


POLICY TITLE: Electronic Records Retention			
		CHILD AND FAMILY SERVICES AGENCY	
Approved By:	Date Approved:	Original Effective Date:	Latest Revision:
Robert L. Matthews	November 29, 2022	November 29, 2022	October 21, 2022

I. AUTHORITY	45 CFR 1355.52 (CCWIS Project Requirements), 75.361 (Retention Requirements for Records), DC Code § 28-4911 (a 1-2), (g) (Retention of Electronic Records), § 2-1706 (Maintenance of Public Records), District of Columbia General Records Schedule 20 (Electronic Records System), and Title IV-E of the Social security Act.
II. APPLICABILITY	This policy applies to all Child and Family Services Agency (CFSA) employees, contractors, and volunteers.
III. RATIONALE	The purpose of this policy is to provide guidelines on the responsible management of all electronic records created or received by CFSA's Child Information Systems Administration (CISA) through the Comprehensive Child Welfare Information System (CCWIS), also known as <u>Stronger Together Against Abuse and Neglect in DC (STAAND)</u> . The management of all Agency electronic records must align and support federal regulations and the District of Columbia Records Retention Schedule 20 .
IV. POLICY	<p>CISA will manage the implementation of CFSA's CCWIS and the creation, receipt, maintenance, use, and disposition of any CFSA's electronic records information that have been stored in the system.</p> <p>Whenever CISA creates or receives an electronic record, it shall be kept in accordance with the established District of Columbia record retention schedule and stored safely so it remains accessible for as long as it's needed.</p>
V. CONTENTS	<ul style="list-style-type: none"> A. Definitions B. Maintaining CFSA's Electronic Data C. Lifecycle of A Record D. Retention of Electronic Records E. Financial Records, Supporting Documents, and Statistical Records A. CFSA Printers and Security Checks
VI. SECTIONS	<p>Section A: Defintions</p> <ol style="list-style-type: none"> 1. Archives: records that have been selected for permanent preservation because of their administrative, informational, legal, and historical value as evidence of official CFSA business. Archives are a very small, but an important subset of CFSA's official records. Archiving electronic records, CISA shall protect valuable evidence of CFSA by ensuring their preservation and availability or accessibility.

	<ol style="list-style-type: none"> 2. Documents: any recorded information or objects that can be treated as individual units. Examples include works in progress such as draft communications or lists, and transitory records such as emails confirming a meeting or acknowledging receipt of a document. If a document is superseded by other documents, such as a draft report that is replaced by a newer version, and the first draft is not needed as evidence, or if the document contains information needed for only a short time – such as a confirmation of the location of a meeting – the document can be destroyed, if it's no longer useful. 3. Electronic record: information recorded by a device that is produced and received by an agency or individual activity that includes emails messages, word-processed documents, spreadsheets, digital images, and databases. 4. Hard copy record: any document, record, report, or data printed on paper. 5. Information: data, ideas, thoughts, or memories irrespective of medium. However, information sources could be considered “non-records” if they are useful but may not provide evidence of a significant activity related to CFSA. Examples include journals, newspapers, publications, or reference sources not created by CFSA’s CISA. If the item in question provides information only and does not provide evidence of an activity, decision, or transaction related to CFSA and is no longer needed, it may be destroyed. 6. Records: information created, received, and maintained as evidence and information by CFSA, in pursuance of legal obligations or in the transaction of official business. Examples include final reports, emails confirming an action or decision, spreadsheets showing budget decisions, photographs, or maps of field missions, which need to be kept as evidence. If the record created or received as a document during CFSA official business and it provides evidence of an activity, decision, or transaction, it shall be kept as evidence, according to the established District of Columbia retention schedule. That document becomes a record and must be stored safely so it remains accessible.
	<p>Section B: Maintaining CFSA’s Electronic Data</p> <p>Any data considered a record created or received by CFSA during official business is the property of the District of Columbia Government and may ONLY be destroyed, sold, transferred, or disposed of in any manner as prescribed by law, by the District of Columbia records retention schedule, or by any other authorization approved by the District of Columbia Records Disposition Committee (DCRDC).</p> <ol style="list-style-type: none"> 1. Any data that includes financial records, supporting documents, statistical records, and all other Agency records pertinent to a federal award shall be kept, and stored in accordance with federal regulations and the District of Columbia record retention schedule.

	<ol style="list-style-type: none"> 2. If any client data is under review, the data shall be retained and available until the review is finished. 3. Any inactive data or record of CFSA which is deemed to have continuing historical, evidentiary, or other significant value (records that are listed based on the electronic records retention schedule 20) shall be properly preserved, arranged, described, and made available for reference purposes or from CFSA's CISA database. 4. Electronic retention schedule applies to any subject-matter that exists in a single document in hard copy form, when converted to electronic form. For example, input data, processing files, transaction files, master files, in addition to the hard copy inputs, record layouts, codebooks, technical specifications, users' guides, and outputs. 5. Any electronic records that CFSA think is not fully covered by the Electronic Records Retention Schedule (75 years or less) shall consult with CFSA's Records Management Unit to determine if the record should be included in the CFSA records retention schedule for electronic records. 6. Electronic records may not be destroyed without an approved records disposition authorization.
	<p>Section C: Lifecycle of A Record</p> <p>The lifecycle of each record and their availability shall be determined by the District of Columbia record retention schedule. The lifecycle in a record refers to the stages of a record's life span from its creation, distribution, organization, storage, retrieval to its preservation or disposal.</p> <ol style="list-style-type: none"> 1. The District of Columbia Record Retention Schedule 20 shall determine if a record can be destroyed or kept for evidentiary, legal, financial, or historical purposes. When a record is in an inactive phase of the lifecycle, CFSA's CISA may free up space for new files, but shall ensure that inactive records that are not destroyed are readily available. 2. To ensure that all inactive records are accessible, CFSA's CISA data administrator shall complete the following tasks: <ol style="list-style-type: none"> a. Identify the records or information that are not required to be stored in a primary data base (e.g., hard copy information) or systems or shared drives, b. Organize and list each record, c. Transfer the record to an electronic storage field for available use, if needed, and d. Retrieve only those records that are needed on an as needed basis. 3. The final stage of the records lifecycle occurs when retention periods expire for inactive records. When record information is identified as no longer being required according to the District's Record Retention Schedule 20, the record may be destroyed or transfer to archives.

	<ol style="list-style-type: none"> 4. There are at least three basic categories for this schedule and they are: <ol style="list-style-type: none"> a. Documentation which covers those records that services code books, record layouts, technical specifications and users' guides for converting from machine-readable data into human readable data. b. Processing files that are raw data input files and valid transaction files used to create or update a master file. c. Master files that constitute the definitive state of electronic records systems, that is, all the data that goes into a file for a definite time period and given final approval. 5. The disposition phase shall be based on the District's Record Retention Schedule 20. There are two disposition actions: archive or destroy. A record or some portion of the record with historical value shall be archived, while parts that have no historical value may be destroyed. 6. To ensure that the disposition phase is carried out correctly, CISA shall partner with CFSA's Records Management Unit to: <ol style="list-style-type: none"> a. Identify records with historical value to be preserved in the CISA CCWIS system for retrievable purposes before they are destroyed with the Records Management Unit. b. Identify records that have no historical value to be destroyed.
	<p>Section D: Retention of Electronic Records</p> <p>Hard copy records can be converted into an electronic format, unless prohibited by federal and District law, but hard copies must be retained in its original format for evidentiary use, auditing, or similar purposes.</p> <ol style="list-style-type: none"> 1. Electronic records information that is retained shall meet the following standards: <ol style="list-style-type: none"> a. Accurately reflects the information set forth in the hard copy record before it was converted into an electronic format; and b. Remains available in electronic format for later reference. 2. If a law requires that a record be retained, the requirement does not preclude CFSA from specifying additional requirements for the retention of a record. 3. As federal guidelines are considered for retention and archiving if the District's requirements will take precedence if they provide more of a stringent retention schedule for certain documents.
	<p>Section E: Financial Records, Supporting Documents, and Statistical Records</p> <p>Generally, the retention requirement for financial records, supporting documents, statistical and the like shall be kept in accordance with CFSA's Records Retention Schedule. Records pertaining to litigation and audits may require additional time and could be retained longer due to appeals or penalties.</p>

	<ol style="list-style-type: none"> 1. For records related to title IV-E reimbursement claims, the retention requirement shall be three years from the date of submission of the final expenditure report. 2. If any litigation or audit of records is started before the expiration of the three-year period, the records shall be retained until all litigation or audit findings involving the records have been resolved and final action has been taken.
	<p>Section F: CFSA Printers and Security Checks</p> <p>All Ricoh Secured printers located throughout CFSA shall operate through a secured network. To obtain printed information from a Ricoh Secured printer, CFSA staff must have an active ID badge or they must use their email address and current password on the printer login prompt to retrieve printouts.</p> <ol style="list-style-type: none"> 1. CISA shall ensure that protective measures are in place to store printed information on all CFSA Ricoh Secured printers 2. To ensure that sensitive information is protected, all CFSA printed information will be sent to a single virtual queue where the job is “parked” and encrypted until the person printing the information log in to use any Ricoh Secured printer on the network to print documents. 3. For basic security checks, CISA will: <ol style="list-style-type: none"> a. Track copier and printer activity by device and user. b. Create and retain system audit logs and records to monitor, analyze and investigate reports of suspicious, unusual, unlawful, or unauthorized system activities. c. Ensure that the actions of individual system users can be uniquely traced to hold them accountable for unauthorized actions. d. Review and update logged events. e. Create an alert in the event of an audit logging process failure. f. Provide audit reports and analysis. g. Design a system structure that compares and synchronizes internal system clocks to generate time stamps for audit records. h. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.