

Guidelines for the Transfer of Digital Files to the State Archives of North Carolina

August 2021
Version 3.2



NC DEPARTMENT OF
NATURAL AND CULTURAL RESOURCES

Contents

Purpose	2
Brief Overview of Electronic Storage	2
General Guidelines for File Management and Transfer	3
<u>1.</u> Preferred File Formats for Transfer	3
<u>2.</u> Frequency of File Transfer	3
<u>3.</u> Regulations for Digital File Transfer	3
Steps for Transferring Electronic Records to the State Archives.....	3
<u>4.</u> Creating a “For Archives” Folder	3
<u>5.</u> Organizing Records for Transfer	4
<u>6.</u> Requesting Electronic Records Transfer	6
<u>7.</u> Using Bagger for Electronic Records Transfer.....	6
<u>8.</u> Deleting Files.....	7
Appendix: Checklist for Preparing Electronic Records for Transfer	8
<u>9.</u> Best practices for file names.....	8
<u>10.</u> Best practices for file paths.....	8
<u>11.</u> Digital preservation issues	8

Purpose

The State Archives of North Carolina houses records, papers, photographs, and other materials of enduring value that document citizen rights, government actions and interactions with the citizenry, and reflect change over time. As society shifts from a paper-based to a digital world, the State Archives of North Carolina will continue to be the custodian of permanent archival records and materials, regardless of physical form or characteristics.¹ General Statute §121 designates the Department of Natural and Cultural Resources as the “archival and historical agency of the State of North Carolina” and further defines the powers and duties of the agency.² In this role, the State Archives receives records and materials of enduring value from state agencies, local government, and private individuals and entities. In the world of electronic records, it is imperative to ensure that these records and collections transfer via a method that maintains the authenticity of the original files.

This guide will assist with the transfer of electronic records identified for permanent retention to the custody of the State Archives, as prescribed on the approved retention schedule.³ It provides an overview of best practices for preparing electronic records for transfer, including the most appropriate file names and formats. This document also provides instructions about the tools used for file transfer and the steps that should be taken to ensure a smooth transfer process.

Brief Overview of Electronic Storage

Electronic files, by nature, are fragile and subject to alteration, either through human action or through corruption of data known as “bit rot.” They require constant care to ensure that the data they contain is preserved. A good digital preservation program protects records against data decay, obsolescence from ever-changing technologies, hardware failure, and natural or human disaster.

The North Carolina Digital Repository, jointly managed by the State Archives and the State Library, provides digital preservation and long-term storage for electronic records and publications with enduring historical value. The records kept in the Digital Repository are state and local government records scheduled for permanent retention in the custody of the State Archives, as well as permanent state agency publications managed by the State Library. **The State Archives does not provide temporary security storage for electronic records.**

Each agency must adhere to the records retention and disposition schedule and to the recommendations of the assigned records analyst. Records that have permanent value should have a disposition instruction to transfer them to the custody of the State Archives. To contact your records analyst, please see the Directory of Records Management Analysts.⁴

¹ North Carolina General Assembly, “General Statutes, G. S. 132.”
<http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=132>, accessed April 19, 2018.

² North Carolina General Assembly, “General Statutes, G. S. 121.”
<http://www.ncleg.net/gascripts/statutes/statutelookup.pl?statute=121>, accessed April 19, 2018.

³ For the Functional Schedule for North Carolina State Agencies, see <https://archives.ncdcr.gov/government/retention-schedules/state-agency-schedules/functional-schedule-north-carolina-state>. For local government schedules, see <https://archives.ncdcr.gov/government/retention-schedules/local-government-schedules>.

⁴ For state agencies, see <https://archives.ncdcr.gov/government/retention-schedules/state-agency-schedules/records-analysts-state-agencies>. For local agencies, see <https://archives.ncdcr.gov/government/records-management-services-and-training/local-records-services-and-training>.

General Guidelines for File Management and Transfer

Preferred File Formats for Transfer

The State Archives of North Carolina (SANC) has guidelines on preferred file formats recommended for records transfer, which were selected because they are sustainable for future use, are widely supported for access and functionality, and can support a variety of uses and needs.⁵ These formats are considered the best suited for preserving data through future technological changes. If you have file formats that are not listed or cannot be converted to the preferred file format, please contact your records management analyst prior to transfer.

Frequency of File Transfer

A regular schedule for transfers of digital records is important to ensure that the data they contain remains accessible. Preservation actions performed by SANC ensure that files are authentic and remain accessible well into the future. It is recommended that agencies should consult their records retention schedule and their records analyst to determine frequency of transfer.

Regulations for Digital File Transfer

The North Carolina Administrative Code Title 7, Chapter 4, Subchapter M, Section .0503 includes the following information on transferring electronic records:⁶

1. The custodian will create a checksum for each file transferred using a DNCR-approved hash algorithm and include this information with the transfer (accomplished by using Bagger tool).
2. The custodian of the electronic records must check them for computer viruses.
3. The file's metadata should also be included in the transfer.⁷

See also the checklist for preparing electronic records for transfer at the end of this document.

Steps for Transferring Electronic Records to the State Archives

Creating a “For Archives” Folder

It is not necessary to transfer all your digital files or every draft of a single file. Instead, records custodians should create a “For Archives” folder on a shared drive and move the final copy of the records scheduled for transfer to the “For Archives” folder. The State Archives will not take drafts or additional copies of records. The SANC recommends that this “For Archives” folder be organized into sub-folders with the Item Number from the Records Retention and Disposition

⁵ <https://archives.ncdcr.gov/documents/file-formats-transfer-electronic-records-state-archives-north-carolina>;
http://www.digitalpreservation.gov/formats/intro/format_eval_rel.shtml#factors

⁶ <http://reports.oah.state.nc.us/ncac/title%2007%20-%20natural%20and%20cultural%20resources/chapter%2004%20-%20archives%20and%20history/subchapter%20m/07%20ncac%2004m%20.0503.pdf>, accessed April 19, 2018.

⁷ Metadata includes complete and intact e-mail header information, sidecar metadata (any other files containing information about the file), spreadsheets or databases used to track a project or file, and any information created by geolocation data or an image editing program. For more information on metadata see: <https://archives.ncdcr.gov/documents/metadata-public-record-north-carolina-best-practices-guidelines-its-retention-and>

Schedule serving as the folder name. If you are having difficulty locating the Item Number, you can contact your chief records officer or records management analyst for assistance.⁸

Organizing Records for Transfer

When copying your records into the “For Archives” folder, the sub-folders structure should be organized by the Item Number on your retention schedule. The next level should match your agency’s filing system. Please note that while the Windows 10 operating system supports file paths longer than 255 characters, older versions of Windows do not and **it is strongly recommended to keep path length within this limit**, or they will likely become inaccessible. The file path begins with the drive name, includes any folders and ends with the filename (for example, C:\Example\path.txt). As you organize your records for transfer, please check that long file names and deeply nested folders do not result in a path over the limit, as they will not be able to transfer to the Archives. Please consult with your IT department if you have difficulty with long file paths or other technical issues. If you have any questions about organizing your file structure, please contact your records analyst.

Accessibility

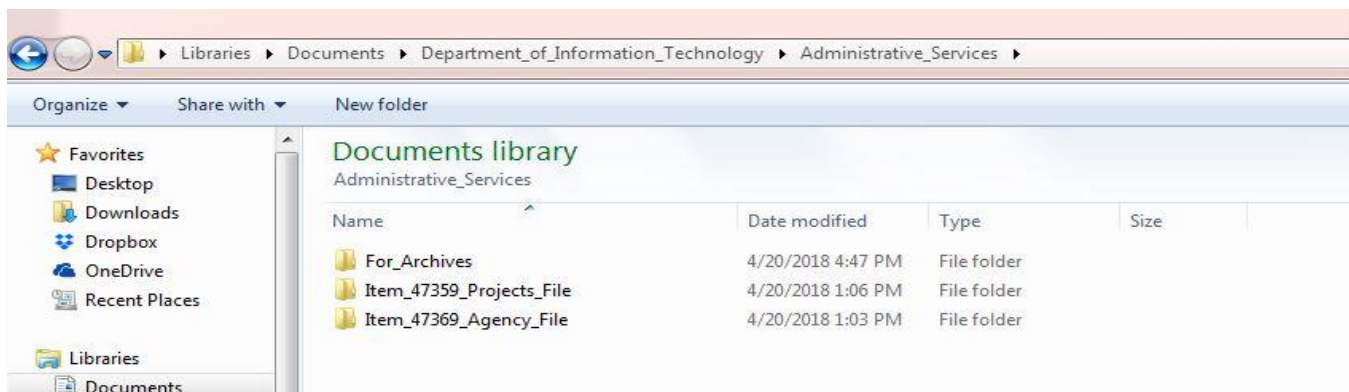
Records should not be password-protected, encrypted, or have other digital rights management that prevents the document from being opened. If the encryption key or password are lost the files will remain inaccessible to future users and cannot serve their documentary purpose or be properly preserved. Agencies should confirm that records are accessible (i.e., able to be opened) prior to transfer.

Confidentiality

If confidential or restricted data exists in the transfer, the agency should inform the records analyst and specify the data, as well as indicating its presence on the transfer form. One option is to nest a folder labeled “confidential” or “restricted” within each item number. Alternatively, you can include a readme.txt file or MS Word file that contains a description of the confidential or restricted records. If transferring the contents of a database with confidential or restricted information, the transfer should include the database index including a listing and description of the confidential fields. The bag name should contain the word CONFIDENTIAL or RESTRICTED, for example 20180509_Item_47359_CONFIDENTIAL. See below for more information on using the Bagger tool to package files for transfer.

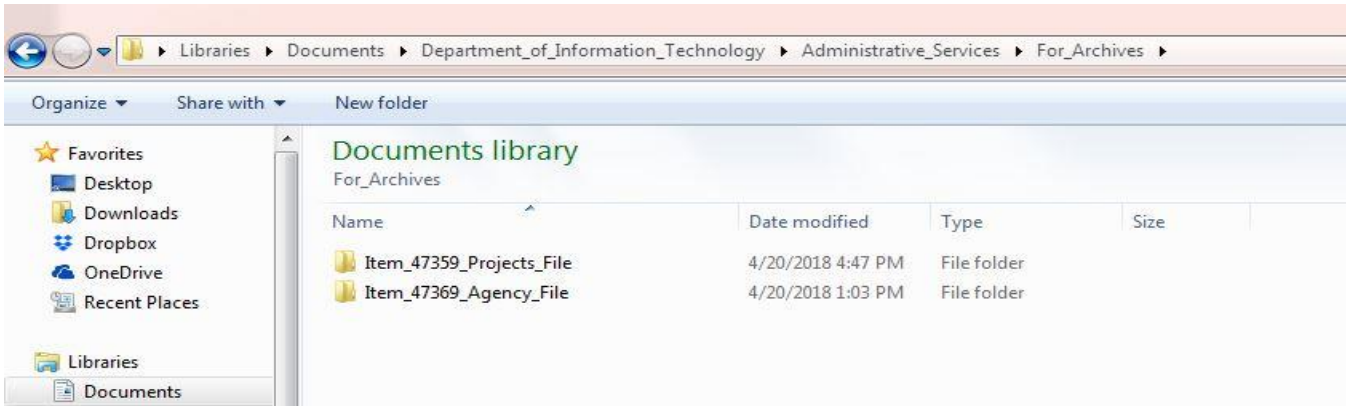
File Organization Examples:

This is an example of the suggested filing structure. The “For Archives” folder should be located with the rest of the files for your agency/division.

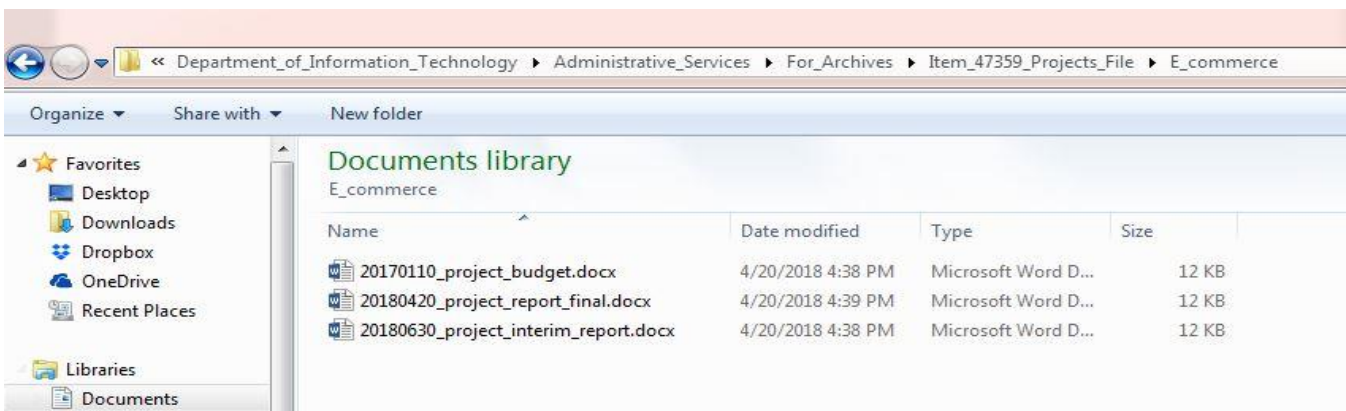
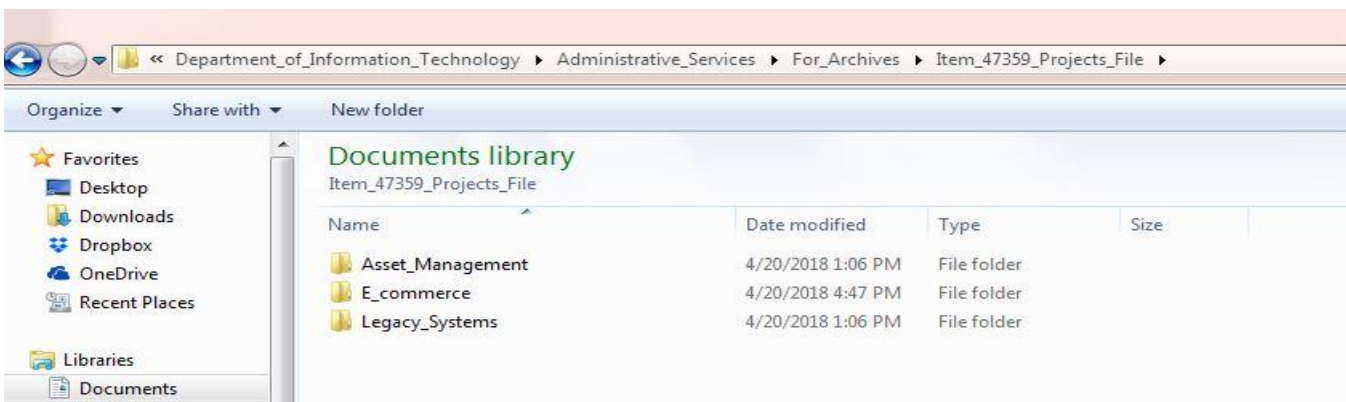


⁸ <https://archives.ncdcr.gov/government/records-management-services-and-training/chief-records-officers>

Within the “For Archives” folder, files should be organized according to the Item Number on your retention schedule. The retention schedule will tell you which types of files should be placed in each folder.



Within each item number folder, files should be structured the same way your agency organizes files in active use.



Electronic files need to be named accurately and consistently so that they are identifiable and accessible. This practice is necessary for administrative use, public access, and maintaining confidentiality. A good file name should include

consistently formatted dates, all necessary descriptive information, and the version of the file. It should also be concise, bearing in mind the 255 character limit for file paths. See our instructions on good-file naming practices.⁹

Requesting Electronic Records Transfer

Please contact your agency's records analyst before beginning the transfer process and complete the State Agency Electronic Records Transfer Form RC-2D or State Agency Email Transfer Form RC-2D-E.¹⁰ **Remember to note any confidentiality, file format, accessibility, or other preservation concerns on the form.**

Using Bagger for Electronic Records Transfer

The State Archives takes responsibility for the devices and tools used to transfer and authenticate the electronic files and is committed to working with state and local government offices and private donors during the transfer process. In this way, the State Archives can certify the records and files in its repository as true, unchanged, and authentic. Per the Administrative Code 07 NCAC 04M.0503, SANC uses a data transfer and authentication tool to transfer records. Currently SANC uses Bagger, a tool developed by the Library of Congress to verify the integrity and authenticity of electronic records prior to and after they have been transferred. The Bagger tool performs the following functions:

- Packages files into a single directory
- Creates a manifest of checksums (unique identifiers) for each file
- Creates a subdirectory that contains the actual files and data
- Packages the file structure of an entire directory (called a "bag")

By using Bagger, SANC can validate the records' integrity, confirm that the files are unchanged bit-for-bit by the transfer, and by capturing the file structure allow SANC to identify and store the files following the transfer. The records can also be validated for auditing purposes or after future transfers by invoking the tool each time the files are moved.

The "data" folder along with the four text files serve as the complete "bag:" two "manifest" files and two "info" files. Once the information transfers, the State Archives will re-run the Bagger program to ensure that the files validate and none of them changed in the transfer process. This way, the archives can prove that it has received the files as they were, bit for bit, on the file system from which they were transferred.

The Bagger software is open-source, well documented, and easy to use. Bagger is built on top of an earlier, command-line tool, BagIt, created for the same purpose. The data sender or depositor creating bags may use either BagIt or Bagger to perform the actions described above. Senders/depositories may choose to use BagIt instead of Bagger in certain types of workflows, such as automation or batch processing. SANC can provide you with flash drives with Bagger already configured, or you may choose to download and configure Bagger on your machine prior to transfer. **For step-by-step instructions about installing and using Bagger, please see our Bagger user guide.**¹¹

If agencies have packaged files using the Bagger tool themselves, they should place the bagged files on a portable hard drive or flash drive to be delivered to the State Archives. Please contact your records analyst if you have any questions about how to transfer files.

⁹ <https://archives.ncdcr.gov/documents/best-practices-file-naming>

¹⁰ <https://archives.ncdcr.gov/documents/electronic-records-transfer-rc-2d>

¹¹ <https://archives.ncdcr.gov/documents/bagger-gui-user-guide>

Bagger must be used prior to file transfer so that the files may be validated after they have been transferred, as required by 07 NCAC 04M.0503. If the files are not bagged before transfer, SANC cannot provide any proof as to their integrity and authenticity. Using Bagger ensures that the records are transferred completely and accurately. If SANC staff finds that the files are corrupted during the transfer, SANC will contact the transferring agency to repeat the process.

For Special Collections acquisitions, it is not always feasible to have files bagged on arrival. In such a case, the State Archives reserves the right to use the Bagger tool once in possession of the files. This will begin the authenticity chain once files transfer into the digital repository.

Deleting Files

Once State Archives staff has validated the transfer of files, you will be contacted and instructed to delete your copy of the “For Archives” folder. The Administrative Code 07 NCAC 4M. 0510 defines electronic records destruction as overwriting, unlinking and deletion of data and metadata so that they cannot be reconstructed.¹² For more information about records destruction, please contact the State Archives.

The agency should also retain documentation of the transfer in office permanently as a part of its Records Management File.

¹² <http://reports.oah.state.nc.us/ncac/title%2007%20-%20natural%20and%20cultural%20resources/chapter%2004%20-%20archives%20and%20history/subchapter%20m/07%20ncac%2004m%20.0510.pdf>

Appendix: Checklist for Preparing Electronic Records for Transfer

When preparing related files for transfer to the State Archives of North Carolina, it is important for files to comply with best practices so that they can be preserved and accessed into the future. The checklist below provides an overview of steps to take to ensure the files sent to the State Archives can be accessed by the appropriate persons in perpetuity. If you have any questions, consult the State Archives website or contact the archivist/records analyst with whom you are working.

Best practices for file names

- Avoid using special characters such as \ / : * ? " < > | [] & \$,
- Use underscores instead of periods or spaces
- Err on the side of brevity
- Include all necessary descriptive information independent of where file is stored
- Be consistent with file names

More details can be found in the State Archives' file naming best practices document at

<https://archives.ncdcr.gov/documents/best-practices-file-naming>

Best practices for file paths

- The file path (or folder structure) in which files are stored should also follow the file naming steps above.
- Additionally, files should not be deeply nested. The full file path – or the letter drive, folder names, and file name combined, e.g. C:\Users\my_name\Documents\my_file.pdf – must not be longer than 255 characters. Some operating systems are unable to store or open files with longer paths.

Digital preservation issues

- Avoid compression of files, as this may cause data loss. Files sent to the State Archives should be uncompressed.
- Avoid encryption or password protection of files. If the password or key is lost, the files will be inaccessible.
- Documents containing digital signatures should have open time stamp authorities that can be verified – should not prevent opening the document.