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 increases the reliability and accuracy of records stored digitally.

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:

- Produced by methods that ensure accuracy;
- Maintained in a secure environment;
- Associated and linked with appropriate metadata; and
- 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.

Employees are encouraged to name files in a way that allows for effective organization, recognition, storage, and utilization of the file and its contents. For guidance, employees may look to the Best Practices for File Naming published by the North Carolina Department of Natural and Cultural Resources ("DNCR").

Electronic files should be saved in formats that comply with DNCR's File Format Guidelines for Management and Long-Term Retention of Electronic Records. These file formats 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:

- Access rights are managed by the IT department and are assigned by a supervising authority to prevent unauthorized viewing of documents.
- Either the information technology system is able to separate confidential from non-confidential information, or data creators must organize and name file systems in such a way to identify confidentiality of the documents.
- Folders with confidential information are restricted, and access rights to confidential data are carefully managed. Confidential material is redacted by the data owner 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.

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. Storage Media is Regularly Assessed and Refreshed as Needed

The following steps are taken to help ensure the continued accessibility of records kept in electronic formats:

- Storage media is audited and assessed at least annually. If there is evidence of hardware failure, data should be migrated to new media.

- Metadata is maintained during transfers and migrations where applicable.

- On-premise storage media is maintained in an environment that adheres to the media manufacturer's recommendations.

- Storage media is clearly labeled with enough information that its contents can be determined.

- Once the new media and file transfer has been verified, the original media may be destroyed according to the guidelines of 07 NCAC 04M .0510.

III. COMPONENTS OF INFORMATION TECHNOLOGY SYSTEM

A. Audit Trails

At a minimum, the IT department will maintain documentation on who has read and/or write 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.

B. Audits

Internal user access audits are initiated at least annually by College IT staff.

C. Documentation

Each department will maintain documentation which outlines their system processes, workflows, and business continuity plan. The IT department will maintain service level agreements, the risk assessment plan, system documentation, and infrastructure documentation.

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 cloud-based storage.

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. Department Heads or Vice Presidents may authorize the disposition of the paper records after digital conversion. The Department of Cultural Resources' Authorization to Dispose of Paper Records form should be used.

Adopted:	August 2, 2023
Revised:	N/A
Legal Reference:	Best Practices for File Naming, Record Retention and Disposition Schedule, File Format Guidelines for Management and Long-Term Retention of Electronic Records, 07 NCAC 04M .0510
Cross-Reference:	Policy 7.1.2 – Internet and Network Acceptable Use (Referenced By)