I. PURPOSE

The procedure reflects the guidelines established by the North Carolina Department of Cultural Resources publication *Guidelines for Managing Trustworthy Digital Public Records*. Complying with this procedure increase the reliability and accuracy of records stored in digitally and will ensure these records remain accessible over time.

College employees will retain and destroy electronic records only in conformity with State law, College policy, this Procedure, and approved Record Retention and Disposition Schedule ("the Schedule") for community colleges adopted by the North Carolina Department of Cultural Resources and the North Carolina State Board of Community Colleges.

II. MAINTENANCE OF TRUSTWORTHY ELECTRONIC RECORDS

When creating electronic records or converting paper records to an electronic record, the electronic record shall be:

1) Produced by methods that ensure accuracy;

2) Maintained in a secure environment;

3) Associated and linked with appropriate metadata; and

4) Stored on media that are regularly assessed and refreshed.

A. Produced by Methods that Ensure Accuracy

All platforms used by the College to create and manage electronic records, including e-mail clients, social media platforms, and cloud computing platforms, will conform with all College policies.

Electronic files are named in accordance with the *Best Practices for File Naming* published by the North Carolina Department of Natural and Cultural Resources ("DNCR").

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

B. Maintained in a Secure Environment

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

1) Access rights are managed by the IT department and are assigned by a supervising authority to prevent unauthorized viewing of documents.

2) 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.

3) Folders with confidential information are restricted, and access rights to confidential data are carefully managed. Confidential material is redacted before it is shared or otherwise made available.

4) Physical access to computers, disks, and external hard drives is restricted.

5) All system password and operating procedure manuals are kept in secure off-site storage.

C. 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.

D. 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:

1) Data is audited and assessed annually. If there is evidence of file corruption, data should be migrated to new media.

2) Records are periodically verified through hash algorithms. This is required before and after transfer to new media to ensure the records were not altered.

3) Media is refreshed every three to five years. The College 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.

4) Records are periodically migrated to new file types, particularly when a new information technology system requires that they be brought forward to render the file properly.

5) Metadata is maintained during transfers and migrations.

6) 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 College adheres to the media

manufacturer's recommendations for specific environmental conditions in which the media should be stored.

7) Whatever media is used to store data is clearly labeled with enough information that its contents can be determined.

III. COMPONENTS OF INFORMATION TECHNOLOGY SYSTEM

A. Training Programs

The IT department will conduct training for system use and electronic records management. 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 training offered by the North Carolina 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.

B. Audit Trails

At a minimum, the IT department will maintain documentation on who has read and/or written permission to files maintained by the College. 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.

C. 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 College IT staff, at least annually.

D. Documentation

The College 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 upon implementation of a new information technology system. Such documentation maintained by the institution includes:

1) Procedural manuals

2) System documentation

3) Security backup and disaster recovery procedures as a part of the Continuity of Operations Plan

4) Service level agreements for contracted information technology services

IV. OTHER ELECTRONIC RECORDS MANAGEMENT PRACTICES

A. Security and Disaster Backup and Restoration

The College 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 and are stored in secure off-site storage.

B. Cloud Computing

The college will primarily use a public cloud deployment model for non-sensitive data and applications. We will use a private cloud deployment model for sensitive data and applications that require higher levels of security and control. We may also use a hybrid cloud model when appropriate.

The college will only use cloud providers that have appropriate security controls and certifications, such as ISO 27001, SOC 2, and PCI DSS. We will ensure that all data stored or transmitted in the cloud is encrypted at rest and in transit. Access to cloud resources will be controlled using identity and access management (IAM) tools, and only authorized personnel will have access to the data.

The college will ensure that all cloud providers we use comply with relevant regulations and standards, such as GDPR and FERPA. We will also ensure that all data stored in the cloud is subject to appropriate privacy and security controls, and that our organization's policies and procedures are followed.

The college will establish SLAs with cloud providers that cover uptime, availability, and performance. We will ensure that the SLAs align with our organization's business needs and risk tolerance. We will also monitor cloud providers' performance against the SLAs and take appropriate action if necessary.

The college will establish a disaster recovery plan for all critical data and applications stored in the cloud. The plan will include backup and recovery procedures, as well as procedures for testing and verifying the plan's effectiveness. We will also ensure that cloud providers have their own disaster recovery plans that align with our organization's requirements.

V. CONVERTING RECORDS TO DIGITAL FORMAT

When converting non-permanent paper records, that have not met their retention period, to digital records, the appropriate College employees will complete the Compliance and Electronic Records Self-Warranty Form for each group of converted records. After digital conversion, the records custodian may request to dispose of the paper records from their supervisor. The following administrators may authorize the disposition of the paper records after digital conversion: [insert

titles, i.e. Department Heads, or Deans, or Vice President, etc.] The Authorization to Dispose of Paper Records form should be used.

Adopted: August 26, 2022

COMPLIANCE AND ELECTRONIC RECORDS SELF-WARRANTY FORM

The completion of this form by all signing employees signals that all employees will adhere to the rules set forth in College policy and procedure. Furthermore, this section is to be used as a self-evaluation tool to ensure that electronic records produced by the College 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.

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.

IT Professional
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. 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 College'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: _____

College Records Custodian
The College Records Custodian coordinates records management training and compliance. The College Records Custodian certifies:

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

_____ 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.

_____ Participation in the design and implementation of campus electronic records initiatives.

Approved by: _____ Date: _____

Title: _____

Signature: _____

AUTHORIZATION TO DISPOSE OF PAPER RECORDS

This form is used to request approval from the College Records Custodian 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.

Before a college office may dispose of any paper record that has not met its required retention period and keep only a digital surrogate of that record, **all** the following conditions must be met:

□ The office agrees to abide by all guidelines and best practices as published by the Department of Natural and Cultural Resources, including File Format Guidelines and Best Practices for File-Naming.

□ An electronic records policy has been approved by the office and authorized by the Department of Natural and Cultural Resources.

□ All records series that will be scanned and their paper records destroyed after quality audits are listed in the table below:

Records Series Title	**Inclusive Dates** (e.g., 1987-1989; 2005-present)	**Required Retention Period**

□ Quality control audits have been performed on the electronic records.

□ The digital surrogates will be retained for the entirety of the required retention period.

Requested by: _____
Signature Title Date

Approved by: _____
Signature Department/Office Head Date

Concurred by: _____
Signature College Records Custodian Date