

Florida Supreme Court Standards for Electronic Access to the Courts

Adopted June 2009

Adopted modifications November 2016

Version 17.0

TABLE OF CONTENTS

1.0. PORTAL TECHNOLOGY STANDARDS	4
2.0 PORTAL FUNCTIONALITY	4
2.1. E-Portal Minimal Functionality.....	4
3.0 ELECTRONIC TRANSMISSION AND FILING OF DOCUMENTS.....	4
3.1. E-Filing Standards.....	4
3.1.1. Size of Filing.....	4
3.1.2. Document Format	4
3.1.3. Document Rendering	5
3.1.4. Archiving	5
3.1.5. File Name Standards.....	5
3.1.6. Time Stamp.....	6
3.1.7. Electronic Notification of Receipt	7
3.1.8. Review by Clerk of Court	7
3.1.9. Security.....	7
3.1.10. Filing Process and Payment	7
3.1.11. Transmission Envelope.....	7
3.1.12. Court Control of Court Documents - Data Storage.....	8
3.1.13. Requirements for Individual Filers	8
3.1.14. Adding a Party	9
3.1.15. Docket Numbering.....	9
3.2. TECHNICAL FAILURE	9
3.2.1. Retransmission of Electronic Filing.....	9
3.2.2. System Availability and Recovery Planning.....	9
3.3. ADA AND TECHNOLOGY COMPLIANCE	11
3.4. ELECTRONIC PROCESSES - JUDICIAL.....	11
3.4.1. Delivery of Electronic Case Files	11
3.5. ELECTRONIC SIGNATURES	12

3.5.1. Signatures of Registered Users 12

3.5.2. Multiple Attorneys of Record Signatures 12

3.5.3. Original Documents or Handwritten Signatures 12

3.5.4. Judge Signature 12

 3.5.4.1. Security 13

 3.5.4.2. Functionality 13

3.5.5 Clerk Signature 13

3.6 ELECTRONIC NOTARIZATION 13

1.0. PORTAL TECHNOLOGY STANDARDS

The Florida Court's E-Filing Portal ("Portal") is governed by the Florida Courts E-Filing Authority. The Portal provides a single statewide point of access for filing court records and interfaces with other existing statewide information systems.

2.0 PORTAL FUNCTIONALITY

2.1. E-Portal Minimal Functionality

1. Single statewide login.
2. Process for non-attorneys and for self-represented users to access the system.
3. Uniform authentication method.
4. Single point of access for filing and service.
5. Consolidated electronic notification.
6. Process for local validation.
7. Automated interface with other e-filing systems.
8. Utilize the current XML ECF Standards.
9. Accommodate bi-directional transmissions to and from courts.
10. Integrate with other established statewide systems.
11. Accept electronic forms of payment.
12. All court based e-filing processes will use Internet-based open standards.

3.0 ELECTRONIC TRANSMISSION AND FILING OF DOCUMENTS

With the establishment of the Florida Courts E-Filing Portal, the Florida Courts have a single state-wide e-filing system. On June 21, 2012, the Supreme Court issued opinions approving recommendations to require e-filing by attorneys and e-service, through a phased in implementation.

3.1. E-Filing Standards

3.1.1. Size of Filing

A single submission, whether consisting of a single document or multiple documents, shall not exceed 50 megabytes (50 MB) in size.

3.1.2. Document Format

All electronically filed documents should be legibly typewritten or printed on only one side of letter sized (8 ½ by 12 inch) paper; should have one inch margins on all sides and on all pages and pages should be numbered consecutively; should be filed in a format capable of being electronically searched and printed; should be filed in black and white; reduction of legal-size (8 ½ by 14 inches) documents to letter size (8 ½ by 12 inches) is prohibited; documents that are to be recorded in the public records of any county shall leave a 3-inch by 3-inch space at the top right-hand corner of the first page and a 1-inch

by 3-inch space at the top right-hand corner on each subsequent page blank and reserved for use by the clerk of court; Optical Character Recognition (“OCR”) scanned documents should be at a resolution of 300 DPI as defined in the State of Florida Electronic Records and Records Management Practices; at all times possible, documents should be electronically signed as defined in Section 2.8; multiple pleadings, motions, etc., should not be combined into one single file, but rather each individual document should be uploaded via the Portal document submission process and should comply with accessibility requirements set forth in section 2.6. Deviation from these guidelines may result in the submitted filing being moved to the Pending Queue by the Clerk with the filer being notified via email and requested to correct the issue(s) with the document(s) and resubmit the filing.

3.1.3. Document Rendering

The clerk shall be able to render document images in searchable PDF format for viewer interfaces where the judicial viewer does not already provide searchable documents.

3.1.4. Archiving

Electronic documents shall be archived in a manner that allows for presenting the information in the future without degradation, loss of content, or issues with software compatibility relative to the proper rendering of electronic documents.

3.1.5. File Name Standards

The following special characters are not allowed in a file name:

- Quotation mark (")
- Number sign (#)
- Percent (%)
- Ampersand (&)
- Asterisk (*)
- Colon (:)
- Angle brackets (less than, greater than) (< >)
- Question mark (?)
- Backslash (\)
- Slash (/)
- Braces (left and right) ({ })
- Pipe (|)
- Tilde (~)

File names may not end with any of the following strings:

- .files
- _files
- -Dateien
- _fichiers
- _bestanden
- _file
- _archivos

- -filer
- _tiedostot
- _pliki
- _soubory
- _elemei
- _ficheiros
- _arquivos
- _dosyalar
- _datoteke
- _fixters
- _failid
- _fails
- _bylos
- _fajlovi
- _fitxategiak

In addition, file names cannot exceed 110 bytes in length, including spaces. Spaces must be counted as three (3) bytes each.

This required information will be submitted in a uniform e-filing envelope, in compliance with current rules of procedure. The Florida Courts Technology Commission (FCTC) has established, and shall update as necessary, the requirements for the e-filing envelopes for each division and court type. The e-filing envelope will be maintained on the e-filing system of each court. These requirements can be found at <http://www.flcourts.org/resources-and-services/court-technology/efiling/>.

The e-filing envelope shall be designed to collect the data elements in .XML format that support the filing, indexing, docketing, calendaring, accounting, reporting, document development, case management and other necessary functions of the court. In an effort to reduce redundant data entry, emphasis is placed on providing the ability to extract text from the electronic submission.

3.1.6. Time Stamp

Date and time stamp formats must include a single line detailing the name of the court or Portal and shall not include clerk seals. Date stamps must be 8 numerical digits separated by slashes with 2 digits for the month, 2 digits for the date, and 4 digits for the year. Time stamps must be formatted in 12 hour time frames with a.m. or p.m. included. The font size and type must comply with The Americans with Disabilities Act requirements.

The Portal's official file stamp date and time shall be affixed in the upper left hand corner. The Florida Supreme Court and District Courts of Appeal stamps shall be on the left margin readable horizontally. Any administrative agency stamp shall be in the right margin and readable horizontally. The clerk's stamp for circuit and county courts shall be in the bottom of the document.

3.1.7. Electronic Notification of Receipt

All submissions must generate an acknowledgment message that is transmitted to the filer to indicate that the portal has received the document.

At a minimum the acknowledgment must include the date and time the submission was received which is the official filing date/time.

3.1.8. Review by Clerk of Court

When information has been submitted electronically to the Clerk of Court's Office, via the Florida Courts E-Filing Portal, the Clerk of Court will review the filed document and determine whether it contains the required information for placement into the clerk's case maintenance system. If, during the local document receiving process a determination is made that the filed document conflicts with any court rules or standards, then the clerk shall place the filed document into a pending queue. A filing may be placed in a pending queue for any reason that prevents the filing from being accepted into the clerk's case maintenance system, e.g. documents that cannot be associated with a pending case; a corrupt file¹; or an incorrect filing fee.

Once placed in a pending queue, the clerk shall attempt to contact the filer and correct the identified issue(s). The filing will remain in a pending queue for no more than 5 (five) business days, after which time the filing will be docketed, as filed, and processed for judicial review.

3.1.9. Security

The Portal shall provide initial screening and protection against unauthorized network intrusions, viruses, and attacks for all filings. The Portal shall be isolated from other court networks or applications. Software and security devices such as antivirus software, firewalls, access control lists, filters and monitoring software must be used by the Portal to provide this initial protection to court networks.

Computers that receive and accept filings from the Portal must be protected against unauthorized network intrusion, viruses, and attacks. These computers interface with the local CMS to accept e-filings. Software and security devices such as antivirus software, firewalls, access control lists, filters, and monitoring software must be used to protect the local court systems.

3.1.10. Filing Process and Payment

The Portal shall support both an interactive filing process and a batch (non-interactive) process. The Portal shall support electronic payment methods.

3.1.11. Transmission Envelope

Any electronic document or information submitted through the Portal with an initial filing or any subsequent case action must be transmitted using a data structure that

¹ Document(s) that cannot be opened or read

provides universal access to the court file. A submission, whether consisting of a single document or multiple documents, shall not exceed 50 megabytes (50 MB) in size.

The Portal shall be capable of providing a validation of the submission to detect any discrepancies (e.g., incomplete data or unacceptable document type) or other problems (e.g., viruses) prior to being received by the Portal. Where possible, the filer will be notified immediately if the Portal detects discrepancies or other problems with the submission, based on technical issues. The validation rules will be specific to the type of submission (for example: new case initiation as opposed to filings in an existing case).

3.1.12. Court Control of Court Documents - Data Storage

The official copy of court data must be physically located in Florida and in the custody of the clerks of court. Copies of data may be stored within or outside the State of Florida for the purposes of disaster recovery of business continuity.

3.1.13. Requirements for Individual Filers

3.1.13.1 Embedded Hyperlink

Hyperlinks embedded within a filing should refer only to information within the same document, or to external documents or information sources that are reasonably believed to be trustworthy and stable over long periods of time. Hyperlinks should not be used to refer to external documents or information sources likely to change.

3.1.13.2 Exhibits

Each exhibit accompanying a document shall be separately attached and denominated with a title referencing the document to which it relates. Each exhibit shall conform to the filing size limitation in Section 3.1.1. To the extent an exhibit exceeds the size limitation each portion shall be separately described as being a portion of the whole exhibit (e.g., Exhibit A, Part 1 of 5, Part 2 of 5, etc.).

Each documentary exhibit marked for identification or admitted into evidence at trial shall be treated in accordance with Florida Rule of Judicial Administration 2.525(d)(4) or (6), and then converted by the clerk and stored electronically in accordance with rule 2.525(a).

3.1.13.3 Confidentiality and Sensitive Information

The Portal shall provide the following warning before documents are submitted through the Portal, “WARNING: As an attorney or self-represented filer, you are responsible to protect confidential information under Florida Rules of Judicial Administration [2.420](#) and [2.425](#). Before you file, please ensure that you have complied with these rules, including the need to complete a Notice of Confidential Information [form](#) or motion required under Rule 2.420 regarding confidential information. Your failure to comply with these rules may subject you to sanctions.”

3.1.13.4 Emergency Filing

The Portal must provide a mechanism to indicate that a filing is an emergency.

3.1.14. Adding a Party

The Portal shall facilitate the addition of parties after the initial pleading is filed.

3.1.15. Docket Numbering

- At a minimum, the local clerk CMS would assign and store a sequence number for each docket entry that contains a document on each case. The sequence number would be unique only within each case. For example, each case will start with 1, 2, 3, etc. and increment by 1.
- The sequence number would be displayed on each document/docket display screen in the local clerk CMS and any associated access systems (websites, etc.)
- Each assigned document/docket sequence number would need to remain static for each case once assigned. If documents/dockets are inserted, then the sequence numbers would not necessarily align with the dates for the documents/docket. As long as they are unique within each case this would be allowed.
- The sequence number may be implemented on a “go-forward” basis if necessary; sequence numbers are not required for historical documents/dockets.
- The sequence numbers are only assigned and stored in the local clerk CMS. The sequence numbers would not be included in the interface between the Portal and the local clerk CMS and would not be provided to the filer as part of the e-filing notification process.
- This requirement does not apply to legacy CMS applications which have a known end date.

3.2. TECHNICAL FAILURE

3.2.1. Retransmission of Electronic Filing

If, within 24 hours after filing information electronically, the filer discovers that the version of the document available for viewing through the Electronic Case Filing System is incomplete, garbled or otherwise does not depict the document as transmitted, the filer shall notify the Clerk of Court immediately and retransmit the filing if necessary.

3.2.2. System Availability and Recovery Planning

Computer systems that are used for e-filings must protect electronically filed documents against system and security failures during periods of system availability. Additionally, contingencies for system failures and disaster recovery mechanisms must be established. Scheduled downtime for maintenance and updates should be planned, and a notification shall be provided to filers in advance of the outage. Planned outages shall occur outside normal business hours as determined by the Chief Judicial Administrative Officer of the Court. E-filing systems shall comply with the security and backup policies created by the Florida Courts Technology Commission.

Plan 1: Contingency Plan

Timeframe: Immediate - during normal working hours.

Scope: Localized system failures while court is still open and operational. This plan will also be put into operation when Continuity of Operations (“COOP”) and Disaster Plans are implemented.

Operational Levels: Levels of operation will be temporarily limited and may be conducted in electronic or manual processes. Since court will still be open, this plan must address how documents will be received while the system is down.

Objectives:

- Allow the court to continue with minimum delays by providing a temporary alternate solution for access to court files.
- Conduct tests to verify the restoration process.
- Have local and local off site backup of the operating system, application software, and user data available for immediate recovery operations.
- Identify areas where redundancy is required to reduce downtime, and provide for “hot” standby equipment that can be utilized in the event the Contingency Plan is activated.

Plan 2: Business Continuity/Disaster Recovery

Timeframe: Disaster dependent, varies.

Scope: Declared disasters either local or regional that impact the geographic area.

Operational Levels: Temporarily unavailable or limited until facilities are deemed functional or alternate facilities can be established. Mission Essential Functions as defined in the Supreme Court’s COOP for the affected area must be addressed in the designated priorities and timeframes.

Objectives:

- Allow court operations to recover in the existing location or alternate facility.
- Provide cooperative efforts with impacted entities to establish access to court files and allow for the continuance of court proceedings.
- Provide in the Contingency Plan a temporary method to meet or exceed Mission Essential Functions identified in the Supreme Court’s COOP.
- Provide another tier level of recoverability by having a backup copy of the operating system, application software, and user data in a protected environment outside of the local area not subject to the same risks as the primary location for purposes of recovery according to standards approved by the FCTC.
- This plan may provide another out-of-state tier for data backup provided that the

non-local in-state tier is established.

3.3. ADA AND TECHNOLOGY COMPLIANCE

All Court technology must comply with the Americans With Disabilities Act (“ADA”).

3.4. ELECTRONIC PROCESSES - JUDICIAL

The integrity of and efficient delivery of information to the judiciary are primary goals. Any electronic processes that involve the judiciary must be approved by the judiciary prior to implementation.

3.4.1. Delivery of Electronic Case Files

An electronic case file being provided to the court should meet or exceed the capabilities and ease of use provided by a paper case file. Electronic documents shall be available to court officers and personnel in a manner that provides timely and easy access, and shall not have a negative operational impact on the court. The court shall have the opportunity to review and approve any changes to the current business process before the system may be implemented.

Any system that intends to deliver electronic files instead of paper files in part or in total that impacts the judiciary, that involves electronic workflow, functionality, and electronic document management service must be approved by the judiciary before the paper files may be discontinued. The Clerk of Court must be able to deliver paper case files upon request until the electronic case file delivery system is fully accepted by the judiciary. The electronic file created by the Clerk of Court shall be made available and delivered to the judiciary in a manner that provides improved workflow and document management service to the judiciary and court staff. At a minimum, the system must have search capability to find cases, have the ability to incorporate digital signatures, the ability to attach notes to cases, and be able to print specific portions or all pages of a document. The system must have logging capabilities for events such as failures, outages, correction of case file numbers, deletion of documents, and rejections due to incorrect filing or unusable documents due to poor quality images. Documents in an electronic file shall be available for viewing by the court immediately upon acceptance and validation by the clerk of court.

The court must validate that the electronic case file is accurate, reliable, timely, and provides needed reporting information, and is otherwise acceptable as part of its review and acceptance process.

3.5. ELECTRONIC SIGNATURES

3.5.1. Signatures of Registered Users

A submission by a registered user is not required to bear the electronic image of the handwritten signature or an encrypted signature of the filer. Electronic signatures may be used in place of a handwritten signature unless otherwise prohibited by law. The information contained in the signature block shall meet the following required elements defined in Rule 2.515(a) and (b), Florida Rules of Judicial Administration. Electronic signature formats of s/, /s or /s/ are acceptable. Additional information is optional.

Attorney Example

s/ John Doe
Bar Number 12345
123 South Street
City, FL 12345
Telephone: (123) 123-4567

ProSe Example

s/ Jane Doe
123 North Street
City, FL 12345
Telephone: (123) 123-4567

3.5.2. Multiple Attorneys of Record Signatures

When a filing requires the signatures of two or more attorneys of record:

The filing attorney shall initially confirm that the content of the document is acceptable to all attorneys required to sign the document and shall obtain the signatures of all attorneys on the document. For this purpose, physical, facsimile, or electronic signatures are permitted.

The filing attorney then shall file the document electronically, indicating the signatories, (*e.g.*, “s/ Jane Doe,” “/s John Smith,” “/s/ Jane Doe Smith,” etc.) for each attorney’s signature.

3.5.3. Original Documents or Handwritten Signatures

Original documents, such as death certificates, or those that contain original signatures such as affidavits, deeds, mortgages and wills must be filed manually until further standards have been adopted.

3.5.4. Judge Signature

Judges are authorized to electronically sign all orders and judgments. If digitized signatures of judges are stored, they are to be placed at a minimum 256 bit encryption and protected by user authentication.

3.5.4.1. Security

An electronic signature of a judge shall be accompanied by a date, time stamp, and the case number. The date, time stamp, and case number shall appear as a watermark through the signature to prevent copying the signature to another document. The date, time stamp, and case number shall also appear below the signature and not be obscured by the signature. When possible or required, the case number should be included also. Applications that store digitized signatures must store signatures in compliance with FIPS 140-2.

3.5.4.2. Functionality

The ability to affix a judicial signature on documents must include functionality that would improve the process. This functionality at a minimum should include the following:

1. The ability to prioritize documents for signature.
2. Allow multiple documents to be reviewed and signed in a batch in addition to individually.
3. The judge must have the ability to review and edit, reject, sign and file documents.
4. Have a standard signature block size on the document.
5. Allow forwarding of queued documents to another judge for signature if the primary judge is unavailable.
6. After documents are signed or rejected, they should be removed from the queue.
7. Have the ability to electronically file the signed documents into the case management system to be electronically distributed to all appropriate parties.

3.5.5 Clerk Signature

Unless otherwise required by law, Clerks and Deputy Clerks are authorized to electronically sign any documents that require the signature of the clerk, subject to the same security requirements that apply to a judge signature under standard 3.5.4.1.

3.6 ELECTRONIC NOTARIZATION

Electronic notarization is authorized as provided in Florida Statute 117.021.