# Indiana Archives and Records Administration Electronic Records Guidelines

Version 3.0

Indiana Archives and Records Administration
Records and Information Management Division
July 2023

# Contents

# About These Guidelines

The Indiana Archives and Records Administration Electronic Records Guidelines were developed to help State agencies and County/Local government offices determine how to:

- scan records in-house or in partnership with a vendor
- manage electronic records (born digital or scanned)
- organize and name files
- store electronic records for the long-term

**The field of Electronic Records Management is rapidly evolving, and these guidelines will be updated as new information is available.** The recommendations in this document are consistent with currently accepted best practices, and the update history can be found at the end of this document. If you have questions that are not addressed in one of the following sections, please reach out to the Electronic Records program at erecords@iara.in.gov.

This guide can be read in full or taken piecemeal as needed. It is written to work with Oversight Committee on Public Records Policies 20-01 and 20-02, which can be found at iara.in.gov. For further guidance and training on records management, please visit iara.in.gov.

# Introduction to Electronic Records Management

Electronic records are any records created, maintained, altered, or deleted in a digital format. These records are subject to the same record keeping requirements as are paper records. However, the complexities of media (the physical storage objects on which electronic records are stored) and format (the programs, versions, file types, and operating systems that are required to access the records) require agencies to think ahead and incorporate records retention requirements within record keeping systems at the point of design.

Electronic Records Management (ERM) addresses the creation, maintenance, use, and disposition of records over the course of their lifecycle. It provides best practices surrounding preservation and access, media and formats, trustworthiness, and storage. Electronic records require thorough planning to address their unique storage needs and to ensure they remain accessible for as long as they are needed.

## Trustworthy Records

The trustworthiness of electronic records depends on their:

- Integrity: the content is complete and unaltered. Any modifications are documented according to pre-established policies.
- Usability: the content can be located and viewed. Any relevant context should be maintained.
- Reliability: the content is a complete and accurate representation of agency activities.
- Authenticity: the content can be proven to have been created by the originating agency.

An excellent way to establish trustworthy records is to create thorough documentation of record keeping systems as they are implemented. Consulting with the Indiana Archives and Records Administration during the design phase of your system or electronic records program can help ensure that you are creating records that will be usable for the entirety of their legally required lifespan.

Agencies collecting information on citizens, particularly that of a personal nature, should be aware of the Fair Information Practices Act (FIPA), IC 4-1-6-1, as it defines statutory requirements for documentation. Because of FIPA, the importance of documenting procedures for systems that transmit or store personal information cannot be overemphasized.

## Media and Formats

Records are created, maintained, and preserved in many formats and on many different types of media. Paper and film are two of the most traditional mediums, but USB keys, hard drives, CDs, and Blu-rays are also popular. MP4s, video, audio recordings, negatives, PDF, chat, social media, databases, and dashboards are all also ways of creating, maintaining, and preserving records. Retention best practices for some electronic records, like dashboards, are only just emerging. For others, like MP4s, best practices are well established.

## Recommended Scanning Specifications

Whether you are embarking on an in-house digitization project or working with a vendor, a vital first step is setting scanning specifications. Below are recommended specifications based on industry best practices. If you have questions about digitizing electronic records please contact erecords@iara.in.gov. If you are interested in the digitization services the State Imaging and Microfilm Laboratory offers please visit iara.in.gov or email imaging@iara.in.gov.

Scanning specifications for total retention periods of 14 years or less.

| Type | Bit Depth and color space | Resolution | File Format |
|---|---|---|---|
| **Textual documents** | 8-bit grayscale<br>24-bit color | 200 ppi | TIFF v6<br>PDF<br>PDF/A |
| **Photographic negatives** | 8-bit grayscale<br>24-bit color | 3000 ppi across long edge | TIFF |
| **Photographic prints** | 8-bit grayscale<br>24-bit color | 400-600 ppi | TIFF |
| **Oversize items** | 8-bit grayscale<br>24-bit color | 300-600 ppi | TIFF |
| **Microforms** | 8-bit grayscale<br>24-bit color | 300-400 ppi | TIFF |

Scanning specifications for total retention periods of 15 years or longer.

| Type | Bit Depth | Resolution | File Format |
|---|---|---|---|
| **Textual documents** | 8-bit grayscale<br>24-bit color | 300 ppi | TIFF<br>PDF<br>PDF/A |
| **Photographic negatives** | 8-bit grayscale<br>24-bit color | 4000 ppi across long edge | TIFF |
| **Photographic prints** | 8-bit grayscale<br>24-bit color | 400-800 ppi | TIFF |
| **Oversize items** | 8-bit grayscale<br>24-bit color | 300-600 ppi | TIFF |
| **Microforms** | 8-bit grayscale<br>24-bit color | 400 ppi | TIFF |

## Quality Control

According to OCPR 20-02, a *digitized record* is an electronic copy of a physical record and acts "as authentic duplicate", meaning digital images or data must be verified against original records for completeness and accuracy. Incorporating quality control requirements in your digitization process is crucial to ensuring the quality of digitized images. Quality control is the process of verifying that your digital records against your original paper records for completeness and accuracy.

Inspecting the digitized records requires that you compare the paper records to the digital record to confirm that the digitized record contains all the same information as the paper record. Document the procedures you use for performing quality control for your digitization projects to ensure consistency across all projects. The individual conducting quality control ideally should be a different person than the individual who scanned the records.

### *Sample Set*

You do not have to visually inspect every single scanned record. Inspect a sample set of records by either a random sampling of a minimum of 10 digital records **or** 10% or the images per scanning batch, whichever option requires less work for you.

### *Visual Inspection*

What quality control measures you should be reviewing in the visual inspection:

- Open files – Can you open and display the file?
- Resolution – Does the image looks pixelated or of a poorer resolution quality than the paper record?
- Color accuracy – Do the colors represented on the paper record match what can be seen in digitized record?
- Completeness – Does the digitized record have the same page count as the paper record?
- Image loss – Does the digitized record have any cropped, incomplete, or distorted pages compared to the paper record?

Other things to include are checking that the file naming conventions used for the project are correct, the file extension (e.g., .pdf or .tiff) match your scanning specifications, and that the digital files maintain any organization or hierarchy that was present in the paper records. Much like when digitizing records, be sure to use the appropriate computer equipment for performing quality control so that you can properly assess the digitized files.

A visual inspection requires a 100% success rate from sample set to pass as "an authentic duplicate". You cannot destroy the source records until you have verified the sample set has passed the visual inspection.

# Electronic Records Storage Location Best Practices

## Overview

There are a host of storage locations for electronic records, ranging from physical file servers to the Cloud to hard drives. Proper records retention and disposition must include full, accurate, and current documentation of the system (hardware and software that, when combined, act as the electronic repository for the records in question), functions supported by the system, how the information is collected, used, accessed, maintained on each of the systems mediums, and the procedural controls employed to preserve the integrity of the system's data.

Documentation files should do the following:

- identify system hardware and software;
- formalize file naming conventions;
- detail back up and security procedures;
- identify the sources and uses of information and their confidential or nonconfidential status;
- and outline quality control procedures and storage requirements.

Documentation should also cover employee training procedures and the verification of employee attendance at training sessions.

The following questions should be addressed when developing an electronic records program as system capabilities and characteristics can vary widely:

- How long are the records to be retained? If the system will contain multiple record series, how will you identify which records within the system belong to which record series?
- If some or all of the electronic records are scheduled to be transferred to the Indiana Archives, how will you identify those records, and can they be exported in a format which the Archives can accept?
- Will secondary information, such as reports, be created from the data, and how will these be maintained?
- Can old records be converted easily to new versions of software without loss of data?
- How will access to the records be maintained?
- Are the records confidential?
- How will the system be secured?
- What is the system back-up and / or disaster plan?
- Who will maintain documentation of the system?

To determine the most accurate, complete, and practical method of managing records, agencies need to develop procedures that fit their specific situations. Understanding the capabilities of a system is a prerequisite to determining how the records will be identified, organized, and stored.

## Collaborative Spaces

Applications such as SharePoint and Teams are considered collaborative spaces, as they allow multiple people to work in a single, shared location. If you are creating a collaborative space, it is a best practice to assign more than one Owner or Administrator to any collaborative space at the point of creation whenever possible. This acts as a backup plan if you are unable to continue managing the collaborative space.

Any files saved exclusively to the collaborative space and which pertain to the work of your agency are public records, and must be retained in accordance with retention schedules approved by the Oversight Committee on Public Records under IC 5-15-5.1-19(c). If a file is saved in the collaborative space and elsewhere, determine which version will serve as the agency's copy of record, which must be retained in accordance with Oversight Committee on Public Records approved retention schedules. The copy of record is the official copy used for reference and preserved in accordance with the

retention schedule. IARA strongly advises that collaborative spaces not be used to store the copy of record for any record with a total retention period longer than 3 years, or with a final disposition of transfer to the Indiana Archives.

If a collaborative space becomes inactive or is no longer needed, ensure content is retained in accordance with Oversight Committee on Public Records approved records retention schedules. This applies to all content created in and saved exclusively to the collaborative space. For example, a single Teams instance may contain multiple channels, multiple conversations within those channels, documents within the associated SharePoint site, images shared in a conversation or elsewhere, video recordings, or chat logs. It is an acceptable practice to copy or remove public records to a secure, backed-up location for the length of their required retention period, transferring permanent records to the Indiana Archives when they reach the end of their agency retention period. The Teams instance should then be maintained for the longest relevant retention period of any records that have not been transferred or copied elsewhere, or for a minimum of three years, whichever is longer.

## Server space, networked drives, and the Cloud

### *Save records to a secure, backed up, agency managed location*

Any files which pertain to the work of your agency are public records regardless of format, and must be retained in accordance with Oversight Committee on Public Records approved retention schedules. When it comes to saving records, look for a location that is secure, backed up, and over which your agency or office has some control.

It is a best practice to save records to a location which is backed up on a regular basis to a secondary geographic location. Never save records to your computer Desktop or an external device such as a USB key or thumb drive, as these locations are not backed up.

Save records to secure locations where you have reasonable assurance they cannot be altered or tampered with. For example, saving records to a location shared with users external to your agency is not a best practice. Whenever applicable, put safeguards on records that prevent others from editing or otherwise tampering with them.

Whenever possible, save records to a space your agency or office manages, maintains, or has some degree of control over. Refrain from saving records to temporary locations, or locations to which you may not have long-term access. If you must save records to a location to which you may not have long-term access, ensure you have a contingency plan for transferring the records to a more permanent location when necessary. Some examples of appropriate locations are a shared server space or an electronic recordkeeping system.

### *Limit your personal items*

- Follow the Information Resources Use Agreement (IRUA).
- To help limit personal items, save personal files to a specific folder. Then during your regular clean up make sure to empty this folder.

### *Stay organized*

- Follow any file or folder naming conventions your agency has created (see File Management for more information on naming conventions).
- Remove duplicates and unnecessary drafts.
- Perform regular clean-ups of any storage space you own or use.

# Electronic Mailboxes

Email messages that are composed, sent, or received in the course of your work are public records, and it is the responsibility of the agency or office to retain them in accordance with retention schedules approved by the Oversight Committee on Public Records.

### *Retention and Disposition*

"Email" is **not** a Record Series. Each email message's content must be mapped to a specific Record Series to determine how long it must be kept.

To determine how long you must retain your sent and received emails, you must first identify what Record Series the emails fall under. Email is a system for transmitting messages or information; the information *within* the email message and/or its attachment are considered the record, and *that* is what you must match up to a Record Series.

Email messages may fall under Record Series pertaining to, but not limited to:

- Correspondence
- Disaster or states of emergency notification and response
- Events, programs, products and services
- Routine day-to-day office management activities
- Personnel information

For additional information on how to identify the record series present in your mailbox please see Retaining Email Records – Quick Reference.

Email pertaining to ongoing or pending audits, lawsuits, litigation holds, or public disclosure proceedings cannot be deleted until the issue is resolved.

### *Nonrecords*

Email messages that do not meet the definition of public records are considered "nonrecords" and may be deleted when no longer useful. Examples of nonrecords include personal email, advertisements, spam, and mailing list messages from outside your agency/office, duplicate email directed at all-staff, and email that contains transitory information that is not related to your work.

### *Basics for Managing Email*

Given the volume of email sent and received, it is crucial to appropriately manage email on a regular basis following these best practices:

- **Limit personal use**. The easiest way to keep email manageable is to limit non-work use. Avoid using work email to communicate with family and friends and for any other personal communications. Avoid using your work email address to sign up for services, accounts or similar items that do not pertain to your work.
- **Use search and sort.**
    - Email client **search** functions can quickly identify emails that are nonrecords. This includes spam, vendor advertisements, newsletter subscriptions, listserv subscriptions, or emails that you know are not your responsibility to retain (such as general announcements from HR, IT helpdesk tickets, calendar invites, or similar).
    - Email client **sort** functions can quickly group similar emails, such as all messages with attachments or everything from a certain sender or time period.
- **Manage subscriptions.** Regularly check subscriptions to listservs, blogs, and similar services, and maintain only those that are work related. Use rules to send these emails to a specific folder for easier organization and eventual deletion.

- **Apply rules**. If you know someone always sends a certain kind of email, or that emails with a certain subject can all be managed in the same way, use the rule feature of your email client to send these items to a specific folder.
- **Manage email regularly.** This is crucial. Regularly managing your mailbox by following the tips above is the best way to keep the volume under control and maintain public records appropriately. Whether this occurs daily, monthly, or quarterly depends on work habits and volume of email.
- **Use clear, concise subjects**. For email sent by you and your office, avoid titling emails with generic, non-descriptive titles. This will help you group threads by project or by topic later, using the search, sort, and rules functions.

### *Shared Mailbox*

If you have primary responsibility for a shared mailbox, it is your responsibility to retain the contents in accordance with retention schedules approved by the Oversight Committee on Public Records. Some best practices are as follows:

- Assign primary responsibility for a shared mailbox to one person.
- If you are replying from your employee email account to a message that came to the shared mailbox, ensure you cc the shared mailbox on your replies. This ensures all records and context is preserved in the shared mailbox.
- Use tags and folders to organize content.

# Social Media Records Management Best Practices

Social media providers do not typically take responsibility for retaining content shared via their platforms. It is therefore crucial for agency social media content creators to understand what constitutes a public record on social media and how to properly retain it in accordance with retention schedules approved by the Oversight Committee on Public Records.

## Identifying public records on social media

Social media posts are considered public records when three conditions are met:

1. The content of the post falls under retention schedules approved by the Oversight Committee on Public Records.
2. The content of the post is unique (i.e., is not saved or stored elsewhere).
3. The content is posted via an official agency account OR is posted via any account with the purpose of distributing agency information to the public.

Social media posts may fall under record retention schedules pertaining but not limited to:

- Correspondence
- Disaster notification and response
- Events, programs, products and services
- Photographs and videos
- Press releases
- Surveys
- Training and education.

## IARA-recommended best practices

1. Familiarize yourself with the IN.gov Governance Council Social Media Guidelines.
2. Have a **content moderation plan**.
3. Be clear with agency staff and users when it comes to rules of engagement with your social media accounts.
4. Publicly post rules of conduct and document any infractions of those rules.
5. If you do remove posts, save them to a secure, backed-up, agency-managed location for future reference. You may need to produce the posts later to support your decision-making process.
6. Have a **content capture plan**. Know how you are capturing and saving posts that are considered records. There are four methods of capturing social media content:
    a. Create and manage any unique original content (i.e., content that does not exist elsewhere) in a location external to the social media platform (recommended).
    b. Collect content manually via screenshots of posts and associated comments. Save screenshots as JPEG files in a secure, backed-up, agency-managed location following any file naming conventions your agency uses.
    c. Download the data “archive” from the site. Please note that multi-media posts may need to be collected separately. This option is best if you believe most of your social media content constitutes a public record. (See below for instructions for manually downloading an archive.)
    d. Use a vendor to capture and manage social media content. If you decide to go this route, it is important that your agency fully understands how a vendor will retain content and how your agency will access content, and to have a plan in place in the event the vendor relationship is terminated.
7. Have a content **retention plan**. Know how long posts must be retained in accordance with retention schedules approved by the Oversight Committee on Public Records and have a plan for providing the Indiana Archives with a copy of any posts that qualify as permanent records.

8. Have an **exit plan**. Ensure any dormant or unused sites are retained in accordance with retention schedules approved by the Oversight Committee on Public Records and are not simply deleted when they are no longer needed or active. *In general, social media accounts should remain online for no less than three years after the date of the final post.* If you have questions about what content needs to be retained, please contact IARA.
9. Turn off any Direct Message/Private Message functions, and instead provide an official agency e-mail address on the profile page of the social media account. Alternatively, input an automatic response message redirecting private messages to an official agency email.
10. For private message conversations that have already occurred, download or take screenshots of all messages in each conversation and save them in a secure, backed-up, agency-managed location following any file naming conventions your agency uses.
11. All screenshots and subsequent emails should then be retained in accordance with retention schedules approved by the Oversight Committee on Public Records.
12. If a public comment is received that warrants a non-public response, reply publicly to that comment indicating that the individual should refer question(s) to an official e-mail account.
13. Ensure all staff who post on behalf of your agency are aware of and understand these best practices.

# File Management Best Practices

## Recommended File Formats

Indiana Code 5-14-3 requires that agencies make public records that are created electronically (born digital) available electronically. As a result, agencies may be required to migrate some legacy or proprietary formats and software before transferring electronic records to the Indiana Archives. In general, it is a best practice for agencies to ensure that electronic records may always be easily accessed, particularly in the event of a public records request. More information may be found in *Indiana's Public Records: The Legal Framework of Records and Information Management in State Government*. The recommendations in this section pertain to both born digital and digitized records.

Electronic records that must be retained for 15 years or longer OR transferred to the Indiana Archives should be saved in a file format that meets the following specifications:

- Non-proprietary and in common usage
- Uncompressed; if compression is unavoidable, format should be lossless
- Adherent to an open, documented standard
- Interoperable among diverse platforms and applications
- Fully published and available royalty-free
- Developed and maintained by an open standards organization where applicable

The following list of accepted formats was compiled after a survey of best practices from the National Archives and Records Administration, Society of American Archivists, Library of Congress, and the Council of State Archivists. The files on this list meet all or most of the above specifications. *Preferred* refers to file formats to which the above institutions give strong support. *Acceptable* refers to either file formats to which the above institutions give good support or IARA is willing to support based on current Indiana State government practices.

### Audio

| | |
|---|---|
| Preferred | WAV or WAVE, BWF, AIFF |
| Acceptable | MXD, FLAC |

### Containers

| | |
|---|---|
| Preferred | TAR, GZIP, ZIP |
| Acceptable | 7z |

### Computer Aided Design (CAD)

| | |
|---|---|
| Preferred | SVG, X3D |
| Acceptable | U3D, PRC |

### Databases

| | |
|---|---|
| Preferred | XML, CSV |
| Acceptable | TXT |

### Email

| | |
|---|---|
| Preferred | EML, MBOX, PST |
| Acceptable | XML, MSG, Native Format (with approval) |

### Geospatial

| | |
|---|---|
| Preferred | SHP, GeoTIFF |
| Acceptable | NetCDF, DBF |

### Image

| | |
|---|---|
| Preferred | TIFF |
| Acceptable | JPEG 2000, PNG, PDF |

### Social Media Archives

| | |
|---|---|
| Preferred | ZIP, HTML, RAR |
| Acceptable | JSON, WARC, ARC, Native Format |

### Statistics

| | |
|---|---|
| Preferred | ASCII, DTA, POR, SAS, SAV |
| Acceptable | CSV |

### Tabular data

| | |
|---|---|
| Preferred | CSV |
| Acceptable | TXT |

### Text

| | |
|---|---|
| Preferred | TXT, XML, PDF or PDF/A |
| Acceptable | RTF, HTML, ASCII, UTF-8 |

### Video

| | |
|---|---|
| Preferred | MOV, MPEG-4, MPEG-2 AVI |
| Acceptable | MXD, MKV |

### Web

| | |
|---|---|
| Preferred | WARC |
| Acceptable | ARC, native format |

## Naming Conventions

It is a best practice to name files and folders according to official and clearly communicated naming conventions that are uniformly applied across your agency, division, or office. Useful naming conventions are consistent, meaningful, and help people find information easily. When developing a standard, keep in mind these best practices:

| | |
|---|---|
| Vocabulary | Select a common vocabulary for file names so that everyone uses the same terminology. This includes abbreviations and acronyms. |
| Order | Confirm which element should go first, so that files on the same topic can be located more easily. |
| Punctuation | Decide on procedures for if/when to use capital letters, hyphens, symbols, or underscores. Avoid special characters and spaces. |
| Dates | Agree on a logical date format so that files display chronologically, e.g., YYYY-MM-DD or YYYYMMDD. |
| Version | Specify the number of digits that will be used in numbering so that files are listed in numerical order. |
| Documentation | Write down your agency's naming rules and make them available. |

The following recommended standards may be used as file naming guidelines. This list is not exhaustive, and not all conventions will apply in every situation.

- Consistency is key. Ensure that agency staff are trained to uniformly use any file naming conventions.
- If abbreviations or acronyms are used, keep a document explaining their full meanings.
- Keep file and folder names short but informative; consider the Windows 260-character file path limitation.
- Use descriptive keywords in the names that reference the content, series, and/or topic of the records.
- Use capital letters, dashes, or underscores rather than spaces to delimit words.
- Order the elements in file names in the most appropriate way to locate and retrieve records.
- Discourage redundancy in file names and directory paths.
- Restrict the use of non-alphanumeric characters whenever possible.
- Include a leading zero when entering numbers in a file name – unless the number is a year – to maintain numerical order.
- Input four-digit years, two digit months and two digit days if incorporating dates.
- Avoid using only personal names on directory folders.
- Place the family (last) name first, followed by the initial(s), if including people's names within file/folder titles.
- Verify that all words are spelled properly and dates are correct.

## File and Folder Structure and Organization

Files and folders should be organized in a structure that is in keeping with the needs of anyone with access, in accordance with any agency established conventions, and consistent across the agency. It is best to avoid too many folders within folders as this can make it difficult to quickly browse files and can prolong search times. Similarly, it is best to avoid placing all files in a single folder as this can also make browsing difficult and can also prevent the ability to provide different levels of access.

# Best Practices for Records Scheduled for Permanent Retention

Not every storage system will be reliable over the long-term and it is important to plan ahead for electronic records that are scheduled for permanent retention.

## Microfilming Electronic Records

For some permanent electronic records, it may be feasible and practical to create a microfilm copy. Under this model, the electronic records act as your Access Copy – primarily used when you need to quickly access information or when you need to make a duplicate Access Copy. The microfilm is kept as the Master Copy – only used in the event the electronic records are inaccessible and a duplicate Access Copy needs to be made. This is a best practice for any records which are designated as critical on an Oversight Committee for Public Records retention schedule.

## Electronic Recordkeeping Systems

The Indiana Archives and Records Administration provides a list of criteria for state and local governments searching for a new electronic recordkeeping system (Appendix III: Recommended Capabilities for Electronic Recordkeeping Systems). This checklist is also useful for ensuring an existing system already in use meets recommended best practices. If you would like feedback or to contribute to IARA's research, please send the completed form to the Electronic Records division of IARA, erecords@iara.in.gov.

## Migrating Electronic Files

While the contents of a record may be permanent, the file format and/or media on which it is stored is not. In accordance with retention schedules approved by the Oversight Committee on Public Records, some electronic records may need to be retained by an agency permanently. Even electronic records which do not need to be retained permanently may require a higher level of planning than you may be accustomed to with paper records.

To help ensure continued accessibility, files need to periodically be migrated from one format to another, or from one storage device to another. It is important to familiarize yourself with file format best practices and the manufacturer of any media you must ensure you are migrating according to approved specifications.

When migrating files to a new file format, best practice is to select a format which is:

- Non-proprietary and in common usage
- Uncompressed;  compression is unavoidable, format should be lossless
- Adherent to an open, documented standard
- Interoperable among diverse platforms and applications
- Fully published and available royalty-free
- Developed and maintained by an open standards organization where applicable

If you must use proprietary formats, please select ones which are well supported and in common, widespread use. See the section in these Guidelines on File Formats for specifics.

When migrating files to a new storage device, ensure you understand the lifespan of the device by reading the manufacturer's specifications and reviews of the device. Physical media formats such as disks, CDs, SD cards, and magnetic tape may require further review by IARA prior to transmittal by for potential preservation issues. Your agency may also be required to convert or migrate records if they have not been held in an acceptable modern format. Depending on how files will be transmitted, you may be asked to run a virus scan and submit proof of virus-free files prior to submission.

If you have questions or concerns about file formats or the migration process, please contact the Electronic Records division of IARA, erecords@iara.in.gov.

# Deleting Electronic Records

Electronic records must be disposed of in a manner that protects any sensitive, proprietary, or state security information.

- Electronic records may include structured and unstructured data.
- Destruction is the act of disposing of records permanently by obliterating records and any associated metadata so that the information can no longer be physically or electronically reconstructed or recovered.

## *How to apply this guidance*

1. These guidelines do NOT pertain to anything that is a non-record, such as:
    a. **Personal:** non-work information belonging to the employee.
    b. **Reference:** published materials that your agency did NOT create, is NOT required to collect or store, and are NOT sensitive or confidential.
    c. **Transitory:** external marketing and advertising materials, copies made for individual employee use and convenience, routine messages such as requests for meetings, training opportunities, or social events.
2. These guidelines DO pertain to all types of existing State government records, and to record types that may not yet have been officially scheduled.
3. All records – regardless of format – that are created during the course of State agency business are *public records* and must not be disposed of prior to the end of their retention lifecycle. Destruction of non-transitory records requires the authorization of the Indiana Archives and Records Administration.

Records destruction should be timely, secure, and irreversible. In many operating systems and file storage locations, 'deleting' a file may only remove it to a recycling bin or remove the user's direct access – the file's contents can remain accessible on a hard drive until they are overwritten or in the Cloud until the provider permanently deletes the file. The simple act of deleting a record may not be sufficient to comply with legal regulations if the file is still accessible. Backups and replicated Cloud storage must also be taken into account, as complete destruction includes the Copy of Record as well as any access or backed up files.

Records subject to audit, pending or active litigation, investigations, or request for records are NOT eligible for destruction, even if their retention period has been reached. Agencies may retain records approved for destruction beyond the period outlined in the records schedule if the records in question pertain to a court order, executive order, law, or approved business justification.

Prior to submitting records for destruction:

1. Verify the records series.
    a. Records may not be destroyed if they are not listed on any retention schedule. If a series is not represented on a schedule, contact IARA's Records Management division for more guidance.
2. Ensure that all known audits, investigations, Freedom of Information Act (FOIA) requests, Access to Public Records Act (APRA) requests, retention schedule updates, and litigation activities are resolved.

## *Disposal Procedures*

1. Refer to the approved Agency and/or General Retention Schedule and ensure that the retention period has passed.
    a. When calculating the destruction date, refer to the last date in the range of files. The year of creation must not be counted in the calculation of years to be retained.
2. Verify that the records in question are approved for destruction, rather than transfer to the Indiana State Archives or other procedures and follow any and all listed disposition guidelines.

3. Identify the records due for disposal.
    a. Create an inventory or log of the records to be destroyed for each record series.
    b. Email the log(s) to erecords@iara.in.gov and notify of your intent to destroy. If your request is in good order, it will be forwarded on to the State Records Center.
4. Have your agency's Records Coordinator complete, sign, and submit a State Form 16: Records Disposition Notification to the Records Center.
    a. Indicate that the records are "digital files" and will be destroyed in-house.[1]
    b. DO NOT begin disposal procedures prior to receiving Records Center authorization.
5. Upon approval, destroy records per the appropriate destruction method (purging, overwriting, degaussing, crushing, etc.)
    a. Records Coordinators should work with their IT department, IOT, and / or third party to ensure that all copies of a record are permanently destroyed at the end of its retention period.
    b. Coordinate any backup procedures so no copies of records are maintained after their retention period expires.
    c. If working with a third party (vendor) or Cloud service, disposal is a shared responsibility between the agency and the provider. Any Service Level Agreements (SLAs) should incorporate secure disposal procedures, including the auditing of data erasure to ensure that the data has indeed been destroyed.
6. **Sensitive and confidential data should be destroyed in accordance with relevant state and federal laws and regulations.** Per IC 5–15–5.1–13, confidential records must be destroyed in such a manner that they cannot be "read, interpreted, or reconstructed."
7. Once the records have been destroyed, retain a copy of the State Form 16 within your agency according to GRREC-2.[2]

Further questions about records retention and destruction may be directed to rmd@iara.in.gov.

[1] Digital records stored on physical or virtualized servers are not required to be sent to the Records Center, even if so stated in the series disposition instructions.
[2] Defensible disposition is a cornerstone of good records management. State Form 16 helps your agency prove that records destruction is part of established business practice. Whether you will be destroying your own records or requesting that the Records Center perform the destruction for you, a Records Destruction Notification must be filled out and submitted.

# Frequently Asked Questions About Electronic Records

**What is an electronic record?**

Electronic files that are created in the course of your work are electronic records. (See IC 5-15-5.1 for details).

**Where can I find my electronic records?**

Electronic records may be located in a wide variety of locations including by not limited to:

- Your agency's shared server space
- An electronic recordkeeping system
- A database
- Outlook
- SharePoint
- Chat clients
- Text messages
- Social media
- YouTube

**What are my electronic records?**

Your electronic records are the electronic files that you create in the course of your work. Electronic records commonly created by state employees include but are not limited to email, Word documents, Excel spreadsheets, chats, and text messages.

**Which electronic records do I keep?**

What you need to keep will depend on the subject of the record, its retention period, and whether or not it will need to be transferred to the Indiana Archives.

The best way to determine what you need to keep is to read your agency's retention schedule and the General Records Retention and Disposition Schedule for All State of Indiana Administrative Agencies.

**How long do I need to keep electronic records?**

How long you keep records will depend on the subject of the record, its retention period, and whether or not it will need to be transferred to the Indiana Archives.

The best way to determine what you need to keep is to read your agency's retention schedule and the General Records Retention and Disposition Schedule for All State of Indiana Administrative Agencies.

**What are my electronic records responsibilities?**

You are responsible for understanding how to manage your electronic records over the course of their lifecycle, as well as for understanding the appropriate use of information resources provided by the State. The lifecycle of a record comprises creation through destruction or transfer to the Indiana Archives.

**Which electronic records do I need to send to the Archives?**

Some records with long-term and historic value need to be transferred to the Indiana Archives. This is referred to as being "scheduled for transfer to the Indiana Archives." You can see which records are scheduled for transfer to the Indiana Archives by reading the General Records Retention and Disposition Schedule for All State of Indiana Administrative Agencies and your agency specific retention schedule.

**When do I need to send electronic records to the Archives?**

It will depend on when they are scheduled to be transferred according to their record retention schedule. This can range from the moment the record is considered complete by your agency to years after the record has been created. It is very important to read your agency retention schedule very carefully, as well as the General Records Retention and Disposition Schedule for All State of Indiana Administrative Agencies.

**How do I send electronic records to the Archives?**

You can send electronic records on a hard drive, through SFTP, or by dropping files onto a secure folder on IARA's server. You will need to send them with a manifest, or list of what you are sending that includes information such as the file name and date the file was created.

**How do I know if I have electronic records?**

If you create digital files in the course of your work, chances are you have electronic records.

**How do I know if I have electronic records that need to be saved for a long period of time or that need to be sent to the Indiana Archives?**

If you are a policy maker, decision maker, or are involved in disaster planning or continuity of operations planning the chances are high that you have created electronic records of lasting value to the State that may need to be transferred to the Indiana Archives. The best way to determine if you have records that need to be saved for a significant period of time or transferred to the Indiana Archives is to read your agency retention schedule very carefully, as well as the General Records Retention and Disposition Schedule for All State of Indiana Administrative Agencies.

## Update History

| Date | Description |
|---|---|
| 5/6/2020 | Published out of excerpt from larger set of guidelines that are pending approval by IOT and GOV. Excerpt published for DOR with GOV approval. |
| 6/28/2021 | Updated to include scanning specifications after IARA Executive Director approved. |
| 9/1/2021 | Updated to incorporate State Records Analyst and Electronic Records Archivist suggestions. |
| 9/17/2021 | Published version 1.0. |
| 03/23/2023 | Updated title of section Shared Mailbox to Electronic Mailbox with more information. Published version 2.0. |
| 06/05/2023 | Added a sections Social Media Records Management Best Practices and Deleting Electronic Records. Updated section on long-term retention to permanent retention. |
| 07/07/2023 | Added subsection Quality Control to Recommended Scanning Specifications |

# Appendix I

**Indiana Oversight Committee on Public Records Policy 20-01**
**Electronic Records Retention and Disposition**

**Applies to:** Electronic records of all Indiana government entities except those exempted in IC 5-15-5.1. If records of exempted entities are transferred to the Indiana Archives they must adhere to this policy.

**Purpose:** To ensure electronic records are retained in a trustworthy, accessible, and appropriate manner.

**Effective Date:** 1/15/2020

**Authority:** Indiana Code 5-15-1-1 (a) and (b), Indiana Code 5-15-5.1-12, and Indiana Code 5-15-5.1-14.

**Definitions:**

*Retention schedule* means a Records Retention and Disposition Schedule approved by the Indiana Oversight Committee on Public Records.

*Electronic records* are stored in digital format on an information technology device and include both born-digital and digitized records.

*Born-digital* records are created in electronic format.

*Digitized records* are electronic copies of physical records and can include images and audiovisual information.

*Physical records* can be read without the aid of an information-technology device and include paper, film, and audio and video tapes.

**Policy:**

1) **General requirements:** Unless separate instructions are specified in the retention schedule, the following requirements apply to all records regardless of format
    a) retention period before final disposition.
    b) confidentiality, access, and disclosure.
    c) final disposition: destruction or transfer to the Indiana Archives.
    d) confidential records must be destroyed according to IC 5-15-5.1-13
    e) Critical Records as described by IC 5-15-5.1-1(d) must be microfilmed according to 60 I.A.C. 2.

2) **Indiana Archives transfer:** Electronic records that are required to be transferred to the Indiana Archives according to their retention schedule must be
    a) created and maintained according to OCPR 20-02.
    b) transferred regularly on the timetable specified in the relevant Record Series.
    c) transferred in consultation with Electronic Records division staff.

3) **Agency retention:** Electronic records that are not required to be transferred to the Indiana Archives according to their retention schedule
    a) must be created and maintained by the agency according to OCPR 20-02 for the specified retention period.
    b) are exempt from retention schedule requirements to transfer records to the State Records Center.

4) **Destruction of digitized physical records:** Physical records which have been digitized may be destroyed if
    a) the terms described in Items 1-3 are met.
    b) the imaged records are verifiable authentic duplicates as described in OCPR 20-02.
    c) the terms in the Indiana Archives and Records Administration Electronic Records Guidelines are met.

5) **Destruction of born-digital records:** Born-digital records and their storage media may be destroyed if the terms in Item 1 are met.

6) When its provisions are met, this policy serves as the "written consent of the administration" described in IC 5-15-5.1-14.

# Appendix II

**Indiana Oversight Committee on Public Records Policy 20-02**
**Electronic Records Technical Standards**

**Applies to:** Electronic records of all Indiana government entities except those exempted in IC 5-15-5.1. If records of exempted entities are transferred to the Indiana Archives they must adhere to this policy.

**Purpose:** To establish consistent standards for the creation and maintenance of public electronic records.

**Effective Date:** 1/15/2020

**Authority:** Indiana Code 5-15-5.1(a)(4).

**Definitions:**

*Retention schedule* means a Records Retention and Disposition Schedule approved by the Indiana Oversight Committee on Public Records.

*Electronic records* are stored in digital format on an information technology device and include both born-digital and digitized records.

*Born-digital* records are created in electronic format.

*Digitized records* are electronic copies of physical records and can include images and audiovisual information.

*Physical records* can be read without the aid of an information-technology device and include paper, film, and audio and video tapes.

*Discoverable* refers to the findability of electronic records during information requests, including during litigation.

**Policy:**

1) **Born digital records:** Electronic records must remain accessible for the duration of the retention period specified in their retention schedule. Accessible means that all electronic records must be
   a) readable
      i) by current, commonly available hardware and software OR
      ii) converted by the originating agency if the existing software or hardware is no longer current or commonly-available.
   b) stored appropriately
      i) in an electronic system accompanied by documentation of release notes, functionality, and backup provisions OR
      ii) on physical storage media that is descriptively labeled and readable by commonly available hardware and software.
   c) discoverable
      i) within a reasonable period of time and without excessive effort;
      ii) via original metadata and any metadata that is necessary to understand the content and structure of the record.
   d) properly maintained by the originating agency which includes
      i) migrating when the current storage medium and/or records management system nears the end of its practical lifespan.
      ii) avoiding proprietary storage systems, records management systems, or file formats.
   e) retained in accordance with OCPR 20-01.

2) **Digitized records:** Records which are digitized must adhere to Item 1 of this policy as well as
   a) Indiana Archives and Records Administration Electronic Records Guidelines
   b) act as authentic duplicates, meaning digital images or data must be verified against original records for completeness and accuracy.

3) **Critical records:** Unless alternate arrangements are approved in the retention schedule, Critical Records must be microfilmed according to 60 I.A.C. 2
      a. regardless of their initial format.
      b. in addition to any conversion to electronic format.
      c. before the original hardcopies may be destroyed.

# Appendix III

## RECOMMENDED CAPABILITIES FOR ELECTRONIC RECORDKEEPING SYSTEMS

This checklist is provided by the Indiana Archives and Records Administration (IARA) for use during the selection of a new recordkeeping system or to assess a current system. If you are in the process of looking for a system, this is a useful list of requirements to share with vendors. When you have completed the checklist, please provide a copy to IARA for our research.

If you have questions about electronic recordkeeping systems, would like feedback about your system, or help with this checklist, please reach out to us at erecords@iara.in.gov.

Name of system / software

Name of agency / department

**FILE MANAGEMENT**

- ☐ Supported file formats meet your operational needs
- ☐ Ability to convert files to different formats
- ☐ File naming practices are supported
- ☐ Indexing system support for files and folders
- ☐ Checksums can be created and validated

**SECURITY**

- ☐ Sufficient rights management
- ☐ Sufficient security mechanisms to meet your operational requirements or standards
- ☐ Ability to prevent the alteration or destruction of records prior to the end of their Oversight Committee on Public Records (OCPR) approved records retention schedule *(Please note that destruction requires IARA permission.)*
- ☐ Ability to destroy records in accordance with all relevant policies and procedures
- ☐ System audit capabilities *(at least on an annual basis)*
- ☐ Timestamped audit trails that document the creator, any modifications, and duplications
- ☐ Secure storage and stable environmental conditions for location of hardware and server space *(Cloud storage included)*

**STANDARDS**

- ☐ Compliant with minimum IARA imaging standards *(only pertains to imaging systems)*
- ☐ Provides quality control mechanisms *(only pertains to imaging systems)*
- ☐ Meets any relevant records, data, or information standards

**DISASTER PLANNING**

- ☐ Ability to refresh hardware or media *(Standard is a minimum of every three (3) to five (5) years.)*
- ☐ Data recovery and continuity capabilities
- ☐ System documentation, including updates to new features
- ☐ Accessible, current procedural manual

**ACCESS**

- ☐ Ability to produce records in compliance with litigation, audit, or public records requests
- ☐ Ability to recover lost data or for provide data during a system outage
- ☐ Documentation regarding planned and unplanned downtime and service interruptions
- ☐ Documentation of who owns data in the system and what rights you have

**INGEST / EXPORT**

- ☐ Bulk ingest capabilities, including any metadata
- ☐ Bulk export capabilities, including any metadata
- ☐ Ability to export data in a timely fashion without a burdensome process

**SUPPORT**

- ☐ Vendor offers affordable ongoing technical support
- ☐ Vendor offers affordable ongoing training for users

**EXIT STRATEGY**

- ☐ Documented vendor exit strategy in the event the vendor ceases operation
- ☐ Plan for how you will execute an exit strategy *(Document any resources you will require.)*