

SUMMARY OF REQUEST:

Attached is a proposed digital public records retention policy, which insures that the County's retention of electronic records is in compliance with the regulations promulgated by the Division of State of Archives of the Department of Natural and Cultural Resources of North Carolina. Staff arrived at this proposal after a great deal of colloquy with the Division representative. It is intended to make sure that all County electronic public records are maintained and disposed of in accordance with the schedules for retention set out by the Division.

County staff will be present and prepared if requested to give further information on this matter.

BOARD ACTION REQUESTED:

Approval of the proposed policy.

If the Board is so inclined, the following motion is suggested:

I move that the Board adopt the proposed Digital Public Records Retention policy.

Before the
Board of Commissioners
Of Henderson County

A POLICY REGARDING
PUBLIC DIGITAL RECORDS RETENTION

Dated September 21, 2016

This policy covers all of the government of the County of Henderson, including all departments, constituent and appointed boards and other subdivisions or units thereof under the authority of the Board of Commissioners of Henderson County.

County of Henderson
1 Historic Courthouse Square
Hendersonville, North Carolina 28792

Table of Contents

Purpose

The records covered by this policy are in the custody of the County of Henderson, a body corporate and politic of the State of North Carolina ("the County"), and are maintained for the benefit of the County's use in delivering services and in documenting operations. This electronic records policy reflects guidelines set in the North Carolina Department of Cultural Resources publication, *Guidelines for Managing Trustworthy Digital Public Records.*

All public records as defined by North Carolina Gen. Stat. § 132-1 *et seq.* 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 department in imaging, indexing, auditing, backing up, and purging electronic records in accordance with the disposition schedule, and in handling the original paper record, if applicable.

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

The form provided in Section 8 of this document, Request for Disposal of Original Records Duplicated by Electronic Means, is to be completed and submitted to the Department of Natural and Cultural Resources whenever the County wishes to dispose of a new 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.

Responsible Parties and Their Responsibilities

The parties with responsibilities under this policy include:

- Department Directors
- Henderson County Information Technology Department ("IT")
- Records Creators

Department Directors: For the purpose of this policy, department directors include the chairs of committees appointed by the Board of Commissioners, all department directors of County government, and the County Manager, the Assessor and the County Attorney.

The responsibilities of department directors include:

1. Determining access rights to the system
2. Approving system as configured by IT
3. Performing quality assurance checks by sampling the department's imaged records before the original documents are destroyed.

IT Department: The responsibilities of the Henderson County Information Technology Department include:

1. Installing and maintaining equipment and software
2. Configuring the system according to department needs, including creating and testing applications and indexes
3. Controlling access 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 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

Records Creators: The responsibilities of creators of public records include:

1. Attending and signing off on training conducted by IT staff or by the Department of Natural and Cultural Resources
2. Creating passwords for computers that are long, complex, and frequently changed
3. Creating and managing electronic records in their purview in accordance with these policies and other guidance issued by the Department of Natural and Cultural Resources, and complying with all IT security policies
4. Reviewing the system records annually and purging records in accordance with the retention schedule
5. Carrying out day-to-day processes associated with the County's imaging program, including:
   - Designating records to be entered into the imaging system
   - Noting confidential information or otherwise protected records and fields
   - Removing transient records
   - 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.
   - Conducting any necessary batch conversions or batch renaming of imaged records
6. Any employees who have been approved to telecommute or use mobile computing devices must:
   - Comply with all information technology security policies, including the County 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

Availability of System and Records for Outside Inspection

The County recognizes that the judicial system may request pretrial discovery of the information technology system used to produce records and related materials. The County's personnel will honor lawful requests for outside inspection of the system and testing of data by opposing parties, the court, and other 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, 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; 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

The County will also honor inspection and copy requests made pursuant to the terms and provisions of Chapter 132 of the North Carolina General Statutes, subject to any exclusions of information or records required by law. The County should where practicable produce the records in the order they were created and used in the course of business, and in the format in which they were created. However, the County may produce the records in any format it is capable of producing if asked by the requesting party, subject to the provisions of N.C. Gen. Stat. §132-6.2.

Maintenance of Trustworthy Electronic Records

The County's electronic records should be:

- 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

All platforms used by the County to create and manage electronic records, including email clients, social media platforms, and cloud computing platforms, should conform with all North Carolina Department of Natural and Cultural Resources' ("DNCR") policies and all applicable security policies.

Where shortened or abbreviated names are required, or where document management systems are not employed, electronic files should be named generally in accordance with the *Best Practices for File-Naming* published by the DCR.

Electronic files are saved in formats that comply with DCR's *File Format Guidelines for Management and Long-Term Retention of Electronic Records,* which may presently be found on the internet at (*http://archives.ncdcr.gov/Portals/3/PDF/guidelines/file_formats_in-house_preservation.pdf*). File formats used by the state are adopted as standard by the County.

Security to the records system and to the records it holds should be maintained in the following ways:

- Access rights are managed by the IT department, and are determined by a supervising authority to prevent unauthorized viewing of documents.
- The information technology system is able to separate confidential from nonconfidential information, or data creators organize and name file systems to reflect confidentiality of documents stored within.
- 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 restricted.
- Duplicate copies of digital media and system backup copies are stored in offsite facilities in order to be retrieved after a natural or human-made disaster.
- Confidential material is redacted prior to publication of records.
- All system password and operating procedure manuals are kept in secure off- site storage (e.g. a bank safety deposit box).

Metadata is maintained alongside the record. At a minimum, metadata retained should include file creator, date created, title (stored as the file name), and when appropriate, cell formulae and email header information. Employees are not instructed to create metadata other than metadata that is essential for a file's current use and/or retention.

Data should be converted to new usable file types as old ones become obsolete or otherwise deteriorate. The following steps should be 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. The County 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 migrated forward in order to properly render the file
- Metadata is maintained during migration
- Records are periodically verified through hash algorithms. This is done before and after migration to new media to ensure that the record did not change during 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 should adhere to the media manufacturer's recommendations for specific environmental conditions in which the media should be stored.
- Whatever media is used to store imaged data is clearly labeled with enough information that its contents can be determined.

Components of the Information Technology System

The County Information Technology System includes the following:

- Training Programs
- Audit Trails
- Audits

Training Programs
The IT 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, trained on them, and confirm by initialization or signature acknowledging 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.

System Audit Trails
A log of activities on the system is maintained, which show who accessed the system, how and by whom records were created and modified, and whether standard procedures were followed.

Quality 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 the County's IT staff.

Documentation of the Information Technology System

The County's Information Technology System will have adequate documentation.

The County will maintain system documentation that describes system procedures and actual practices, as well as system software and hardware, and 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 regularly or upon implementation of a new information technology system by IT staff. Such documentation maintained by the County includes:

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

One set of 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 new operating environment. All such documentation is listed in the County's records retention schedules.

Digital Imaging Program Documentation and Procedures

Digital Imaging within the County's operations includes the following:

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

The IT department is responsible for preparing and updating detailed procedures that describe the process followed to create and recreate electronic records. This documentation should include a description of the system hardware and software. A current procedural manual should be maintained to assure the most current steps are followed.

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:

- Document/image scanner authorized by IT (as approved by IT)
- Driver software for scanner
- Imaging software (as approved by IT)
- Instructions manual, maintained by IT staff, describing in detail the steps required to get from the beginning to the end of the 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
  - If batch conversion or batch file re-naming will be necessary, and what tool is used for such conversions
  - How the scanned images will be stored in the file system
  - Any image enhancement techniques conducted after imaging

Only designated staff that have been formally trained by IT staff and signed off on training documentation on the use of the imaging software and equipment will be allowed to enter records into the content management system. Covered records will be scanned and filed as part of an ongoing regularly conducted activity. 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 the user has been trained. If a user improperly indexes or scans a document, an auditor will address this occurrence with the operator and remedial training will be performed as necessary.

All imaged records must be indexed in order to facilitate efficient retrieval, ease of use, and up-to-date information about the images stored in the system. This index should capture the content, structure, and context of the imaged records, and will be developed by IT staff prior to the implementation of any imaging system. It should also be indexed according to guidelines set by the Department of Natural and Cultural Resources (see this policy, **Other Electronic Records Management Practices**, for more information on database indexing).

The imaging staff 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 County will also periodically audit imaged records for accuracy, readability, and reproduction capabilities. 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 imaging system will automatically document who creates, duplicates, modifies, or otherwise prepares 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
- Email document
- Export document
- Index creation/deletion/modification
- Insert page
- Log in/out
- Move document
- Move pages
- Print document

To obtain permission to destroy original records following imaging, the County will complete the *Request for Disposal of Original Records Duplicated by Electronic Means*. For each new records series to be scanned, 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 an analog copy exists prior to the records' destruction.

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, and the destruction is approved. Prior to destruction of the original record, managerial staff will audit a sample of those records to verify the accurate reproduction of those records.

Digital images of scanned records are maintained for the specified retention periods according to the records retention and disposition schedule. The retention period is considered to have begun when the original document was created, not when the electronic reproduction was created.

Electronic and digital images of scanned records in a document management system will be considered the "official" record. Any hard copy generated from the imaged records will be considered the County's duplicate "working" record.

Request for Disposal of Original Records Duplicated by Electronic Means

The attached form, *Request for Disposal of Original Documents Duplicated by Electronic Means*, is used to request approval from the Department of Natural and 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.

Other Electronic Records Management Practices

The County's other electronic records management practices include:

- System Planning
- Electronic Records Management
- Database Indexing
- Security and Disaster Backup and Restoration

The County should use traditional paper media, electronic systems, or microfilm, based on what format best serves the records retention requirements of unique records groups, given reasonable budgetary forecasting.

System documentation, system access records, digitization and scanning records, metadata, and information maintained by that system is listed in an approved records retention and disposition schedule prior to their destruction or other disposition.

County records are retained for the period of time required by local records retention 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 Department of Cultural Resources' Human-Readable Preservation Duplicates policy.

N.C. Gen. Stat. §132-6.1 requires that databases be indexed with the Department of Natural and Cultural Resources. The County's database indexes contain the following data fields:

- Description of the format or record layout
- Frequency with which the database is updated
- 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 agency's computer facilities
- Schedule of fees for the production of copies in each available form

The County has a disaster recovery plan for its electronic data in place, which includes contact information for data recovery vendors and information about back-ups of all data. Security back-ups to protect against data loss are generated for all but the most transitory of files. Routine back-ups are conducted regularly, and stored in secure off-site storage as documented in the County's I.T. disaster recovery plan.

Contracting

Department Heads shall insure that all agreements with vendors hosting applications offsite (ASP or SaaS) are reviewed by the Information Technology Department and the County Attorney prior to execution. All such agreements must include documentation that the vendor has implemented

information security policies, including policies for access control, application and system development, operational, network and physical security to ensure the security of Henderson County data. Each vendor shall be contractually obligated to comply with card association security standards if credit card transactions are part of the contract. Finally, each vendor must be contractually obligated to provide free access to the County's data, in a mutually agreed form, at the termination of any such contract.

Compliance and Electronic Records Self-Warranty

The completion of this form attests that all County employees will adhere to the rules set forth in this policy.

Records Custodian: The records custodian is the person responsible in each County department or office for creating records or managing the staff who creates records.

Each records custodian certifies that:

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

- The records are of high quality - legible, accurate, and complete.
- The records are produced or reproduced as part of a regularly conducted activity.
- The records conform to DNCR guidance regarding file formats, file naming, and if applicable digital preservation guidance produced by DNCR.
- 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 DNCR as published on its website.

_____ This agency will submit to the DNCR pursuant to this policy, **Request for Disposal of Original Records Duplicated by Electronic Means**, documentation seeking approval for the destruction of original records that have been converted from paper to electronic record.

Approved by:

Date:
Title:

_____
Signature:

Information Technology Department Self-Warranty on behalf of Henderson County::

The IT Department is responsible for providing technical support to the records custodians and is involved in infrastructure and system maintenance.

The IT Department Head hereby 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 generally to all file format, file naming, and digital preservation guidance produced by the DNCR.

_____ Back up procedures are in place and comply with best practices, as established by the
DCR.

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

Approved by:

Date:

Title:

_____
Department Head

Sample Electronic Records and Imaging Policy and Procedures

For Use by Local and State Agencies

March 2016
Version 2.0

State Archives of North Carolina
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 model 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 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. When completing this policy, delete portions that are bold and in brackets; these sections either contain optional language or are intended for guidance purposes only.]

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] http://archives.ncdcr.gov/Portals/26/PDF/guidelines/guidelines_for_digital_public_records.pdf

Table of Contents

1. Purpose

[Describe the purpose of this policy. What records does it protect, what information technology systems are used by the agency, and when will this policy be updated?]

The records covered by this policy are in the custody of **[agency name]** 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.

[Applicable to agencies with an imaging program] This policy also serves to protect those records digitized by the agency's **[specify in-house or contracted]** imaging system, 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.

[Applicable only to local agencies – state agencies should delete this reference along with Section 10 of this document] The form provided in Section 10 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

[Describe the electronic records management responsibilities of the persons or departments responsible for adhering to this policy. Tailor this section to reflect the actual parties and their responsibilities within your agency. To go into effect, this policy will be signed by the individuals listed.]

- Agency Supervisor/Division Director
- Managerial Staff
- IT Department
- **[For state agencies]** Chief Records Officers
- Records Creators

[2] http://archives.ncdcr.gov/Portals/26/PDF/guidelines/guidelines_for_digital_public_records.pdf

Agency Supervisor/Division Director

Responsibilities include:

1. **[For state agencies]** Appointing Chief Records Officers
2. Determining access rights to the system
3. Approving system as configured by IT

Managerial Staff

Responsibilities include:

1. Ensuring training of records creators
2. **[For agencies with an imaging program]** Periodically auditing imaged records for accuracy, readability, and reproduction capabilities before the original documents are destroyed

IT 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. **[For agencies with an imaging program]** Creating and updating detailed procedural manuals describing the imaging process and equipment
10. **[For agencies with an imaging program]** Conducting any necessary batch conversions or batch renaming of imaged records

[For state agencies] Chief Records Officer

Responsibilities include:

1. Coordinating with the Government Records Section all agency requests for records assistance, training, and other offered consultative services
2. Coordinating interactions between the agency business units and the Department of Natural and Cultural Resources in preparing an inclusive inventory of and schedule for records in agency custody and in establishing a time period for the retention and disposal of each records series
3. Assuring that public records are kept in secure but accessible places
4. Assisting in the timely transfer of semi-active records to the State Records Center
5. In cooperation with the Department of Natural and Cultural Resources, establishing and maintaining a program for the selection and preservation of agency records considered essential to the operation of government and to the protection of the rights and interests of citizens
6. Overseeing the design and implementation of electronic records initiatives

Records Creators

Responsibilities include:

1. Attending and signing off on training conducted by IT staff or by the Department of Natural and Cultural Resources
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 IT security policies
4. Reviewing system records annually and purging records in accordance with the retention schedule
5. **[For state agencies]** Guaranteeing that records, regardless of format, be retained for the period of time required by agency records retention schedules and/or the General Schedule for State Agency Records
6. **[For local agencies]** Guaranteeing that records, regardless of format, be retained for the period of time required by local records retention schedules
7. **[For agencies with an imaging program]** 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
8. **[Applicable to public employees approved to telecommute or use mobile devices]** 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

[Describe how the agency complies with requests for pretrial discovery of the agency's electronic records, and how the agency intends to lay a proper foundation for ensuring the admissibility of its records into evidence should legal proceedings arise. Also describe how the agency complies with public records requests for records maintained electronically.]

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

[Describe the processes by which electronic records are produced and managed, including how a record is created, named, saved, accessed, and transferred from one storage medium to another.]

- 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 IT security policies.

Electronic files are named in accordance with the *Best Practices for File Naming* published by the Department of Natural and Cultural Resources.[3] **[Define your agency's file naming standards. What abbreviations are used? What kind of file structure is used?]**

Electronic files are saved in formats that comply with DNCR's *File Format Guidelines for Management and Long-Term Retention of Electronic Records.*[4] File formats used by the agency are identified as standard by DNCR and are well-supported, backwards compatible, and have robust metadata support.

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 IT department and are assigned by a supervising authority to prevent unauthorized viewing of documents.

---

[3] http://archives.ncdcr.gov/Portals/3/PDF/guidelines/filenaming.pdf

[4] http://archives.ncdcr.gov/Portals/26/PDF/guidelines/file_formats_in-house_preservation.pdf

- 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. **[specify which]**
- Folders with confidential information are restricted, and access rights to confidential data are carefully managed. Confidential material is redacted **[define how]** 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 is maintained alongside the record. At a minimum, metadata retained includes file creator, date created, title (stored as the file name), and when appropriate, cell formulae and e-mail header information. Employees are not instructed to create metadata other than metadata that is essential for a file's current use and/or retention.[5]

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. Humidity does not exceed 50% and should not fall below 30%. Room temperature is set between 65° F to 75° F. 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).

5. Components of Information Technology System

[Describe how the agency ensures that its employees use the information system consistently and as intended. Describe what procedures are in place, what documentation is maintained, and what auditing controls are in place to ensure compliance and accuracy.]

- Training Programs
- Audit Trails

---

[5] See DNCR's guidance document *Metadata as a Public Record in North Carolina: Best Practices Guidelines for Its Retention and Disposition* (http://archives.ncdcr.gov/Portals/3/PDF/guidelines/Metadata_Guidelines.pdf) for more information.

- Audits

Training Programs

The IT 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 IT 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 IT staff, at least **[annually]**.

6. Documentation of Information Technology System

[Describe what is contained within system documentation, who maintains it, and its retention period.]

- 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 IT staff **[annually]** 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

One set of 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 **[agency's, county, or municipal]** records retention schedule.

7. Digital Imaging Program Documentation and Procedures

[If your agency has or will be implementing an imaging program, describe the system in detail (including any hardware and software components), procedures for maintaining and operating the system, and how original and imaged records are managed.]

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

System and Procedural Documentation

[Document the information technology system used to produce and manage the agency's imaged records. This section should describe the system hardware and software, the system environment in terms of the organizational structure, functions and responsibilities, and the system processes. Documentation should be complete and up-to-date. If the agency outsources digital imaging, the service level agreement should describe the operating environment and equipment. See Section 8 of this document, *Other Electronic Records Management Practices*, for more about contracting.]

[Example] The IT 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:[6]

- Document/image scanner authorized by IT **[specify scanner manufacturer and model number]**
- Driver software for scanner **[specify]**
- Imaging software **[specify]**
- Instructions manual, maintained by IT 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

[For agencies that scan in-house] Only designated staff that have been formally trained by IT staff and have signed off on training documentation on the use of the imaging software and equipment will be allowed to scan records. 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

[6] 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.

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 IT staff prior to the implementation of any imaging system. It should also be indexed according to guidelines set by the Department of Natural and Cultural Resources **[see Section 8 of this policy, *Other Electronic Records Management Practices*, for more information on database indexing]**. 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

[For agencies that scan in-house] Managerial staff will document by position title employees that have the authority to complete each of the tasks listed.

Retention of Original and Duplicate Records

[For state agencies] The agency's records analyst at the Department of Natural and Cultural Resources will be contacted to amend the agency's records retention schedule to allow for the destruction of original records following imaging.

[For local agencies] To obtain permission to destroy original records following imaging, this agency will complete Section 10 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 an analog copy exists prior to the records' destruction.[7]

[For state and local agencies] 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.[8] 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 agencies that outsource scanning] A copy of the purchase order and a detailed service level agreement with **[name of third-party organization]** is 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

[Describe the agency's other electronic records management practices.]

- System Planning
- Shared Drive Management
- Database Indexing
- Security and Disaster Backup and Restoration
- **[For agencies that contract electronic records management services to third-party vendors]** Contracting

System Planning

[Explain for what purposes the agency uses traditional paper media, electronic systems, or microfilm, based on what format best serves the records retention requirements of unique records groups. Also explain how the agency plans for hardware and software updates, particularly how it takes future budgetary implications into consideration.]

---

[7] 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.

[8] 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.

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*.[9]

Database Indexing

G.S. § 132-6.1 requires that databases be indexed with the Department of Natural and Cultural Resources. Data fields are indexed in accordance with guidelines provided in DNCR's *Public Database Indexing Guidelines*.[10]

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 **[define how often backups are conducted]** and are stored in secure off-site storage **[define where backups are stored, and on what type of storage media]**. **[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.[11]]**
[For agencies with imaging programs] Imaged documents will be synchronized to a secured offsite location **[immediately]** upon document changes or upon document scanning.

Cloud Computing

[For agencies that store electronic records using cloud-based technology: describe your agency's cloud-based practices. How is the technology used: as a storage site that mirrors locally hosted data, as the sole storage entity for data, or as a collaboration tool used during the drafting process? What backup measures are in place? Should the vendor fail or should the agency otherwise discontinue service with the vendor, is the agency able to recover its electronic records, and in what form is that data available? For more guidance, please see the DNCR guidance document *Best Practices for Cloud Computing Records Management Considerations*.[12]]

Vendor-Provided Services/Hosted Solutions

[For agencies that contract out electronic records management services, including digital imaging]

The terms of the service level agreement with **[third-party contractor]** detail:

- File formats
- Plan for converting files to a new format
- File naming practices

---

[9] http://archives.ncdcr.gov/Portals/26/PDF/guidelines/SharedStorageGuidelines.pdf

[10] http://archives.ncdcr.gov/Portals/26/PDF/guidelines/DatabaseIndexingGuidelines.pdf

[11] http://archives.ncdcr.gov/Portals/26/PDF/guidelines/BackupsProceds.pdf

[12] http://archives.ncdcr.gov/Portals/26/PDF/guidelines/cloud_computing.pdf

- 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. Compliance and Electronic Records Self-Warranty

The completion of this form by all signing employees signals that all employees 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 agency are created, reproduced, and otherwise managed in accordance with guidelines for electronic public records published by the North Carolina Department of Natural and Cultural Resources. **[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. Destructions of records are authorized when your agency approves the current retention and disposition schedule(s). If scanned records are intended to take the place of original paper records, state agencies must amend the disposition instructions of the relevant items in their program records schedule to reflect this procedure, and local agencies must submit the *Request for Disposal of Original Records Duplicated by Electronic Means* form.]**

Each signatory should initial each element for certification, print his/her name on the Approved by line, fill in the job title, and sign and date the form.

Records Custodian/Managerial Staff

The records custodian is the person responsible for creating records or managing the staff who create records.[13] 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 DNCR guidance regarding file formats, file naming, and if applicable, digital preservation guidance produced by DNCR.
- Detailed, documented procedures are in place and followed when the records are created, copied, modified, or duplicated.
- The person who creates, copies, modifies, or duplicates 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.
- Employees sign training records after receiving training.

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

_____ **[Local Government Agencies]** This agency will submit to the Department of Natural and Cultural Resources Section 10 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.

_____ **[State Government Agencies]** This agency will contact the Government Records Section to amend the agency schedule to reflect current recordkeeping practices and will comply with the best practices and standards established by the Department of Natural and Cultural Resources.

_____ Affected records creators will be trained on the proper creation and maintenance of electronic records.

_____ Imaged records will be periodically audited for accuracy, readability, and reproduction capabilities before the original documents are destroyed.

Approved by: _____ Date: _____

Title: _____

Signature: _____

[13] G.S. § 132-2 specifies, "The public official in charge of an office having public records shall be the custodian thereof." G.S. § 160A-171 specifies that the city clerk is the custodian of all city records. Therefore, the individual signing this section will likely be the clerk at the local level or the head of the organizational unit.

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 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 followed are in accordance with the agency's documentation.
- are performed routinely on files 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 sources 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 Natural and Cultural Resources.

_____ Backup procedures are in place and comply with best practices as established by the Department of Natural and Cultural Resources.

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

Approved by: _____ Date: _____

Title: _____

Signature: _____

Chief Records Officer

The Chief Records Officer (CRO) coordinates records management training and compliance. The CRO certifies:

_____ Oversight of the design and implementation of agency electronic records initiatives.

Approved by: _____ Date: _____

Title: _____

Signature: _____

Agency Supervisor/Division Director

The agency supervisor or division director is the person responsible for approving internal policies and procedures related to the creation and maintenance of electronic records. The agency supervisor/division director certifies that:

_____ **[For state agencies]** A Chief Records Officer is appointed.

_____ Determinations are made regarding employees' permission rights to the electronic records system.

_____ IT's configurations for the electronic records system are reviewed and approved before the electronic records system becomes operational.

Approved by: _____ Date: _____

Title: _____

Signature: _____

FOR DEPARTMENT OF NATURAL AND CULTURAL RESOURCES USE

Approved by: _____ Date: _____

Title: _____

Signature: _____

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

[For use by local agencies – state agencies should delete this section]

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.[14]

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

Request for Disposal of Original Records Duplicated by Electronic Means

If you have questions, call (919) 807-7350 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