# REQUEST FOR BOARD ACTION

## HENDERSON COUNTY
## BOARD OF
## COMMISSIONERS

**MEETING DATE:** August 5, 2019

**SUBJECT:** Request for Disposal of Original Records Duplicated by Electronic Means

**PRESENTER:** Darlene Burgess, Tax Administrator

**ATTACHMENTS:** Yes

1. Public Disposal Requests and Destruction Logs

**SUMMARY OF REQUEST:**

Staff is requesting approval from the Board of Commissioners to destroy original records listed on the attached Request for Disposal of Original Records Duplicated by Electronic Means included in accordance with the County's Public Digital Records Retention Policy and the provisions of the North Carolina Department of Natural and Cultural Resources Records Retention and Disposition Schedule. Electronic and digital images of scanned records will be considered the "official record".

**BOARD ACTION REQUESTED:**

The Board is requested to approve this request of disposal of original records duplicated by electronic means as presented, pursuant to the requirements of the County's current Public Digital Records Retention Policy.

**Suggested Motion:**

*I move the Board approve the Request for Disposal of Original Records Duplicated by Electronic Means as presented.*

## HENDERSON COUNTY
## RECORDS RETENTION AND DISPOSITION PROCEDURE

## PUBLIC RECORDS DISPOSAL REQUEST AND DESTRUCTION LOG

(Revised March 13, 2002)

**DEPARTMENT:** Tax

| RECORD TITLE & DESCRIPTON, INCLUSIVE DATES, & QUANTITY | RECORDS WILL BE | | RECORDS RETENTION SECTION | IF APPROVED, DATE DESTROYED |
|---|---|---|---|---|
| | DESTROYED | *DUPLICATED | | |
| | | | | |
| | | | | |
| Please | see | attached | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

***If duplication is required, indicate method.**

Approval is requested for the records listed above to be destroyed in accordance with the provisions of G.S. 121 and 132. The period for retention of these records, as prescribed by the North Carolina Department of Cultural Resources, has expired; **OR** where the period for retention has not expired, the original records have been duplicated on microfilm, microfiche, data processing or word processing equipment, with the understanding that said duplication shall be maintained for the specified period of retention. **NONE** of the original records listed above have been scheduled for permanent preservation by the North Carolina Department of Cultural Resources.

Darlene B. B
Department Head

7/31/19
Date

Submitted to the Henderson County Board of Commissioners. The Board:

APPROVED □
DISAPPROVED □

the destruction/duplication of the above records and such approval/disapproval has been entered into the official minutes of the Board of Commissioners meeting held on the _ day of ______________________, _____.

_______________________________
Clerk to the Board

STATE ARCHIVES
of NORTH CAROLINA

Rev. 2018

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: Jennifer Miranda** | **Date (MM-DD-YYYY):**<br>**7/3/19** |
| **Phone (area code): 828-698-3002** | **Email: jmiranda@hendersoncountync.gov** |
| **County/Municipality: Henderson County** | **Office: Henderson County Tax Office** |
| **Mailing address: 200 N Grove St Suite 102 Hendersonville, NC 28792** | |

| **Records Series Title**<br>A group of records as listed in records retention schedule | **Description of Records**<br>Specific records as referred to in-office | **Inclusive Dates**<br>(1987-1989; 2005-present) | **Approx. Volume of Records**<br>(e.g. "1 file cabinet," "5 boxes") | **Retention Period**<br>As listed in records retention schedule |
|---|---|---|---|---|
| | | | | |
| **Tax Abstracts and Lists** | Business Personal Property Listings | 2012 to present | 53 boxes | 10 years |
| | | | | |
| **Tax Abstracts and Lists** | Individual Personal Property Listings | 2013 to present | 7 boxes | 10 years |
| | | | | |
| **Tax Abstracts and Lists** | Manufactured Home Property Listings | 2013 to present | 3 boxes | 10 years |
| | | | | |
| | | | | |

Requested by: Darlene B. B Tax Administrator 7/8/2019
Signature Title Date

Approved by:
Signature Requestor's Supervisor Date

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

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 2
Responsible Parties and Their Responsibilities 2
Availability of System and Records for Outside Inspection 4
Maintenance of Trustworthy Electronic Records 4
Components of Information Technology System 6
Documentation of Information Technology System 6
Digital Imaging Program Documentation and Procedures 7
Request for Disposal of Original Records Duplicated by Electronic Means 9
Other Electronic Records Management Practices 9
Compliance and Electronic Records Self-Warranty 11

## 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: September 21, 2016

Title: Chairman Henderson County Board of Commissioners

Thomas H. Thompson

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: 09-21-16

Title: IT Director

Department Head