


|   |   |                                 |                       |
|---|---|---------------------------------|-----------------------|
| <b>POLICY TITLE:</b>  | <i>Electronic Signatures</i>            |                                 |                       |
|  | <b>CHILD AND FAMILY SERVICES AGENCY</b> |                                 |                       |
| <b>Approved By:</b>   | <b>Date Approved:</b>                   | <b>Original Effective Date:</b> | <b>Last Revision:</b> |
| Brenda Donald   | July 8, 2019                            |                                 |                       |

|                          |  |
|--------------------------|--|
| <b>I. AUTHORITY</b>      | Mayor's Order 2009-118, June 25, 2009; D.C. Law 14-28, Section 422 (6) of the District of Columbia Home Rule Act of 1973, as amended, 87 Stat. 790, P.L. No. 93-198, D.C. Official Code § 28-4917 (2008 Supp.), § 2-1706(a)(1)(2)(A), and Uniform Electronic Act, 1999.  |
| <b>II. APPLICABILITY</b> | CFSA Staff   |
| <b>III. RATIONALE</b>    | <p>With the advent of modern technology in information systems, business models and methods have evolved to take advantage of the speed, efficiencies, and cost benefits of using electronic signatures on official forms, contracts, certifications, and other legally binding agreements. An electronic signature is a basic term for a variety of methods used as an alternative to traditional ink signatures on paper. It involves a user's interaction with a secure electronic application which eliminates the necessity of the production or use of a hard copy, printed form.</p> <p>Therefore the Agency utilizes electronic signatures to maximize efficiencies in the conduct of Agency business.</p> |
| <b>IV. POLICY</b>        | <p>The Director of the Child and Family Services Agency ("CFSA") adopts this policy to be consistent with the Agency's mission and all applicable federal, District of Columbia laws, Personnel Regulations, and applicable collective bargaining agreements.</p> <p>Following receipt of written approval from the District of Columbia's Office of the Secretary, CFSA may utilize, endorse, send and accept electronic signatures that are classified as common electronic signature or digital signatures in the conduct of Agency business, provided that the use of such methods comply with the internal policy guidelines outlined herein.</p>   |
| <b>V. CONTENTS</b>       | <p><b>A.</b> Acceptable Electronic Signature Methods</p> <p><b>B.</b> Elements of Electronic Signature Authentication and Security</p> <p><b>C.</b> Role-based Assignment and Guidelines for Using Electronic Signatures</p> <p><b>D.</b> Records Retention Guidelines</p>   |

|                       |                    |
|-----------------------|--------------------|
| <b>POLICY TITLE</b>   | <b>PAGE NUMBER</b> |
| Electronic Signatures | Page 1 of 4        |

**VI. SECTIONS**

**Section A: Acceptable Electronic Signature Methods**

An electronic signature is an alternative to a traditional ink signature on paper. There are three basic classifications, two of which are appropriate for use for CFSA officials in the conduct of official Agency business.

*Common Electronic Signatures*

1. Common electronic signatures do not employ a specific technology to increase the security, authenticity, or evidentiary value of a signature. Common signatures may include:
  - a. a digitized image of a handwritten signature
  - b. a password or personal identification number
  - c. a mark or symbol indicating an intent to sign
  - d. a symbol (typically “/s/”) affixed to a digital document that demonstrates that the paper copy sent to the addressee was signed with a conventional “wet” signature.
2. Common electronic signatures may be used for non-binding internal documents or public-facing publications such as:
  - a. Policies and other guidance
  - b. Internal memoranda
  - c. Announcements or proclamations for distribution to a large distribution list
  - d. internally stored documents

*Digital Signatures*

3. A digital signature, in conjunction with a digital certificate, uses a private key to sign and encrypt the document and a public key to de-encrypt and authenticate the signature. A digital signature offers the highest level of authenticity, security, and integrity and requires specialized technology to implement.
4. Digital signatures may be used for legally binding documents such as:
  - a. Offer letters
  - b. Contracts
  - c. Memoranda of Understanding or Agreement (MOU/MOA)
  - d. Rental or lease agreements
  - e. Liability waivers
  - f. Financial Agreements
5. CFSA shall operate within District of Columbia standards for system interoperability for digital signatures that are established by the appropriate District authority.

|  |   |
|--|---|
|  | <p style="text-align: center;"><b>Section B: Elements of Electronic Signature Authentication and Security</b></p> <ol style="list-style-type: none"> <li>1. CFSA shall have a plan in place to authenticate that the electronic signature is from the person it represents and has not been altered or misrepresented.</li> <li>2. Signature Intent: The process used to obtain the electronic signature shall demonstrate and document that the user intended to sign the record. Establishing intent includes: <ol style="list-style-type: none"> <li>a. Identifying the process for using an electronic signature to sign a record (made apparent within the context of the transaction).</li> <li>b. Ensuring that the signer has approved each and every individual use of her or his electronic signature.</li> <li>c. Providing notice to the signer that their electronic signature is about to be applied to, or associated with, an electronic record (such as an online notice advising the signer that continuing the process will result in an electronic signature).</li> </ol> </li> <li>3. The Agency shall ensure that any hardware, software, and application used to make digital signatures has secure technology features in place that will link the electronic signature to an individual and device.</li> <li>4. With respect to digital signatures, CFSA shall maintain adequate documentation of the system design, implementation, use, and movement. The documentation shall include a narrative description of the system, physical and technical characteristics, and any other technical information required to access or process an electronic signature. This shall be done in collaboration with the DC Public Records Administrator.</li> <li>5. CFSA shall employ a non-repudiation system to protect against an individual or entity being able to deny having performed a particular action related to an electronic signature. Essential elements of the non-repudiation system include: <ol style="list-style-type: none"> <li>a. Evidence of the origin of the signature</li> <li>b. Evidence of the record being sent</li> <li>c. Evidence of receipt</li> <li>d. A timestamp, as needed, by the agency or origin</li> <li>e. Long-term storage of evidence</li> </ol> </li> <li>6. CFSA's Child Information System Administration ("CISA") shall determine the risks and benefits of the available technologies for specific applications.</li> </ol> |
|  | <p style="text-align: center;"><b>Section C: Role-based Assignment and Guidelines for Using Digital Signatures</b></p> <ol style="list-style-type: none"> <li>1. The Director or designee or designee shall determine which employees will be approved for use of digital signatures, the scope of the employee's authority to use them, the designees of signatory authorities to execute them, and the purposes for their use.</li> </ol>   |
| <p><b>POLICY TITLE</b><br/>Electronic Signatures</p> | <p><b>PAGE NUMBER</b><br/>Page 3 of 4</p>   |

|  |   |
|--|---|
|  | <ol style="list-style-type: none"> <li>2. The Director shall provide to the approved user of a digital signature a letter authorizing the issuance of the digital signature certificate. The letter shall outline the procedures for the protection of digital signatures and notify users of the process for suspension or revocation of digital signature certificate.</li> <li>3. Users of digital signatures shall protect and not disclose or make available their digital signature, private key or password to other persons.</li> <li>4. CISA shall be responsible for revoking or sending a revocation notice to the certification authority for employees no longer authorized to conduct electronic business on behalf of CFSA.</li> <li>5. CFSA shall only use or accept digital certificates if they are issued by authorized certification authorities.</li> </ol>  |
|  | <p><b>Section D: Records Retention Guidelines</b></p> <ol style="list-style-type: none"> <li>1. CFSA shall retain records created as electronic transactions according to the District of Columbia General Retention Schedule, and the District of Columbia Electronic Records Management Guidelines.</li> <li>2. Any record (hard copy or electronic) created or received by CFSA in the course of official business shall not be destroyed, sold, transferred, or disposed of in any manner, as prescribed by law and by the District of Columbia Records Retention Schedule and the District of Columbia Electronic Records Management Guidelines.</li> <li>3. Within the District of Columbia Retention Schedule and the District of Columbia Electronic Records Management Guidelines, if requested, an electronic record must be located, retrieved, presented, and interpreted in connection with the business transaction that created it.</li> <li>4. Electronically signed records shall contain all the information necessary to reproduce the entire electronic record and associated signatures in a form that permits the person viewing or printing the entire electronic record to verify the following: <ol style="list-style-type: none"> <li>a. The contents of the electronic record.</li> <li>b. The method used to sign the electronic record, if applicable.</li> <li>c. The person(s) signing the electronic record.</li> <li>d. The date when the signature was executed.</li> </ol> </li> </ol> |

|                       |                    |
|-----------------------|--------------------|
| <b>POLICY TITLE</b>   | <b>PAGE NUMBER</b> |
| Electronic Signatures | Page 4 of 4        |