

ORC: 117.11; 149.43; 304.01; 1306.01-21; 5153.17
OAC: 123:3-1-01
COA: _____
CFSR: _____
Board: _____
Other: _____

Next Review Date: 9/19
Last Reviewed: 9/16
Review Responsibility: Executive Council

FCCS PROCEDURE

NO.: 12C.09

SUBJECT: Responsible Use of Digital and Electronic Signature

Approved by: Executive Council
Effective Date: August 29, 2011
Date(s) of Revision: Sep 20, 2016
Responsible for Implementation: All Staff

Responsible Use of Digital and Electronic Signature

Administrative Policy

The digital and electronic signature capability is a powerful time saving and efficiency device. However, the inappropriate use of the digital and electronic signature capability can expose the employee and/or the agency to the following types of risks (included but not limited to):

- 1) Negative legal repercussions.
- 2) Contested work products.
- 3) Invalid electronic documents.
- 4) Contested auditing issues.

Procedure for Responsible Use of Digital and Electronic Signature Includes:

- 1) Contact the Information Technology Service Desk to physically capture your digital signature.
 - a) Agency staff will log into a secure device using their FCCS credentials.
 - b) IT staff will walk them through the process of physically capturing and saving their digital signature.

- c) Agency staff will only be able to place their digital signature on a PDF document while connected to the FCCS Network, on an Agency issued device that they have logged into using their FCCS credentials.
 - d) The only signature Agency staff will see is the captured signature that is connected to their FCCS credentials.
- 2) Each employee is responsible for safely maintaining and guarding their FCCS system password.
 - a) Each employee must follow all documented and prescribed policies regarding passwords (see Policies and Procedures section 12C.8 Passwords).
 - b) Each employee should create a strong password for system log in. Strong passwords are the key security procedure employed in the use of electronic signatures. This includes a unique user – ID and an alphanumeric password consisting of at least eight characters including a mix of text and numbers.
 - c) Each employee must maintain the privacy of their password. A password must never be shared or revealed to anyone else. Revealing a password exposes the authorized user to responsibility for actions that another party takes with the password.
- 3) An employee should never access or use another's password. The use of the digital and electronic signature capability should only be used on those electronic records identified and prescribed by the agency:
 - a) This policy applies to all case related documents including but not limited to the following:
 - i) All case related documents including CAPMIS tools, Referral forms, Consent for Information Release, Letters, Memos, Medical Consent and Court Activity Request and Results (CARR).
 - b) Agency contracts and correspondence.
- 4) Agency staff may obtain electronic signatures on any of the above documentation using their mobile device. Agency staff must utilize their digital signature to witness the electronic signature on each document.
- 5) Any violation or misuse pursuant to this policy should be reported directly to the employee's supervisor and the Director of Information Technology for review and possible investigation.

Security

Franklin County Children Services has two levels of security which apply to digital signatures.

- 1) When the user captures their signature, they must log into the device using that FCCS authenticated credentials (unique username and password) to capture their signature. Their signature is then attached to that profile and cannot be accessed using any other username/password combination.
- 2) Users must be authenticated FCCS users and must use at a minimum a unique user-ID and alphanumeric password consisting of at least eight characters, or other security procedures or features as approved by IT. In cases where a user password is used for digital signature authentication, the user must sign in to the device and select their signature. They will only have the option of their signature.

Relevant Definitions:

- 1) *Electronic record* means a record created, generated, sent, communicated, received, or stored by electronic means. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record. Digital and electronic signature systems should provide the signatory and recipient with the ability to print a copy of the document.
- 2) *Electronic signature* means an electronic symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record. Electronic signatures have the equivalent level of legal protection that is given to paper-based signatures. Unlike digital signatures, they cannot by themselves guarantee signer identity and intent, data integrity, and non-repudiation of signed documents.
- 3) *Digital Signature* are a sub-group of electronic signatures that provides the highest levels of security and universal acceptance so that they cannot be copied, altered or tampered with. Digital signatures are based on Public Key Infrastructure (PKI) technology. Through the use of cryptographic operations, digital signatures create 'fingerprint' unique to both the signer and the content, thus ensuring both signer identity and content integrity. Digital signatures can be easily validated.

- 4) *Security Procedure* means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the algorithms or other codes, identifying work or numbers, encryption, or call back or other acknowledgement procedures.
- 5) *Identification and Authentication* means the verification of the identity of a requesting entity (a process helps to enforce access control to the system by verifying the identity of the entity, computer, system or process). Once it is determined who may have access to a system, the identification and authentication (I&A) process helps to enforce access control to the system by verifying the identity of the entity. Systems may use a variety of techniques or combinations of techniques such as user-ID, password, personal identification number and digital certificates to enforce I&A depending on the level of access control required to protect the system.
- 6) *Integrity* means the assurance that information is not changed by accident or through a malicious or otherwise improper act. Any changes occurring through the transmission or processing of an electronic record should either invalidate the signature or clearly show the change and create a security log identifying the user or system that produced the change and the time that it occurred. Comparative record audits and internal control procedures should also be considered to ensure the integrity of the information. These control procedures should be recorded in the system documentation along with any changes to the application, system environment and operating procedures during the lifetime of the system.
- 7) *Risk Assessment* means a process concerned with identifying, analyzing and responding to IT security risks. Risk assessment attempts to maximize the results of positive events and minimize the results of negative events.
- 8) *Interface Requirements* means that there must be a separate and distinct action on the part of the person for each signature action. The separate and distinct action must be clearly marked as indicating the user's intent to electronically sign a record. The separate and distinct action may include a series of keystrokes, a click of a mouse or other similar action.
- 9) *Nonrepudiation* procedures are designed to ensure that the signatory adopted or assented to the record or electronic transaction. An example would be a statement as follows: "By pressing the 'Submit' button you are certifying that you

are an authorized user of this system and agree that you are submitting an Electronic Signature which is comparable to your written signature for the purpose of this document.”

Failure to Comply With Responsible Use of the Digital and Electronic Signature Policy:

Franklin County Children Services will monitor use of the Digital and Electronic Signature Policy. Staff who fail to use this technology responsibly in accordance with this policy may have their access restricted and/or be subject to discipline. Any instances of irresponsible use shall be referred to the employee's supervisor for review and possible investigation.



Protecting Children by Strengthening Families

Date:

Electronic Signature Confirmation

Memorandum for entry of electronic signature into the CoSign product:

Based on my participation in the Electronic Case File and other SharePoint related initiatives, I hereby confirm the following:

I have read, understand and will comply with the following policies:

- Responsible Use of Technology
- Responsible use of Agency email
- Passwords
- Responsible use of Electronic Signature

I understand that my personal signature has been captured in the CoSign product and will be affixed to various internal and external documents (faxes, forms) as I willingly choose. I understand this is a legally binding signature and will not share or compromise my password (or other authentication devices) or those of my co-workers which controls access and usage of my signature and the signature of others.

Printed name

Witnessed by name

Signature

Witnessed by signature