# Florida Supreme Court Technology Standards

Adopted February 2021

**Version 1.0**

## Table of Contents


SECTION 1 PURPOSE ..... 7
SECTION 2 E-FILING STANDARDS ..... 8
2.1 FILER AND DOCUMENT FILING STANDARDS ..... 8
2.1.1 Electronic Transmission and Filing of Documents ..... 8
2.1.2 Document Filing ..... 8
2.1.3 Size of Filing ..... 8
2.1.4 Document Creation and Format ..... 9
2.1.5 Requirements for Individual Filers ..... 10
2.1.6 File Name ..... 10
2.1.7 Retransmission of Electronic Filing ..... 11
2.1.8 Electronic Signatures ..... 11
2.2 PORTAL FUNCTIONALITY ..... 12
2.2.1 Minimum Functionality ..... 12
2.2.2 Electronic Filing Envelope ..... 13
2.2.3 Portal Time Stamp ..... 13
2.2.4 Electronic Notification of Receipt ..... 13
2.2.5 Review by Clerk of Court ..... 13
2.2.6 Docket Numbering ..... 14
2.2.7 Security ..... 14
2.2.8 Filing Process ..... 14
2.2.9 Submission Validation ..... 14
2.2.10 Adding a Party ..... 14
2.2.11 Confidentiality and Sensitive Information ..... 14
2.2.12 Emergency Filing ..... 15
2.2.13 System Availability and Recovery Planning ..... 15
2.2.14 Document Filing ..... 16
2.2.15 Electronic Notarization ..... 16
SECTION 3 ELECTRONIC COURT RECORDS CUSTODIAN STANDARDS ..... 17
3.1 Court Document Format ..... 17
3.2 ADA Compliance ..... 17
3.3 Court Records Redaction ..... 17
3.4 Court Records Storage ..... 17
3.5 Court Records Backup and Archival ..... 18

SECTION 4 CLERKS CASE MAINTENANCE SYSTEM STANDARDS ..... 19
4.1 CMS STANDARDS ..... 19
4.1.1 Document Rendering ..... 19
4.1.2 Electronic Filing Envelope ..... 19
4.1.3 Clerk's Time Stamp ..... 19
4.1.4 Docket Numbering ..... 19
SECTION 5 ACCESS TO ELECTRONIC COURT RECORDS ..... 21
5.1 Purpose and Scope ..... 21
5.2 Access Methods ..... 21
5.3 Access Security Matrix ..... 21
5.4 User Agreements ..... 21
5.5 Gatekeeper ..... 22
5.6 User Roles ..... 22
5.7 Access Levels ..... 30
5.8 Institutional Access ..... 30
5.9 Redaction ..... 30
5.10 Quality Assurance ..... 31
5.11 Clerk Security ..... 31
5.12 Integrity of the Court Record ..... 31
5.13 Performance ..... 32
5.14 Archival Requirements ..... 32
5.15 Authentication Requirements ..... 32
SECTION 6 COURT APPLICATION PROCESSING SYSTEM ..... 33
6.1 Applicability ..... 33
6.1.1 Certification Required ..... 33
6.1.2 CAPS Definition ..... 33
6.1.3 Exclusion for Clerk's Responsibilities ..... 33
6.1.4 Mandating CAPS ..... 34
6.2 Certification ..... 34
6.2.1 Vendor Product Certification ..... 34
6.2.2 General System Certification ..... 34
6.2.3 Provisional Certification ..... 34
6.2.4 Existing Installations ..... 35
6.2.5 Certification Process ..... 35

6.3 System Design and Performance ..... 35
6.3.1 Performance ..... 35
6.3.2 Robustness ..... 35
6.3.3 Compatibility ..... 35
6.3.4 Adaptability ..... 36
6.3.5 Accessibility and Security ..... 36
6.3.6 External Data Access ..... 37
6.3.7 Global Navigation ..... 37
6.3.8 Hardware Independence ..... 37
6.3.9 Printer-Friendliness ..... 37
6.3.10 Disaster Prevention and Recovery Strategy ..... 37
6.4 Calendaring Function ..... 37
6.4.1 Calendaring System Required ..... 37
6.4.2 Planning Flexibility ..... 37
6.4.3 Calendar Control ..... 37
6.4.4 Replication ..... 38
6.4.5 External User Access ..... 38
6.4.6 Direct Access to Calendar Management ..... 38
6.4.7 Automatic Notation and Notification ..... 38
6.4.8 Calendar Display (Internal) ..... 38
6.4.9 Case Calendar Display ..... 39
6.4.10 Daily Event or Reminder ..... 39
6.4.11 Calendar Export ..... 39
6.5 Search and Display Function ..... 39
6.5.1 Case Search and Display ..... 39
6.5.2 Case Search Keywords ..... 39
6.5.3 Lookup Return ..... 39
6.5.4 Case Information ..... 39
6.5.5 Clerk's Progress Docket ..... 40
6.5.6 Document Image Display ..... 40
6.5.7 Word Search ..... 41
6.5.8 Accessing External Data ..... 41
6.6 Case Management and Reporting ..... 41
6.6.1 Reporting ..... 41

6.6.2 Workflow Management ..... 42
6.6.3 Work Queue ..... 42
6.6.4 Daily Reminder (tickler) ..... 42
6.6.5 Alerts ..... 42
6.6.6 Automated Task for Case Management ..... 43
6.7 E-Notification of Data Issues to the Clerk ..... 43
6.7.1 E-Notification of Data Issues ..... 43
6.8 Order Generation and Processing ..... 43
6.8.1 Order Generation and Processing Required ..... 43
6.8.2 Recallable Entries ..... 43
6.8.3 Portal Integration ..... 44
6.8.4 Document Models ..... 44
6.8.5 Templates ..... 44
6.8.6 Electronic Signatures ..... 44
6.8.7 Electronic Filing and Service ..... 44
6.9 Case Notes ..... 44
6.10 Help ..... 45
SECTION 7 INTEGRATION AND INTEROPERABILITY ..... 46
7.1 Bckground ..... 46
7.2 Requirements and Standards for Integration & Interoperability ..... 46
7.2.1 Diagrams ..... 46
7.3 Integration Requirements and Standards ..... 49
7.3.1 Infrastructure Standards and Requirements ..... 49
7.4 Requirements for Interoperability and Data Exchange ..... 69
7.4.1 Software Applications ..... 69
7.4.2 Data Transmission ..... 70
7.4.3 Database Standards ..... 70
7.4.4 Database Connectivity ..... 70
7.4.5 Archival Storage of Electronic Documents ..... 71
7.5 Cloud Computing ..... 72
7.5.1 Approval Process ..... 72
7.5.2 Risks ..... 72
7.5.3 Storage Restrictions ..... 72
7.5.4 Data Encryption ..... 73

7.5.5 Best Practices ..... 73
7.5.6 Resources ..... 73
SECTION 8 DATA EXCHANGE ..... 74
8.1 Introduction ..... 74
8.2 Governance ..... 75
8.3 Data Exchange Security ..... 75
8.4 Transport ..... 76
8.5 Transfer Framework ..... 77
8.6 Integration Toolkit ..... 78
8.7 Conformance ..... 78
SECTION 9 GENERAL TECHNOLOGY ..... 79
9.1 ADA and Technology Compliance ..... 79
9.2 Redaction and ADA Compliance ..... 79
9.3 Archiving ..... 80
9.4 Archival Requirements ..... 80
9.5 Backup of Electronic Court Records ..... 80
9.6 Court Control of Court Documents – Data Storage ..... 81
9.7 Document Storage Format ..... 81
9.8 Document Workflow and Storage ..... **Error! Bookmark not defined.**
SECTION 10 NOTIFICATION BY CLERK OF SYSTEM MODIFICATION ..... 82
Contact Information ..... 82
Change Information ..... 82
APPENDIX A. SYMBOLS AND ABBREVIATIONS ..... 84
APPENDIX B. NORMATIVE REFERENCES ..... 86
APPENDIX C. TERMS AND DEFINITIONS ..... 88
APPENDIX D. DATA EXCHANGE CONTENT MODELS ..... 94
APPENDIX E. DATA EXCHANGE MESSAGES ..... 95
APPENDIX F. DATA EXCHANGE CAPABILITY MODEL ..... 96

# SECTION 1 PURPOSE

The Florida Courts Technology Standards ("Standards")[1] provide a comprehensive expression of technical and functional standards applicable to Florida's court system. The Standards augment the responsibilities and authority of the Florida Courts Technology Commission ("FCTC") a permanent judicial branch commission charged with overseeing, managing, and directing the development and use of technology within the judicial branch under the direction of the Florida Supreme Court, as specified in Florida Rule of Judicial Administration 2.236.[2]

In creating the FCTC, the Court noted the progress of Florida's court system as moving beyond reliance on paper records to primary reliance on digital information and the use of technology in our courts. Consistent with the judicial branch's long-range strategic plan recognizing the value of information technology to improve court access and operations,[3] these Standards are designed as a dynamic compendium to the Florida Rules of Judicial Administration, but able to be revised and adapted to current technology requirements in the court with greater alacrity through recommendations by the FCTC to the Court.

The FCTC is comprised of members appointed by the Court, and its various workgroups and subcommittees, the specific nature and composition of which are identified on the FCTC's website, which also includes meeting schedules and agendas.

This version of the Standards also consolidates the provisions governing access to court records[4] promulgated by the FCTC's Access Governance Board, which includes the Access Security Matrix.

[1] Formerly known as: Florida Courts E-Filing Portal Standards; Standards for Electronic Access to the Courts; Functional Requirements for Court Application Processing System; Integration and Interoperability Document; Data Exchange Standards; and System Modification.
[2] *In re: Amendments to the Florida Rules of Judicial Administration – Rule 2.236, 41 So. 3d 128 (Fla. 2010).*
[3] *See* JUSTICE; Fair and accessible to All, The Long-Range Strategic Plan for the Florida Judicial Branch (2016-2021).
[4] Formerly known as the Standards for Access to Electronic Court Records.

# SECTION 2 E-FILING STANDARDS

All electronic processes such as pleadings, motions, etc. that involve the judiciary must be approved as defined by Florida Rule of Judicial Administration 2.236(b)(1) before implementation and must comply with the Americans with Disabilities Act ("ADA"). Multiple pleadings, motions, etc. should not be combined into one single file, but rather each document should be uploaded via the Portal document submission process.

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

## 2.1 FILER AND DOCUMENT FILING STANDARDS

### 2.1.1 Electronic Transmission and Filing of Documents

With the establishment of the Florida Courts E-Filing Portal, the Florida Courts have a centralized statewide e-filing system. On June 21, 2012, the Supreme Court issued opinions approving recommendations to require e-filing by attorneys and e-service.

### 2.1.2 Document Filing

The Portal will accept new filings in Word, PDF, and PDF/A formats. The preferred format for filing is the PDF/A format where original document intelligence has been maintained.

Documents filed through the Portal will be provided to the clerk in PDF/A format when the clerk is able to receive and store a PDF/A document as follows:

- Documents filed in an approved PDF/A format will be provided to the clerk as originally filed.
- Documents filed in Word format will be converted to an approved PDF/A format.
- Documents filed in other searchable PDF formats will be converted to an approved PDF/A format.
- Documents filed in other non-searchable PDF formats will be rasterized (i.e., converted into bitmap file format) as an approved PDF/A format.
- Digital signatures and digital notarizations will not be passed or maintained by the Portal.

### 2.1.3 Size of Filing

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

### 2.1.4 Document Creation and Format

#### 2.1.4.1 File Format

Document files should not be saved or converted into formats that remove desirable document intelligence (i.e., files should not be flattened).

#### 2.1.4.2 Document Formatting

All electronically filed documents should be legibly typewritten or printed on only one side of letter-sized (8 ½ by 11 inches) paper; should have one-inch margins on all sides and on all pages and pages should be numbered consecutively; shall 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 11 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.

#### 2.1.4.3 Scanned Documents

Scanned documents should be scanned using Optical Character Recognition ("OCR"). The scanning process should use a minimum resolution of 300 DPI. Documents should be electronically signed as defined in Section 2.1.8, Electronic Signatures.

#### 2.1.4.4 Supported PDF/A Document Intelligence Elements

The following PDF/A document intelligence elements are permitted in documents submitted to the Florida Courts: bookmarks, electronic signatures, attachments created using the Insert feature to append pages to a document, internal links, embedded internal hyperlinks, embedded persistent external hyperlinks, and embedded images. Guidelines for hyperlinks are found in Section 2.1.5.1, Embedded Hyperlinks.

#### 2.1.4.5 Prohibited PDF/A Document Intelligence Elements

The following elements must not be used in PDF/A documents submitted to the Florida Courts: embedded attachments, comments, annotations, hidden deleted items (these should be purged), embedded non-persistent external hyperlinks, embedded thumbnails, for fields and actions, JavaScript, and embedded non-display data. These elements are prohibited because they might be flattened, invalidated, modified, or deleted during the document workflow process.

#### 2.1.4.6 Encryption Prohibited

A compliant PDF/A file must be open and available to anyone or any software that processes the file. User IDs and passwords may not be embedded.

#### 2.1.4.7 Searchable Content

PDF documents filed with the Portal must be searchable. Documents filed in non-searchable PDF format will be rasterized (i.e., converted into bitmap file format) as an approved PDF/A format.

#### 2.1.4.8 Accessibility

Documents filed with the Portal must comply with the accessibility requirements of Fla. R. Jud. Admin. 2.526. Additional ADA requirements can be found in Section 9.1, ADA and Technology Compliance.

Deviation from these guidelines may result in the submitted filing being moved to the Correction Queue by the Clerk with the filer being notified via e-mail and requested to correct the issue(s) with the document(s) and resubmit the filing.

### 2.1.5 Requirements for Individual Filers

#### 2.1.5.1 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. Hyperlinks should not be used to refer to external documents or information sources likely to change.

#### 2.1.5.2 Exhibits

Multiple exhibits can be filed in one submission as long as each exhibit is accompanied by a cover page and does not exceed submission file size. On each cover page, the number of pages should be noted for that exhibit. 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.).

#### 2.1.5.3 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 Fla. R. Jud. Admin. 2.420 regarding confidential information. Your failure to comply with these rules may subject you to sanctions."

### 2.1.6 File Name

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 (~)
- Period (.) The filer should not add an extension. The application will add it automatically.

In addition, file names cannot exceed 150 bytes in length, including spaces. Spaces must be counted as three (3) bytes each.

### 2.1.7 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.

### 2.1.8 Electronic Signatures

#### 2.1.8.1 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, Florida Rules of Judicial Administration. Electronic signature formats of s/, /s or /s/ are acceptable.

**Attorney Example**
s/ John Doe
Bar Number 12345
123 South Street
City, FL 12345
Telephone: (123) 123-4567
E-mail Address

**Self-Represented Example**
s/ Jane Doe
123 North Street
City, FL 12345
Telephone: (123) 123-4567
E-mail Address

#### 2.1.8.2 Multiple Attorneys of Record Signatures

When a filing requires the signature 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.

#### 2.1.8.3 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.

#### 2.1.8.3.1 Security

An electronic signature of a judge shall be accompanied by a date, timestamp, 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.

#### 2.1.8.3.2 Functionality

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

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

#### 2.1.8.3.3 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's signature under standard 2.1.8.3.

## 2.2 PORTAL FUNCTIONALITY

### 2.2.1 Minimum Functionality

- Single statewide login.
- Single Portal for attorneys as mandated per administrative order.
- Process for non-attorneys and self-represented users to access the system (e.g., state agencies, local agencies, law enforcement, mediators, process servers, etc.).
- Uniform authentication method.
- Single point of access for filing and service.
- Consolidated electronic notification.
- Process for local validation.
- Automated interface with other e-filing systems as outlined in Portal documentation.
- Utilize the approved XML ECF Standards.
- Accommodate bi-directional transmissions to and from courts.

- Integrate with other established statewide systems.
- Accept electronic forms of payment.
- All court-based e-filing processes will use Internet-based open standards.

### 2.2.2 Electronic Filing Envelope

The Portal shall generate an electronic filing envelope for each submission. The e-filing envelope must comply with current rules of procedure and with e-filing envelope requirements established by the FCTC for each division and court type. These requirements can be found at http://www.flcourts.org/resources-and-services/court-technology/efiling/.

The e-filing envelope shall be in .XML format and contain the data elements needed to support the filing, indexing, docketing, calendaring, accounting, reporting, document development, case management, case maintenance, and other necessary functions of the court. The Portal shall prompt the filer for all relevant information, identifying each data element as required or optional.

### 2.2.3 Portal 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. Timestamps must be formatted in 12-hour time frames with a.m. or p.m. included.

The Portal's official file stamp date and time shall be affixed in the upper left-hand corner in Eastern Time. 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 at the bottom of the document.

### 2.2.4 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.

### 2.2.5 Review by Clerk of Court

When information has been submitted electronically to the Clerk of Court's Office, via the 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 correction queue. A filing may be placed in a correction queue for any reason that prevents the filing from being accepted into the clerk's case maintenance system

("CMS"), e.g., documents that cannot be associated with a pending case; a corrupt file[5]; or an incorrect filing fee.

Once placed in a correction queue, the clerk shall attempt to contact the filer using the filer's registered e-mail address and ask the filer to correct the identified issue(s) and resubmit. If not corrected, the filing will remain in a correction queue for no more than 5 (five) business days, after which time the filing will be moved to the abandoned filing queue.

### 2.2.6 Docket Numbering

The sequence numbers will not be included in the interface between the Portal and the local clerk CMS and will not be provided to the filer as part of the e-filing notification process.

### 2.2.7 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.

### 2.2.8 Filing Process

The Portal shall support both a single session filing process and a system-to-system process.

### 2.2.9 Submission Validation

The Portal shall validate each submission to detect any discrepancies (e.g., incomplete data or unacceptable document type) or other problems (e.g., viruses) before transmission to the clerk of court. The Portal will return a submission to the correction queue if a virus is detected within the submission or if one or more of the documents in the submission is corrupt. The Portal will e-mail the filer 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).

### 2.2.10 Adding a Party

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

### 2.2.11 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

[5] Document(s) that cannot be opened or read

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 Fla. R. Jud. Admin. 2.420 regarding confidential information. Your failure to comply with these rules may subject you to sanctions."

### 2.2.12 Emergency Filing

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

### 2.2.13 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 FCTC.

#### 2.2.13.1 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.

#### 2.2.13.2 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.

### 2.2.14 Document Filing

The Portal will accept new filings in Word, PDF, and PDF/A formats. The preferred format for filing is the PDF/A format where original document intelligence has been maintained.

Documents filed through the Portal will be provided to the clerk in PDF/A format when the clerk is able to receive and store a PDF/A document as follows:

- Documents filed in an approved PDF/A format will be provided to the clerk as originally filed.
- Documents filed in Word format will be converted to an approved PDF/A format.
- Documents filed in other searchable PDF formats will be converted to an approved PDF/A format.
- Documents filed in other non-searchable PDF formats will be rasterized (i.e., converted into bitmap file format) as an approved PDF/A format.
- Digital signatures and digital notarizations will not be passed or maintained by the Portal.

### 2.2.15 Electronic Notarization

Electronic notarization is authorized as provided in Florida Statute 117.021.

Note, electronic notarizations may be flattened, and the certificate invalidated as the document moves through the filing process.

# SECTION 3 ELECTRONIC COURT RECORDS CUSTODIAN STANDARDS

Electronic court records custodians are responsible for the storage, processing, security, availability, accessibility, and integrity of electronic court records (i.e., images and data) under their care.

These standards are minimum standards. If a custodian stores court-related data from another jurisdiction or agency with stricter requirements, the custodian must comply with the stricter standards for that data.

## 3.1 COURT DOCUMENT FORMAT

Custodians shall ensure that:

- Electronic documents that are part of a court file (i.e., the record copy) are stored in the PDF/A format.
- This is a day-forward standard.
- Upon implementation of the PDF/A standard for incoming filings, existing electronic documents may remain in their current format(s) if the clerk's CMS is capable of managing multiple file formats.
- The record copy of each electronic court document retains the original document intelligence (i.e., as filed with the Portal) except features that use a digital hash. For example, digital signatures and electronic notarizations may be flattened and the certificates invalidated as the document moves through the filing process.

## 3.2 ADA COMPLIANCE

Custodians of electronic court documents are not responsible for adding ADA-compliance features to documents that they did not originate. However, custodians are required to follow acceptable ADA practices for access to court documents.

## 3.3 COURT RECORDS REDACTION

Custodians shall ensure that confidential information contained within a court record is redacted before release or review of the record as defined by Fla. R. Jud. Admin. 2.420. Redaction software that identifies confidential information may be used; however, a manual process must also exist to identify confidential information that may not be readily identified by an automated redaction process or for case types/documents that are available upon request.

Redacted copies of electronic court documents are not required to retain the original document intelligence. These copies may be flattened to accommodate existing redaction workflow processes.

## 3.4 COURT RECORDS STORAGE

Custodians shall ensure that:

- All court data under their care is stored in the United States. This includes the record copy and all backup and archival copies.
- The production data or backup copy will reside in a hardened (CAT 5) facility. If a hardened (CAT 5) facility is unavailable, a tertiary copy (redundant backup) will also be maintained in its own off-site, independent facility. The production electronic court records and at least one copy of the backup(s) shall not be housed in the same building.
- Agreements with third-party vendors for Cloud or offsite copies acknowledge the confidentiality of electronic court data they store and prohibit data mining and other access/use of the data for any purpose other than to make the data accessible to the custodian.
- All copies of court data must be readily available to the custodian.
- Any known breach, or other malicious events, is reported to the chief judge or his/her designee and the Chief Information Security Officer at the Office of the State Courts Administrator Office of Information Technology as part of the custodian's Computer Security Incident Response plan.
- Physical and electronic data transfer processes conform to the confidentiality and security guidelines outlined in Section 8, Data Exchange.

## 3.5 COURT RECORDS BACKUP AND ARCHIVAL

Custodians shall ensure that:

- Electronic court records in their care are securely backed-up and any backup data stored at a third-party location must also be encrypted. The custodian of the electronic court records shall have exclusive access to the encryption key. In instances where vendors are supporting appliances onsite and are required to maintain an encryption key, the custodian will have operational policies and procedures that serve as a control prohibiting vendor access without invitation and monitoring.
- Random sample testing is performed annually to verify that backup data is accessible and recoverable.
- Archival copies are created 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.

# SECTION 4 CLERKS CASE MAINTENANCE SYSTEM STANDARDS

## 4.1 CMS STANDARDS

### 4.1.1 Document Rendering

The clerk must render document images in searchable PDF/A format for viewer interfaces where the Court Application Processing System ("CAPS") does not already provide searchable documents.

### 4.1.2 Electronic Filing Envelope

The Portal shall generate an electronic filing envelope for each submission. The e-filing envelope must comply with current rules of procedure and with e-filing envelope requirements established by the Florida Courts Technology Commission ("FCTC") for each division and court type. These requirements can be found at http://www.flcourts.org/resources-and-services/court-technology/efiling/.

The e-filing envelope shall be in .XML format and contain the data elements needed to support the filing, indexing, docketing, calendaring, accounting, reporting, document development, case management, case maintenance, and other necessary functions of the court. The Portal shall prompt the filer for all relevant information, identifying each data element as required or optional.

### 4.1.3 Clerk's 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. Timestamps must be formatted in 12-hour time frames with a.m. or p.m. included.

The Portal's official file stamp date and time shall be affixed in the upper left-hand corner in Eastern Time. 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 at the bottom of the document.

### 4.1.4 Docket Numbering

- At a minimum, the local clerk CMS shall assign and store a sequential document identification number or DIN for each docket entry on each case that contains a document. The document identification number will be unique only within each case. For example, each case will start with 1, 2, 3, etc., and increment by 1.
- The document identification number shall be stamped on each document and shall be displayed on each document/docket display screen in the local clerk CMS, the court application processing systems, and other court record access systems.
- Each assigned document identification number shall remain static for each case once assigned. If documents/dockets are inserted, then the sequence numbers will not

necessarily align with the dates for the documents/docket. As long as they are unique within each case this is allowed.

- The document identification number may be implemented on a "go-forward" basis if necessary; document identification numbers are not required for historical documents/dockets.
- The document identification numbers are only assigned and stored in the local clerk CMS. The document identification numbers are not provided to the filer as part of the e-filing notification process, at this time.
- This requirement does not apply to legacy CMS applications that have a known end date.

# SECTION 5 ACCESS TO ELECTRONIC COURT RECORDS

## 5.1 PURPOSE AND SCOPE

These standards establish statewide technical and operational requirements for access to electronic court records by the public, special user groups, judges, and court and clerk's office personnel. These standards also implement the Access Security Matrix ("Matrix"), which governs remote web-based and clerks' office access to electronic court records.

## 5.2 ACCESS METHODS

There are three different methods for accessing electronic court records:

1. Direct access via application to internal live data;
2. Web-based application for replicated or live data with security; and
3. Web-based portal for public viewing of replicated data and variable levels of security based on user role.

Direct or web-based access to live production data is generally limited to authorized court and clerk's office personnel. Most users will access replicated data to protect the integrity and availability of the official court record maintained by the clerk.

## 5.3 ACCESS SECURITY MATRIX

The Access Security Matrix governs access to electronic court records based upon user roles and applicable court rules, statutes, and administrative policies. The Matrix performs the following functions:

1. Establishes user groups;
2. Establishes access levels; and
3. Assigns access level for each user group based on case type.

The Access Governance Board ("the Board"), under the authority of the Florida Courts Technology Commission ("FCTC"), is responsible for maintaining the Matrix by timely incorporating legislative and rule changes that impact access to electronic court records. Access permitted under the Matrix applies equally to electronic and paper court records.

## 5.4 USER AGREEMENTS

The FCTC, in conjunction with the clerks, must develop and maintain agreements clearly defining responsibilities for user access.

Clerks may use an online agreement, instead of a paper agreement, that requires users to agree to terms using an online click-through (for example, clicking on the "I AGREE" button, as with other online term agreements) as long as the agreement terms are versioned so that updates can be tracked. When agreement terms change, users are required to accept the new terms, either electronically or in paper. A notarized agreement is required for each user role, except for the Registered User role as defined by the Matrix. User agreements submitted in paper shall be retained by the clerk.

## 5.5 GATEKEEPER

In an effort to effectively manage access and ensure security, an agency may utilize one or more gatekeepers or a designee authorized by an agency head or an authorized gatekeeper who shall be an employee of that agency, for the purpose of adding, updating, and deleting user or agency information. A gatekeeper shall only add users commensurate with an agency's user role type and/or as registered users. Each agency shall be responsible for ensuring that each user added by the gatekeeper is only given access that is commensurate to their job duties. Nothing in this definition shall nullify any other duties imposed upon the gatekeeper by the Board.

## 5.6 USER ROLES

Access to electronic court records is determined by the user's role and applicable statutes, court rules, and applicable administrative policy. Access may be restricted to certain user roles based on case type, document type, or information contained within court records. All individuals and entities authorized under these standards to have greater access than the general public must establish policies to protect confidential records and information in accordance with applicable court rules and statutory requirements. Remote electronic access may be more restrictive than in-person in-house electronic access at clerks' offices.

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| **User Role 1**<br>Judges and authorized court and clerk's office personnel | All court records, except those expunged under §943.0585, F.S., with discretionary limits based on local security policy. Each court and clerk must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties.<br><br>Access to records sealed under §943.059(4), F.S., is permitted for judges to assist in the performance of case-related adjudicatory responsibilities. | In-house secure network and secure web access. |

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| **User Role 2**<br>Florida State Attorneys' Offices and the Office of Statewide Prosecution | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order.<br><br>Access to Social Security numbers by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S.<br><br>Access to HIV test results as permitted by §381.004(5)(c), F.S.<br><br>Access to sexually transmitted disease results as permitted by §384.29(1), F.S.<br><br>Access to birth certificates as permitted by §§382.013)5) and 382.025(1)(a)5, F.S.<br><br>Access to mental health records as permitted by §§394.4615(3)(b) and 394.4655(3)(4)(c), F.S.<br><br>Access to identities of victims of sexual and child abuse when originating from law enforcement as permitted by §119.0714(1)(h), F.S.<br><br>Access to children and families in need of services records as permitted by §984.06(3), F.S.<br><br>Access to juvenile records as permitted by ss. 39.0132(4)(a)(1) and 985.04(1)(b), F.S. | Secure access through username and password by written notarized agreement. The agency gatekeeper is responsible for maintaining an authorized list of users.<br><br>Each state attorney must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties. |

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| **User Role 3**<br>Attorneys of record | All records except those that are expunged or sealed; access may be denied to records or information automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order, depending upon the type of case and the language of the court order. Access will be changed to Registered User when the attorney's appearance is terminated under rule 2.505, Fla. R. Jud. Admin. | Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining an authorized list of users. |
| **User Role 4**<br>Parties | All records in the party's case except those that are expunged or sealed; access may be denied to information automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin. or made confidential by court order, depending upon case type and the language of the order. | Secure access on a case-by-case basis. Access by notarized request to ensure the identity of a party. |
| **User Role 5**<br>Public in Clerks' offices and registered users | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin. or made confidential by court order.<br><br>Viewable on request remote access to images of records in cases governed by the Florida Family Law Rules of Procedure, Florida Rules of Juvenile Procedure, or Florida Probate Rules, under §28.2221(5)(a), F.S. | Secure access through username and password or in person at Clerks' offices. |

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| **User Role 6**<br>General government and constitutional officers | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order.<br><br>Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. | Secure access through username and password by written notarized agreement. The agency gatekeeper is responsible for maintaining an authorized list of users.<br><br>Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties. |
| **User Role 7**<br>General public (without registration agreement) | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order.<br><br>No remote access to images of records in cases governed by the Florida Family Law Rules of Procedure, Florida Rules of Juvenile Procedure, or Florida Probate Rules, under §28.2221(5)(a), F.S. | None. Anonymous web-based access permitted. |
| **User Role 8**<br>Certified law enforcement officers of federal and Florida state and local law enforcement agencies, Florida Department of Corrections, and their authorized users | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order.<br><br>Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S.<br><br>Access to HIV test results as permitted by §§381.004(2)(e) and 951.27, F.S. | Secure access through username and password by written notarized agreement. The agency gatekeeper is responsible for maintaining an authorized list of users.<br><br>Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties. |

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| | Access to sexually transmitted disease results as permitted by §384.29(1), F.S.<br><br>Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S.<br><br>Access to identities of victims of sexual and child abuse when originating from law enforcement as permitted by §119.0714(1)(h), F.S.<br><br>Access to children and families in need of services records as permitted by §984.06(3), F.S.<br><br>Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S. | |
| **User Role 9**<br>Florida Attorney General's Office and the Florida Department of Children and Families | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order.<br><br>Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S.<br><br>Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S.<br><br>Access to children and families in need of services records as permitted by §984.06(3), F.S. | Secure access through username and password by written notarized agreement. The agency gatekeeper is responsible for maintaining an authorized list of users.<br><br>Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties. |

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| | Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S. | |
| **User Role 10**<br>Florida School Districts (Truancy) | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order.<br><br>Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S.<br><br>Access to juvenile delinquency records as permitted by §985.04(1)(b), F.S. | |
| **User Role 11**<br>Commercial purchasers of bulk records. | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order.<br><br>No remote access to images of records in cases governed by the Florida Family Law Rules of Procedure, Florida Rules of Juvenile Procedure, or Florida Probate Rules, under §28.2221(5)(a), F.S. | Secure access through username and password by written notarized agreement. The commercial purchaser gatekeeper is responsible for maintaining an authorized user list. |

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| **User Role 12**<br>Office of the Public Defender (institutional access only) | All records except those that are expunged or sealed; access may be denied to records or information automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order, depending upon the type of case and the language of the court order.<br><br>The Office of the Public Defender is considered the attorney of record at a defendant's first appearance as permitted by §985.045(2) and rules 8.010 and 8.165, Florida Rules of Juvenile Procedure for juvenile defendants and §27.51 and rule 3.130, Fla. R. Crim. P. for adult defendants.<br><br>Access will be changed to User Role 6 when the public defender is no longer the attorney of record or another attorney is assigned. | Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining an authorized list of users.<br><br>Each public defender must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties. |
| **User Role 13**<br>Office of Criminal Conflict and Civil Regional Counsel (Institutional Access only) | All records except those that are expunged or sealed; access may be denied to records or information automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order, depending upon the type of case and the language of the court order.<br><br>The Office of Criminal Conflict and Civil Regional Counsel (OCCCRC) is | Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining an authorized list of users.<br><br>Each regional counsel must establish written policies to ensure that access to confidential records and information is limited to those individuals who require access in |

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| | considered the attorney of record at a party's first appearance in civil proceedings listed in §27.511(6), F.S., and in criminal proceedings is entitled to appointment as attorney of record upon the Public Defender's declaration of conflict in case types listed in §27.511(5), F.S.<br><br>Access will be changed to User Role 6 when the OCCCRC is no longer the attorney of record or another attorney is assigned. | performance of their official duties. |
| **User Role 14**<br>Statewide Guardian ad Litem Office | All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), Fla. R. Jud. Admin., or made confidential by court order.<br><br>Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S.<br><br>Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S.<br><br>Access to children and families in need of services records as permitted by §984.06(3), F.S.<br><br>Access to juvenile records as permitted by §§ 39.0132(4)(a)(1) and 985.04(1)(b), F.S. | Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining an authorized list of users.<br><br>Each guardian ad litem must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in the performance of their official duties. |

| MATRIX USER ROLES | ACCESS PERMITTED | USER SECURITY REQUIREMENTS |
|---|---|---|
| | Access for guardian ad litem appointed as permitted by §39.822, F.S. | |

## 5.7 ACCESS LEVELS

Access levels are defined as follows:

A. All but expunged, or sealed under Ch. 943, F.S.;
B. All but expunged, or sealed under Ch. 943, F.S., or sealed under rule 2.420, Fla. R. Jud. Admin.;
C. All but expunged, or sealed under Ch. 943, F.S. and sealed under rule 2.420, Fla. R. Jud. Admin., or confidential;
D. All but expunged, sealed, or confidential; record images viewable upon request;
E. Case number, party names, dockets only;
F. Case number and party names only;
G. Case number only; and
H. No access.

Viewable on request access level applies to documents containing confidential information that must be redacted; this access level requires examination of the case file by a clerk to identify and redact confidential information before the record can be viewed.

## 5.8 INSTITUTIONAL ACCESS

Institutional Access applies to roles of the Office of Public Defender and the Office of Criminal Conflict and Civil Regional Counsel in cases where they are appointed or are the presumptive attorney of record. The term "institution" as used within these standards means a statutorily-created organization or agency responsible for providing legal representation to an individual or group of individuals. This designation allows institutional users - including paralegals, legal assistants, and other staff - to view assigned cases as if they were the "attorney of record." Once an institution ceases representation in a case, access is severed and the institution's users default to the General Government user role.

## 5.9 REDACTION

Redaction is the process of obscuring confidential information contained within a public record from view. Redacted portions of a record are blacked out. Redaction may be accomplished manually or through the use of technology such as redaction software. Redaction software is used when information is in electronic form. If redaction software is used, it must identify and

protect confidential information through redaction of confidential content. For efficiency, redaction software is preferred over manual processes when the files are in electronic form.

There are generally two levels of redaction:

- Level 1 -The system reads the images and uses the knowledge base to auto-redact suspect regions
- Level 2 -Redacted images are presented to a first reviewer to accept or decline to redact selected data on the image

Redaction software that identifies confidential information may not be used; however, a manual process must also exist to identify confidential information that may not be readily identified by an auto redaction process or for case types/documents that are available upon request.

## 5.10 QUALITY ASSURANCE

Clerks must employ redaction processes through human review, the use of redaction software, or a combination of both. Clerks must audit the process adopted at least annually for quality assurance and must incorporate into their processes new legislation or court rules relating to the protection of confidential information. It is recommended that clerks advise commercial purchasers that court records are regularly updated and encourage the use of updated records.

## 5.11 CLERK SECURITY

No sensitive security information should be presented on the user interface. Sensitive data shall be exchanged over trusted paths or by using adequate encryption between users; between users and systems; and between systems. The system must employ appropriate security and encryption measures to prevent the disclosure of confidential data to unauthorized persons.

Minimum Technical Requirements:

1. Encryption (general public and authenticated)**;
2. No “cutting and pasting” of workable links;
3. Hyperlinks must not include authentication credentials
4. No access to live data; replicated records will be used for public access;
5. Authenticated access for access beyond general public access; and
6. Monitor bulk data transfers to identify and mitigate abuses of the system by utilizing access programs using automated methods.

**Encryption protects the integrity of the record and prevents exposure to potential security risks. It also prevents authenticated users with higher access from sending links to information to non-authorized users.

## 5.12 INTEGRITY OF THE COURT RECORD

To protect the integrity and availability of the court record, public access will not be to the original record, but to a replicated version that is redacted, if applicable.

Online links shall be encrypted to prevent return access to a URL via "cutting and pasting". Link refresh times shall appropriately time out as determined by each clerk, but links shall refresh no less than one every 30 minutes.

## 5.13 PERFORMANCE

Search parameters for web-based access to electronic records will be limited to the following:

A. User Role 7 (General Public)
    1. Case type;
    2. Case number;
    3. Party name;
    4. Citation number; and
    5. Date range.

B. Authenticated users may have more robust search features than public users.

Non-confidential data or data accessed by an authenticated user may be viewed immediately. Some images may be "viewable upon request" to allow time for the redaction process.

Online access to documents stored as images may be provided. Documents stored as images are "view only." If a requested document is maintained by the clerk in a searchable format, the document may be provided to the public in that format, but only in response to a specific request. Search capability, if available, will be limited to such requested document and must not support automated bulk searches.

Only authorized automated search programs, to be used solely on the indices, shall be used with the court's electronic public access system. Automated search programs may not be used on any other component of the court's electronic public access system. The court and clerk will determine the criteria for authorization of any automated search programs. Such authorization may be revoked or modified at the discretion of the court and clerk.

## 5.14 ARCHIVAL REQUIREMENTS

Electronic records must be archived in a manner that protects the records from degradation, loss of content, or problems with software compatibility relative to the proper rendering of electronic records and in compliance with applicable law or Supreme Court guidelines.

## 5.15 AUTHENTICATION REQUIREMENTS

Members of the general public do not require a username or password to access information that is generally available to the public. For information that is accessible to individuals or entities beyond general public access, users must be authenticated to verify their role and associated access levels. Users must subscribe to the access system and provide information to verify their identity. Users are then assigned a login account. At a minimum, users accessing records and information beyond general public access must have a username and password and have the ability to change their password using self-service within the web-based application.

# SECTION 6 COURT APPLICATION PROCESSING SYSTEM

The Florida Courts Technology Commission ("FCTC"), upon motion of its Certification Subcommittee, adopts this Functional Requirements Document ("FRD") to provide specifications for Court Application Processing Systems ("CAPS") to coordinate the use of information technology and electronic case files, in court and in chambers, by trial court judges and staff. In addition to the functional requirements outlined in this document, systems must comply with applicable Rules of Judicial Administration, and other technical and functional standards established by the Court that may apply to CAPS.

## 6.1 APPLICABILITY

### 6.1.1 Certification Required

Any system meeting the definition of CAPS in this section must be certified under Section 6.2, Certification below before being deployed, renewed, or substantially modified. Each circuit determines which certified system best meets its needs. The chief judge's approval shall be required before the purchasing or upgrading of any system.

**6.1.1.1**

Certification may only be granted when a product or combination of products meets or exceeds the functional standards specified in this document unless excluded.

**6.1.1.2**

The system shall meet the general criteria of 6.3 and perform each of the following functions, as specified in the sections cited, and be accessible in a seamless program via a single log on:

- Calendar (6.4);
- Search (6.5);
- Case Management and Reporting (6.6);
- E-Notification of Data Issues (6.7);
- Orders (6.8);
- Case Notes (6.9); and
- Help (6.10).

### 6.1.2 CAPS Definition

CAPS is defined as a computer application designed for in-court and in-chambers use by trial judges, their staff, and Court Administration personnel to access and use electronic case files and other data sources in the course of managing cases, scheduling and conducting hearings, adjudicating disputed issues, and recording and reporting judicial activity.

### 6.1.3 Exclusion for Clerk's Responsibilities

The FCTC recognizes that existing law establishes the clerks as the official custodians of court records. Systems built and maintained by clerks of court and limited to their historical functions are excluded from this definition. Specifically, general-purpose files, indexes, or document viewers made available by the clerk to users other than the judiciary and in-court participants are not subject to the functional requirements of this document, although they remain subject to all other FCTC policies and requirements, including but not limited to the

Integration and Operability standards and all other requirements set forth by the Supreme Court. This standard does require the clerks of court to make their official court files available to the CAPS in read-only fashion in real-time or from a replication delayed no more than five minutes from real-time.

### 6.1.4 Mandating CAPS

A CAPS shall be made available to the trial courts of this state, in every division, county, and circuit. The CAPS shall accept and display case information from the clerk's CMS in form and function consistent with these functional requirements.

## 6.2 CERTIFICATION

### 6.2.1 Vendor Product Certification

A product offered by a single commercial vendor must be certified by the FCTC under this section before the vendor may sell or otherwise deploy a new installation, or renew a contract for an existing installation, as meeting the definition of CAPS in Section 6.1.2. When a vendor obtains certification for a product, the State Courts Administrator is authorized to enter into such agreements as she deems advisable to facilitate transactions between such vendor and any trial court unit that chooses to purchase the certified product.

### 6.2.2 General System Certification

Any CAPS product or system that is not subject to the vendor product certification section requires general system certification before a new installation or deployment. General system certification can be granted for:

**6.2.2.1**
Internally developed systems that comply with the functional requirements of this document; or

**6.2.2.2**
Aggregated systems, consisting of components that individually may not meet the functional requirements but taken together do satisfy the requirements.

### 6.2.3 Provisional Certification

Provisional certification is for six months and may be renewed at the discretion of the FCTC. It may be granted for:

**6.2.3.1**
Partial systems or subsystems that meet only a part of the standards when a plan for attaining certification within a reasonable time has been approved by the FCTC;

**6.2.3.2**
Systems that lack specific data reporting requirements because the local clerk's office does not maintain that data and it is not otherwise reasonably available from machine-readable sources; or

**6.2.3.3**
Any other partially compliant subsystem. Approval will be on a case by case basis under the procedures outlined in Section 6.2.5.

### 6.2.4 Existing Installations

An existing system requires certification upon the earliest of the following events:

**6.2.4.1**
Substantial modification of the system; or

**6.2.4.2**
Expiration of the contracts under which any vendor provides the system or a subsystem.

### 6.2.5 Certification Process

The certifying entity is the FCTC. The FCTC delegates its authority to make initial certification determinations to the State Courts Administrator.

**6.2.5.1**
Administrative Decision. The State Courts Administrator shall issue certification, or a notice that certification has been denied, within a reasonable time. Unless an interested party files a written application for review within thirty days of the Administrator's decision, that decision will constitute the final decision of the FCTC.

**6.2.5.2**
Review and Final Action. Review of any disputed certification decision by the administrator is conducted by a subcommittee of the FCTC appointed by its Chair for that purpose. The subcommittee's decision shall constitute final action unless, within 30 days of its rendition, the FCTC adopts a resolution accepting review of the certification decision.

## 6.3 SYSTEM DESIGN AND PERFORMANCE

### 6.3.1 Performance

The system must meet or exceed the efficiencies delivered by conventional paper systems or previous electronic systems.

### 6.3.2 Robustness

The system must be engineered so that it does not break down upon foreseeable peaks of usage, user error, data corruption, or other stress. The system's design must provide redundancy to eliminate a single point of hardware failure from interrupting CAPS availability to the Court users.

### 6.3.3 Compatibility

The system must be adaptable at a reasonable cost to be compatible and interoperable with any of the clerk's systems being used in the state. It must use, to the extent feasible, industry-standard document formats and transmission protocols, and avoid all use of proprietary formats, data structures, or protocols.

### 6.3.4 Adaptability

The system must be designed in a way that anticipates obsolescence of hardware and software and is upgradeable and modifiable as new technologies become available or statutes, rules, or court procedures change. In particular, the system must be able to accommodate, at a reasonable expense, additional data elements for specific divisions of court as adopted by the FCTC.

### 6.3.5 Accessibility and Security

The system must prevent access by unauthorized persons and facilitate access by authorized persons according to a defined set of user permission levels. The system must be usable by judges, and also by judicial assistants, clerks, and case managers as the judge may direct.

**6.3.5.1**
Security. The system must comply with industry-standard security methods, including encryption and authentication protocols, to protect access to the application and associated data.

**6.3.5.2**
User Permission Levels.

- System-assigned User Permission Levels. The system shall provide the system administrator with the ability to configure user permissions to restrict access to the application, sub-applications (functions), and case data (as needed to comply with statutory restrictions on access to case data).
- The system shall provide a means for a judge to manage which other authenticated individual users or judge-defined user groups may view or change case-related information he originates, such as notes, document annotations, contents of work folders, case management information, and personal and system calendar entries.

**6.3.5.3**
Password Protection. The system must authenticate users and their permission levels based on username and password, providing access to all functional modules using the same credentials.

**6.3.5.4**
Electronic Signatures. The system must ensure that electronic signatures may be applied to orders only by the authenticated user.

**6.3.5.5**
Remote Access. The system must be accessible remotely via the web by judges and other
personnel having appropriate permission levels.

**6.3.5.6**
Persons with Disabilities. The system must comply with Section 508 of the Rehabilitation Act of 1973 (as amended), which lists standards necessary to make electronic and information technology accessible to persons with disabilities.

### 6.3.6 External Data Access

The system must allow access to the database(s) of the clerk(s) in the circuit to avoid any unnecessary re-keying of data by court personnel. It must be able to retrieve basic case information, any scheduling or calendaring information the clerk may maintain, the clerk's progress docket, and the set of electronic documents that constitute the official court file.

### 6.3.7 Global Navigation

Each top-level module of 6.1.1.2 shall be accessible from any non-modal screen in the application by clicking once on a global navigation menu.

### 6.3.8 Hardware Independence

The system must be reasonably hardware-independent and must work with a touch screen, mouse or other pointing devices, or keyboard entry.

### 6.3.9 Printer-Friendliness

All displays of case data or document images shall be printable, using either a screen print function or a developed printer-friendly routine. When a document is being displayed, the court shall have the option to print one or more pages at once.

### 6.3.10 Disaster Prevention and Recovery Strategy

The system must use reasonable measures to prevent service interruption and have a plan for the continuation of operations if an interruption occurs. It must be designed to minimize the risk of data loss, including but not limited to secure, regular, and redundant data backup.

## 6.4 CALENDARING FUNCTION

### 6.4.1 Calendaring System Required

A system must include a planning and calendaring function that permits the court to allocate blocks of future time for specific purposes, that permits the court or authorized other persons to book specific hearings or other events into allocated time, and that displays or prints the schedule for a day, week, or month with the appropriate level of detail. Each schedulable block and event must also be able to be canceled by an authorized person as determined by the presiding judge/magistrate.

### 6.4.2 Planning Flexibility

The system must accommodate docket planning using either time-certain or multiple-case-docket approaches, or such other approach as the court may specify. It must permit the court to specify the capacity of any multiple case docket and displays must be able to show the portion of capacity remaining.

### 6.4.3 Calendar Control

The calendaring system must prevent a user from inadvertent double booking a hearing for the same time slot that is not a mass docket or intentionally double booked. It must also prevent booking a multiple case docket in excess of its capacity unless the user deliberately overrides the capacity.

### 6.4.4 Replication

The system must permit the court to allocate blocks of time on a recurrent basis (e. g. every other Thursday or every fifth Friday) with minimum data entry. It must also be able to call up a list of cases based on defined criteria and schedule or reschedule all of the cases simultaneously into a new time block.

### 6.4.5 External User Access

The system must be capable of displaying allocated time blocks to external users such as attorneys or parties as the judge may direct and must also provide a means by which the external users can either request to book a hearing into an allocated time block, or automatically and directly book a hearing into an allocated time block, as the judge may direct.

### 6.4.6 Direct Access to Calendar Management

The calendar display screens must provide direct access to functions by which a judge, judicial assistant, or case manager can directly and immediately manage the court's calendar with minimal click count, including set, re-set, continue, or cancel hearings or trials; and add a case to or remove a case from a docket.

### 6.4.7 Automatic Notation and Notification

The system shall, as directed by the judge, create immediate automatic e-mail alerts to parties, or paper copies and envelopes to parties without an e-mail address, attorneys, clerks, case managers, court staff, whenever a calendared event is changed on a calendar by a judge, judicial assistant, or case manager.

### 6.4.8 Calendar Display (Internal)

The calendaring system shall contain a general-purpose calendar viewing function for internal users that displays allocated time blocks, any appointments scheduled within those blocks, and any unallocated time as the user may select.

**6.4.8.1**
The displayable fields shall be at least: hearing type; case type; case name; case number; date; time; judge; parties; attorneys; location (court and hearing rooms) and case age.

**6.4.8.2**
The fields displayed shall be limited appropriately by the user's permission level. The display must have the ability to sort and filter by any displayed field.

**6.4.8.3**
When a specific appointment is listed on the display, clicking on the time and date portion shall call a function that permits editing, canceling, or rescheduling the event without retyping identifying information. Clicking on the case name will bring up a case calendar display (Section 6.4.9). There shall also be a control that opens the progress docket (Section 6.5.5).

**6.4.8.4**
When an allocated but still available time block, or any portion of unallocated time, is listed on the display, clicking on it shall call a function that permits entry of a new matter into that time block.

### 6.4.9 Case Calendar Display

The system shall have the ability to list all events (past and future) scheduled in a specific case.

### 6.4.10 Daily Event or Reminder

The calendaring function must support the daily reminder function of the case management module 6.6.4 by accepting items posted to a specific date without a specified time, for use as a reminder or tickler system.

### 6.4.11 Calendar Export

The system must be able to export calendaring information in industry-standard formats (e.g., iCalendar and Outlook).

## 6.5 SEARCH AND DISPLAY FUNCTION

### 6.5.1 Case Search and Display

The system must be able to retrieve and display basic case information from the clerk's database and from any internal database it maintains. Basic case information includes at a minimum: case style (parties names, case number, and division of court); type of case; date opened; current status; identities, roles, and contact information of parties and attorneys.

### 6.5.2 Case Search Keywords

The system must be able to search for cases by case number, party name, party role, case filing date or date range, case type, or a combination of these fields.

### 6.5.3 Lookup Return

The result of a lookup function must return either a list of cases meeting the search criteria, a Basic Case Information display screen if only one match was found or a notification that no cases were found.

### 6.5.4 Case Information

A Case Information display must contain at least:

**6.5.4.1**
Basic Case Information and appropriate subsets of the events scheduled in the case and of the clerk's progress docket.

**6.5.4.2**
Controls that call:

- the full progress docket;

- display of detailed information including a search for related cases on a party, attorney, witness, or another participant;
- an e-mail window pre-addressed to all the parties or attorneys in the case;
- a button that opens the scheduling function (and remembers the current case);
- a control that opens the list of orders that the system can generate; and
- a search window permitting single word and multiple word searches of the searchable electronically filed documents in the case, returning a subset of the progress docket containing the search terms.

### 6.5.5 Clerk's Progress Docket

The clerk's progress docket is a list of the documents in the official court file for the case. It is the most common entry point for the display of the contents of the court file. The court application must display the docket sequence number for each docket entry in the progress docket.

**6.5.5.1**
Each electronically filed document listed on the progress docket must have a link or button that immediately opens the document for viewing. It must be able to retrieve and display the documents and associated sequence number without unnecessary delay.

**6.5.5.2**
The progress docket must list the documents filed in the case in such a way as to readily distinguish, via icons or color-coding, electronically field documents from those which have been filed in paper form and not converted.

**6.5.5.3**
Orders must similarly be distinguished from motions and other filings.

**6.5.5.4**
There must be a word search function for the progress docket.

### 6.5.6 Document Image Display

The system must display multiple documents from the clerk's official court files consistent with time standards adopted by the FCTC.

**6.5.6.1**
The CAPS must be capable of displaying up to three document viewing workspaces side-by-side. The purpose of having up to three open workspaces is to allow the user to view either three different documents or three pages of the same document at the same time. The first viewing workspace will be referred to as the initial workspace, the second and the third viewing areas will be called the second and the third viewing workspace respectively. The initial viewing workspace shall open first, and the second and third workspace viewing areas shall open as the second and third documents are loaded for display. Each workspace must contain a control for paging the document forward or back.

**6.5.6.2**
A document being opened for viewing must open in the next available workspace to the right of the last viewing workspace opened. If all workspaces are in use displaying a document, the document shall open as a tab in the initial workspace, or via a horizontal scrolling in the same viewing area.

**6.5.6.3**
The workspace viewing area must contain controls that zoom, shrink, rotate or flip the document they contain.

**6.5.6.4**
The display must afford the user an option to specify user settings that identify the documents that can automatically be pre-loaded by default into three display workspaces when a case is opened for viewing.

**6.5.6.5**
The system must automatically adjust page workspace viewing area sizes to fit the monitors on which the documents are displayed. For example, smaller monitors would only need to be able to automatically display two workspace viewing areas rather than three.

**6.5.6.6**
Variances from these display standards are permitted or tablets and mobile devices to allow for effective use of their smaller displays.

### 6.5.7 Word Search

The system must be able to search the contents of the documents in the official court files of a single case or multiple cases selected according to limiting criteria, including division of court, date range, related cases of a party, attorney, or other participant, charges or causes of action, and document type.

### 6.5.8 Accessing External Data

The system must make reasonable use of available sources of machine-readable data, organized into a display format useful to the court. It must contain a direct means for accessing legal research providers including but not limited to Westlaw and Lexis-Nexis.

## 6.6 CASE MANAGEMENT AND REPORTING

### 6.6.1 Reporting

The system must have a comprehensive reporting function for case management data and must be flexible to meet the reporting needs of individual circuits or counties. At a minimum it must provide:

**6.6.1.1**
Active Case List, including title, type, age attorneys or firms, next scheduled event date, and time since last activity with the ability to sort and filter on any field.

**6.6.1.2**
Critical Case List, including a listing of cases by type which is near or has exceeded

Supreme Court time standards for such cases.

**6.6.1.3**
Inactive Case List, including a listing of cases with no activity for 180 days; with motions filed but not set for hearing; with no service of process after 120 days.

**6.6.1.4**
Pending Orders List, containing cases having matters held under advisement by the judge, with the number of days since being placed in a work queue, see Section 6.6.3.

**6.6.1.5**
List of cases on appeal, if the data is retrievable from the clerk's database.

**6.6.1.6**
Performance Measures. The system shall have the ability to report the clearance rate of
cases, age of pending cases, and time to disposition of cases.

### 6.6.2 Workflow Management

The workflow management system shall contain a work queue for each internal user and a due date monitoring system.

### 6.6.3 Work Queue

The system shall have a function for tracking the court's work queue.

**6.6.3.1**
The judge, when viewing a document or a progress docket, shall have the ability to place a reference to the document directly into the work queue for subsequent action, with the ability to over-ride default due date or such other due date the judge may select.

**6.6.3.2**
The work queue shall also accept other manually entered items.

**6.6.3.3**
Each work queue must be able to accommodate the classification of work queue items into separate item types, such as "proposed orders," "internally generated orders," requests for Domestic Violence Injunctions, Warrants, emergency motions, and other user-specified types.

### 6.6.4 Daily Reminder (tickler)

The system shall have a function for tracking due dates of specified tasks.

### 6.6.5 Alerts

The system must afford each user the ability to specify (and edit) a watch list of cases, sending an alert (electronic notification) advising that there has been a new filing or entry posted within the last twenty-four hours to the progress docket of any case on the user's watch list.

### 6.6.6 Automated Task for Case Management

The system must be able to run automated tasks that provide case management functions for the court, enabling the court to perform a SQL like query of any of the available data elements and populate form orders for each returned result.

## 6.7 E-NOTIFICATION OF DATA ISSUES TO THE CLERK

### 6.7.1 E-Notification of Data Issues

CAPS shall provide the user a button that, when clicked, creates a communication to the Clerk's office for review of that case in question.

**6.7.1.1**
The communication should auto-include the case number in question.

**6.7.1.2**
The communication should provide an editable text field in which the user can describe the issue.

**6.7.1.3**
The CAPS shall maintain a record of communications generated and conveyed to the clerk for review.

**6.7.1.4**
An e-mail generated automatically from within the CAPS is an acceptable solution.

**6.7.1.5**
Each communication should include:

- the user reporting the issue;
- the case number in question;
- the issue to be reviewed (e.g., a case is pending in error); and
- a date and time stamp memorializing the time of the transmission.

**6.7.1.6**
Communications should be able to be easily aggregated for periodic transmission (e.g., a flat file).

## 6.8 ORDER GENERATION AND PROCESSING

### 6.8.1 Order Generation and Processing Required

The system shall have the capacity to generate court orders by merging information from the accessible databases and runtime user input into a bank of forms. The CAPS shall permit editing of the proposed order and file the signed order in PDF/A format.

### 6.8.2 Recallable Entries

The order generation subsystem shall be able to recall previous entries by the same user to avoid the necessity of re-keying content.

### 6.8.3 Portal Integration

The CAPS shall permit proposed orders to be received through the Portal and shall permit signed orders to be filed directly to the clerk's CMS or Portal and served through the Portal, CMS, or CAPS.

### 6.8.4 Document Models

The document model for the order generation function must not be proprietary. Neither the court nor any county may be prevented from building or customizing their own form banks.

### 6.8.5 Templates

The order generation function shall permit the court to generate orders from templates that merge, case style, case data, signature lines, distribution list data, and free text with the template.

### 6.8.6 Electronic Signatures

The order generation function must support the electronic signing of documents that results in a signed PDF document from either an internally generated or submitted proposed orders.

**6.8.6.1**
Unless a document is signed when generated, it shall be placed in the judge's work queue.

**6.8.6.2**
The court must have the option of electronically signing some, all, or none of the documents in the work queue at the same time.

**6.8.6.3**
The subsystem must have a means for rejecting proposed orders submitted for signature with an explanation of the reason for rejection.

**6.8.6.4**
An electronic signature of a judge shall be accompanied by a date, timestamp, and 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.

### 6.8.7 Electronic Filing and Service

The system shall effectuate electronic filing and service of orders according to the Florida Rules of Judicial Administration.

## 6.9 CASE NOTES

### 6.9.1

The system shall have a case note function that accepts input from internal users and may be viewed only by authorized personnel.

**6.9.2**

The subsystem shall accept note entries through text entry and insofar as feasible shall be compatible with speech-to-text utilities.

**6.9.3**

The subsystem shall be capable of accepting and storing documents or scanned images as part of the case notes.

**6.9.4**

When a case note is originally entered from a document viewing screen, the case note must be able to recall the same document when the note is later viewed.

**6.9.5**

The system shall automatically document the following in an audit log: scheduling events, changes to scheduled events, orders and judgments stent from the system, and the name of the user who initiated the entry or generated the order or judgment.

## 6.10 HELP

**6.10.1**

The system must have a help system that adequately provides tutorials and documentation for users.

**6.10.2**

There must be a control on every screen other than a modal window that can access the help menu.

**6.10.3**

The help menu must describe how to use each component of the system.

**6.10.4**

The help menu must contain a feedback channel for alerting system administrators of any performance issues or other problems.

# SECTION 7 INTEGRATION AND INTEROPERABILITY

This section contains subsections that describe the scope of the processes to which the Integration and Interoperability requirements apply.

## 7.1 BACKGROUND

The Integration and Interoperability requirements and standards are derived primarily from industry best practices and existing standards. The functional requirements of the judicial branch drive the need to define an environment that can fulfill the needs of all justice partners as they interact with the public and other federal, state, and local agencies. The hardware and software platforms, network infrastructure, and methods for data exchange that are discussed and recommended in this document support the strategic vision of the Florida Courts Technology Commission ("FCTC") relative to integration and interoperability among heterogeneous systems.

## 7.2 REQUIREMENTS AND STANDARDS FOR INTEGRATION & INTEROPERABILITY

This section contains the preliminary requirements and recommended standards for interoperability and integration between technology systems that provide information to or on behalf of the judicial branch. The requirements and standards were defined by analyzing Legislative/Supreme Court mandates, functional requirements, existing information systems architecture, and incorporating the results of that analysis into a solution that leverages contemporary information technology management industry standards and best practices for optimal performance, return on investment and efficient technical solutions.

### 7.2.1 Diagrams

The diagrams in this section give an overview of the Florida court system network topology (Figure 1) and the circuit court approved clerk interface (Figure 2).

***Figure 1. Florida Court System Network Topology Overview***

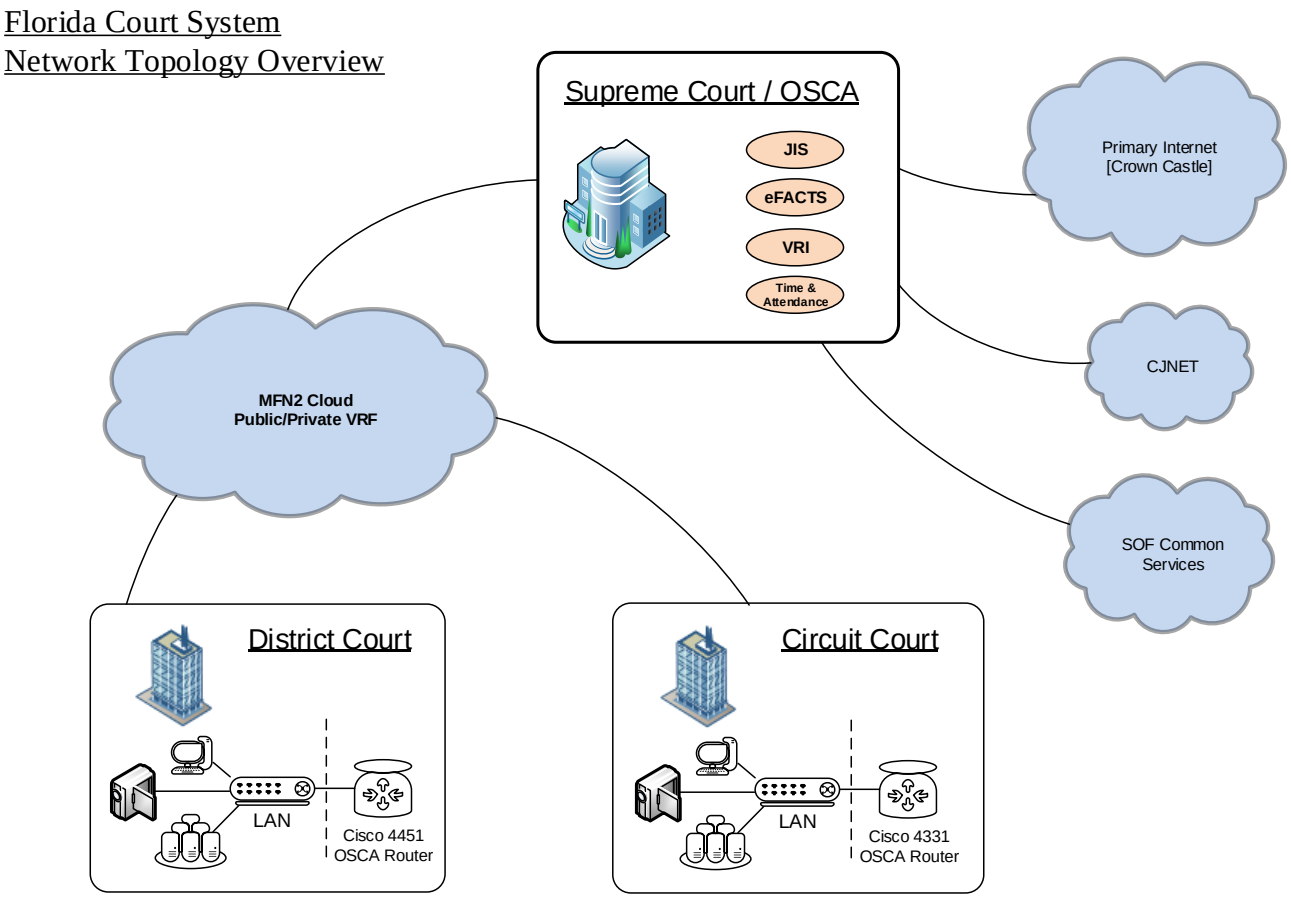
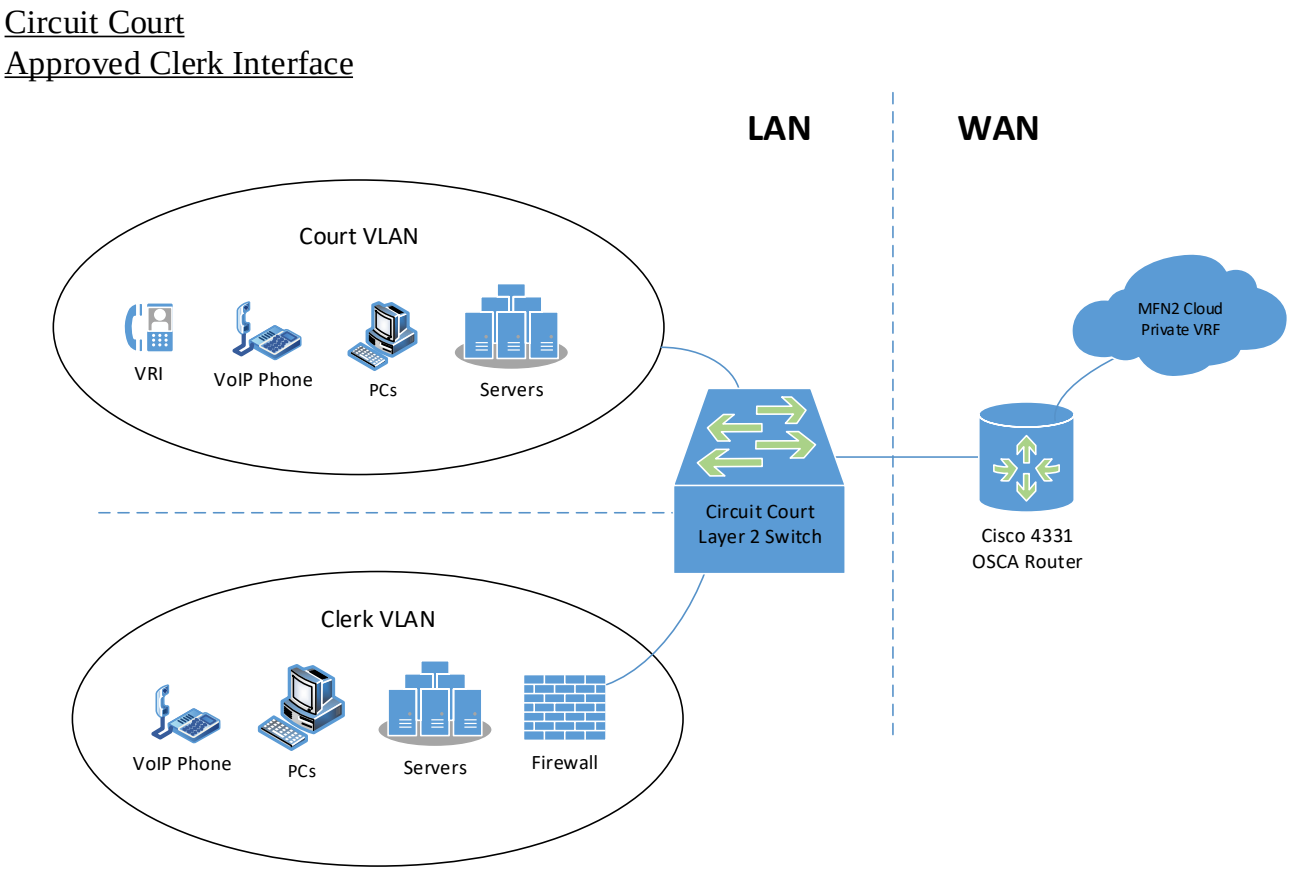


***Figure 2. Circuit Court Approved Clerk Interface***



## 7.3 INTEGRATION REQUIREMENTS AND STANDARDS

Integration requirements and standards are needed to provide the court with an understanding of both the high-level logical design requirements and the physical infrastructure standards and requirements that will be required to efficiently integrate the disparate systems that will support the courts.

### 7.3.1 Infrastructure Standards and Requirements

Standards and requirements are established to provide a strategic approach to hardware and software standardization and lifecycle management that will assist circuits in planning, procuring, and implementation of technologies necessary to comply with Supreme Court and Legislative technology mandates. Florida Statute 29.008 states that counties within each Judicial Circuit are responsible for the court's technology needs, including but not limited to computer hardware (e.g., PCs, video displays, laptops, servers, etc.) To most effectively manage the technology's total cost of ownership, lifecycle management should include hardware and software procurement strategies, physical asset management, technical support strategies, and retirement and disposal strategies that maximize the hardware's utility in support of the court's business objectives. Finally, when planning technology solutions, it is imperative to remember that the personnel costs required for the maintenance of the solutions often exceed the cost of the physical solution itself. Proper support ratios should be factored in to ensure the efficacy of the solution.

The goal of these guidelines is twofold: first, provide a blueprint for a robust extensible infrastructure that will support the growth, integration, and interoperability of information systems supporting the judicial branch; and secondly, reduce aggregate costs through standards that offer economies of scale.

#### 7.3.1.1 Desktop PC Standards

Desktop Personal Computer ("PC") procurements must be scheduled to meet certain lifecycle and performance objectives. Due to increasingly intensive software requirements, a three-year lifecycle is recommended. The minimum and recommended performance level requirements for desktops currently are listed in Figures 3 and 4. The performance level required will be determined by evaluating system needs, including the number, type and complexity of applications being run, system resources necessary to simultaneously run these applications; and performance metrics requisite for compliance with court standards.

- **Courtroom/Hearing Room**. Video displays: Per the Court Application Processing System ("CAPS") standards, courtroom and hearing room displays shall have sufficient screen size to display multiple electronic documents. The minimum recommended size for a video display is 30". Video display installations should allow for a range of movement and flexible placement to prevent obstruction of the judge's view of the courtroom or hearing room. Due to the diverse size, complexity, and nature of myriad judicial proceedings, the final determination for size and placement may vary depending on the environment.

- **Judge Chambers**. Video display: 24” or greater with capability for dual displays.
- **Video Display**. Video display replacement lifecycles may differ from desktop lifecycles based on functionality and usage requirements. Touch screen displays shall be used where deemed appropriate by the court.

***Figure 3. Minimum Desktop Configuration for New Machines***

| | | Details |
|---|---|---|
| **Hardware** | **Processor** | Quad Core Business Class Intel or AMD (**3.4** GHz or greater) |
| | **Memory (RAM)** | 8 GB or greater |
| | **Storage** | 500 GB Solid State Drive (“SSD”) |
| | **Video** | DirectX 12 or greater Capable (WDDM Driver Support recommended) |
| | **Graphics RAM** | 256 MB or greater, the system should be able to accommodate dual displays |
| | **Sound** | Audio is required in accordance with the planned use of the system |
| | **Ports** | HDMI and multiple USB 3.0/USB C ports as required |
| | **Lifecycle** | 3 years |
| **Network Connectivity** | **Bandwidth** | 100/1000BaseT Ethernet, wireless as required |
| | | |

### 7.3.1.2 Laptop Standards

The court’s migration toward a paperless environment and the implementation of electronic warrant applications offers unprecedented access to judicial officers in nontraditional venues and create an increased need for access to electronic court files/forms from secure, mobile devices.

***Figure 4. Recommended Laptop Configurations***

| | | Details |
|---|---|---|
| **Hardware** | **Processor** | Quad Core Business Class Intel or AMD (3 GHz or greater) |
| | **Memory (RAM)** | 8 GB or greater |
| | **Storage** | 250 GB Solid State Drive (“SSD”) |
| | **Graphics** | DirectX 12 or greater Capable (WDDM Driver Support recommended)<br>256 MB (in addition to RAM) |

| | | |
|---|---|---|
| | **Sound** | Audio required |
| | **Ports** | HDMI or mini-display USB 3.0/USB C ports as required |
| | **Lifecycle** | 3 years |
| **Network Connectivity** | **Bandwidth** | Integrated 100/1000 Ethernet LAN (standard) |
| | **Wireless** | Internal adapter supporting 802.11 b/g/n/ac |

#### 7.3.1.3 Client (Desktop/Laptop) Software Standards

Software requirements for desktops provide a standardized environment for users. This standardization will both simplify and increase the efficiency of the initial software deployment and on-going support for desktops and laptops.

***Figure 5. Software Requirements and Standards***

| Software | Details |
|---|---|
| Operating System | Windows 10 Professional or higher (OS must be active in the MS Support Lifecycle for patches and updates) |
| Office Suite | G Suite, Office365, or Microsoft Office version currently supported by Microsoft |
| Other Productivity Software | 1) PDF Reader<br>2) PDF Writer |
| Security Software | 1) Anti-virus<br>2) Anti-malware |

#### 7.3.1.4 Mobile Devices

This document defines mobile devices for those that have sufficient computing power for Internet access, receive e-mail reception, client-side applications, and interoperability with server-side applications. Examples of these mobile personal computing devices include but are not limited to tablets, smartphones, and hybrids. Mobile devices with limited security features should be limited to less sensitive areas of access unless a specialized security measure can be applied that will meet security standards. Mobile device usage must comply with the Criminal Justice Information Services (CJIS) Security Policy under the U.S. Department of Justice, Federal Bureau of Investigation.

#### 7.3.1.5 Recommended Mobile Device Configurations

All mobile devices should exceed the minimum standards available at the time of purchase.

#### 7.3.1.6 Mobile Device Computing: Any device, anytime, anywhere

Mobile computing technologies increase productivity and flexibility, as well as support continuity of operations in an emergency. Mobile Computing is a rapidly growing segment of court technology; however, with new efficiencies come new security risks: great diligence must be applied to ensure that developing standards for e-filing and data protection factor devices that can access, view, manipulate and store private court information. The introduction of CAPS that can be accessed off-premise has made mobile devices more utilized than ever.

Mobile devices generally refer to smartphones and tablet devices that support multiple wireless network connectivity options (primarily cellular and Wi-Fi), as well as voice and data applications. This section will focus on the mobile computing or data element.

- **Mobile Device Management ("MDM")**. A key component to successful control and administration of mobile computing is an MDM Enterprise System that provides security, accessibility, and content policies on many popular tablets and smartphones.

  MDM products have been developed to mitigate threats to mobile devices by enabling enterprise-controlled device configuration, security policy enforcement, compliance monitoring, and response (e.g., remotely lock and/or wipe a mobile device that has been reported as lost or stolen). MDM solutions typically include an enterprise server(s) component and an application installed on the mobile device to manage device configuration and security and report device status to the MDM.

  Small Florida court technology budgets juxtaposed against the tremendous popularity of the smartphone and tablet have led to an unprecedented rise in Bring Your Own Device, or BYOD. Standards to exercise control, manage expectations, and define acceptable use policies should be developed and implemented for all such users.

- **DDNA**. Securing mobile devices should focus on the following 4 categories:
  1. **Device** security: methods to prevent unauthorized device use, such as an MDM.
  2. **Data** security: protecting data at rest even on a lost/stolen device, such as an MDM.
  3. **Network** security: network protocols and encryption of data in transmission.
  4. **Application** security: security of the applications, and operating system, such as a MAM.
- **Recommended MDM Requirements**
  1. Enforce passcodes on devices.
  2. Allow remote location of devices.
  3. Allow remote wiping of device's drive/data.
  4. Allow remote locking.
  5. Detect rooted/jailbroken phones, which are more vulnerable to malicious code.
  6. Inventory of devices.
  7. Policy compliance.
- **Mobile Application Management ("MAM")**. MAM allows the court to set up an enterprise application store to deploy approved applications, enforce application policies, and remotely upgrade or uninstall applications.

To mitigate the threat of malicious or vulnerable mobile applications to mobile devices, the court should use MAM to provision for application whitelisting or allowing installation of mobile applications from authorized enterprise application stores application blacklisting, which blocks the installation of known vulnerable applications.

- **Recommended MAM Requirements**
    1. Allow for the installation of applications from a private site.
    2. Control the push/pull of updates to devices.
    3. Allow for the remote installation of applications.
    4. Allow for the remote wiping of non–standard applications.
    5. Whitelisting of select applications from public sites.
    6. Blacklisting of select applications based either on application or site.
    7. Application inventory.
- **Standards for Acceptable Use: Managing Expectations**
  Until the FCTC approves a standard policy, each circuit is recommended to develop an acceptable use consent policy that will outline expectations for security, support, and data access on a mobile device. It is recommended that each circuit develop a policy for approval by the Chief Judge. This policy should at a minimum address the following areas:
    1. What is the circuit policy for bringing your own device ("BYOD") hardware?
    2. For BYOD devices:
        a. What is the data backup policy?
        b. What is the extent of policy enforcement versus device support?
            i. Security enforcement – when can a device be wiped?
        c. Is the user cognizant of rules that constitute the creation of the public records?
        d. What enforcement exists for connectivity to unsecured networks (e.g., public wireless connection)?
        e. Is confidential data storage on the device prohibited?
    3. For court provided devices:
        a. What are acceptable recreational uses for the device (e.g., music, photos)?
        b. What is the data backup policy?
        c. Are secure network connections enforced?
        d. What is the acceptable use of data storage on the private or public cloud?
- **Wireless Networking Security**. Though both wired networks are vulnerable to the threat that intruders might snoop out network traffic, or inject rogue traffic, wireless networks are more susceptible to data theft and hijack. Mobile computing poses an inherent risk to data security that must be strictly managed and monitored. Using a VPN tunnel to encrypt mobile access to corporate resources makes for an excellent first line of defense. Additionally, it is important to educate users concerning the dangers of connecting to a wireless network that does not use 256-bit WPA2 encryption.

Users should understand that most public Wi-Fi is not encrypted and is, by its nature, not secure. By utilizing an encrypted VPN connection, the data transmitted between the device and the VPN endpoint are encrypted, even though the Wi-Fi connection itself is not encrypted. If no VPN is in use, then using encrypted protocols (such as HTTPS instead of HTTP) where possible will provide encryption between the device and the remote endpoint.

For internal wireless court/county networks, VLANS or MAC address filtering provide additional controls over secure connectivity.

Bluetooth settings, when not in use, should be turned off.

- **Best Practices for CJIS Connections**. Only use properly encrypted connections.
- **Best Practices for Non-CJIS Connections**. For wireless connections, only use properly encrypted connections. There are other potential confidential or sensitive data transmitted outside of CJIS systems.

  Be aware of Federal Information Processing Standards ("FIPS") 71A-1 Subsections 001-023, and the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy Sections 4.3, Personally Identifiable Information, and Section 5 regarding securing technology that accesses, stores, transmits and logs Criminal Justice Information governed by this referenced policy. The most current version of this policy can be viewed at http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/.

#### 7.3.1.7 Servers

Production servers should support both common/shared services as well as organization-specific services. Servers should meet a combination of priorities, including affordability, performance, scalability, space-optimization, and support for the mission-critical applications that will comprise the system. A maintenance contract with a qualified vendor must be maintained for any mission-critical servers.

#### 7.3.1.8 Network Components

- **Courts Local Area Network ("LAN") Considerations/Recommendations**
  A standard for agency LAN implementations should be established. It is recommended that the standard include the following:
  1. Naming conventions using Domain Name Service ("DNS") should be standardized across the courts.
  2. Ethernet topology (over unshielded twisted pair cabling).
  3. High-speed copper (UTP) to the desktop (CAT 5e or better).
     a. Utilize BICSI Standards as a guideline for structural wiring.
  4. Fiber optic cable for interconnections between high-speed concentration areas.
     a. Standardized connectors (ST, SC, LC, FC) and type single/multimode.

5. Networking equipment should be based on a full-switched TCP/IP network.
    a. Backbone should have Layer 3 capability for VLAN/Routing/QoS.
    b. Switches should have fiber uplink capability.
    c. Switches shall be manageable via IP or other remote protocol.
6. Scalable high-speed Ethernet/Fiber switches.
7. Bandwidth standards and requirements within and among each judicial location are recommended at:
    a. Gigabit to servers
    b. Gigabit to workstations

The use of existing LAN technology at judicial locations should be evaluated on a location-by-location basis. Where required, the LAN infrastructure should be upgraded to meet the standard.

Any LAN technology dedicated for use by the court should meet the following requirements:

| | |
|---|---|
| Feature Sets | IP Routing, VRRP, HSRP, STP enhancements, 802.1s/w, IGMP snooping, IEEE 802.3af Power over Ethernet (PoE). |
| Security | ACL, port security, MAC address notify, AAA, RADIUS/TACAC+, 802.1x, SSH, SNMPv3, IPv6 |
| Advanced QoS | Layer 2–4 QoS with Class of Service (CoS)/Differentiated Services Code Point (DSCP), & Differentiated Services Model (DiffServ) supporting shaped round robin, strict priority queuing.<br>QoS compliant with DiffServ (IETF) standards as defined in RFC 2474, RFC 2475, RFC 2597 and RFC 2598 and DSCP (IETF) standards as defined in RFC 791, 2597 2598, 2474, 3140 4594[MediaNet]. 802.1p, 802.1Q, 802.11e<br>Resource Reservation protocol (RSVP) in RFC 2205. |
| Management | One IP address and configuration file for the entire stack.<br>Embedded web-based cluster management suite to Layer 2/3/4 services easy configuration of network-wide intelligent services in local or remote locations automatic stack configuration. |
| Performance | Distributed Layer 2 and Layer 3 distributed providing *wire-speed* switching and routing via Gigabit Ethernet and Fast Ethernet configurations |
| Deployment | Automatic configuration of new units when connected to a stack of switches.<br>Automatic OS version check of new units with the ability to load images from a master location.<br>Auto-MDIX and Web setup for ease of initial deployment.<br>Dynamic trunk configuration across all switch ports.<br>Link Aggregation Control Protocol (LACP) allows the creation of Ethernet channeling with devices that conform to IEEE 802.3ad.<br>IEEE 802.3z-compliant 1000BASE-SX, 1000BASE-LX/LH, 1000BASE-ZX, 1000BASE-T and CWDM physical interface support through a field-replaceable small form-factor pluggable (SFP) unit.<br>10 gigabit Ethernet IEEE 802.3-2008 |
| Configuration / Survivability | Switches must work standalone and in a stacked configuration.<br>Stack up to 9 units, Separate stacking port.<br>Minimum 32Gbps fault-tolerant bidirectional stack interconnection.<br>Master/slave architecture with 1:N master failover.<br>Less than 1 second Layer 2 failover with nonstop forwarding.<br>Less than 3 second Layer 3 failover with no interrupt forwarding. |

| | |
|---|---|
| | Cross-stack technology, cross-stack QoS<br>Single network instance (IP, SNMP, CLI, STP, VLAN).<br>Minimum of 24 Ethernet 10/100/1000 ports and 2 SFP uplinks with IEEE 802.3af and pre-standard Power over Ethernet (PoE). |
| Software | Intelligent services: Layer 3 routing support via RIP, OSPF, static IP routing. Dynamic IP unicast routing, smart multicast routing, routed access control lists (ACLs), Hot Standby Router Protocol (HSRP) support, and Virtual Router Redundancy Protocol (VRRP). |

- **Courts Wide Area Network ("WAN")**. The WAN infrastructure supporting the courts will use the State network as its primary transport media, if applicable. Specific WAN hardware and software solutions should be evaluated and customized to handle the additional traffic that may be required from the system. Integration of local county network infrastructure to the State Network will be addressed on a case-by-case basis in compliance with definitions outlined in Florida Statutes 29.008(f)(2).

- **WAN Considerations/Recommendations**
  1. The court should strive to standardize Domain Naming Services ("DNS") conventions, Network Address Translation ("NAT") conventions, and TCP/IP conventions (including subnetting) based on RFP standards.
  2. The current infrastructure supports high-speed switching technology The WAN infrastructure should include the use of TCP/IP for inter-agency communications.
  3. Where possible, the communications infrastructure should provide for coexistence with existing architectures until these architectures are compliant with the standard.
  4. Multi-protocol WAN bandwidth may have to expand to handle traffic while supporting other emerging applications and business requirements.
  5. Each courthouse or remote facility should have a high-speed connection back to the State network unless a high-speed network has already been provided by the county. Network speeds for each circuit will vary depending on bandwidth requirements.
  6. Throughput on the WAN should be benchmarked at key junctures before the system becomes operational It should be monitored continually thereafter.
  7. State-provided bandwidth is a shared resource; accordingly, bandwidth management at the circuit level is strongly recommended.

#### 7.3.1.9 Wireless Technologies

In the courts, wireless technologies include point-to-point connectivity and multi-point connectivity. Point-to-point is utilized to extend ta WAN, connecting physically separate networks. Multi-point wireless is used to extend the LAN to wireless users within a limited geographic area. Wireless is beneficial when providing network connectivity for mobile judicial users, as well as fixed-user locations where wired LAN connectivity is unavailable. The following guidelines should be considered when developing a wireless security plan.

- **General Wireless Guidelines**
    1. Must meet current CJIS security standards.
    2. Change the default level of product security – out of the box, WLANs implement no security.
    3. Change the out-of-the-box settings – do not use default or null SSIDs or passwords.
    4. Implement wireless access points on switched network ports.
    5. Develop and publish standards and policies for departmental WLANs.
    6. At a minimum, use 256-bit keys or greater.
    7. Implement MAC address tracking to control network security.
    8. Monitor access logs or use network-based instruction detection to detect unauthorized access or attack.
    9. Highly sensitive networks should use a minimum of 256-bit encryption. The SSID should not be broadcast, and MAC authentication should be required.
    10. Disable Wi-Fi Protected Setup ("WPS").
    11. Each circuit should develop a practical and comprehensive wireless solution including a detailed IEEE 802.1x-based security plan.

- **Multi-Point Wireless**. Due to the open broadcast nature of wireless networks, each organization should design and publish security standards for their wireless solution. The WLAN uses several standards defined by the IEEE 802.11 classification that addresses both bandwidth and security issues. While cost will vary between technologies, priority for essential elements such as security through encryption and authentication is strongly recommended. Restricting the area of coverage for wireless access points should also be considered; covering only the areas within the physically controlled area reduces the accessibility by unauthorized users. Given the ongoing evolution of wireless standards, any guidelines and metrics should be reviewed during the planning stages of multi-point wireless projects.

  The following general guidelines should be considered when developing and implementing a wireless security plan for your WLAN.

  **Multi-Point Wireless Guidelines**
    1. Develop and publish standards and policies for departmental WLANs, including acceptable use and levels of service for multiple user types (if applicable).
    2. Perform site surveys in advance of access point placement to ensure adequate signal coverage and identify related power requirements.
    3. Implement wireless access points on switched network ports.
    4. Address security on two levels: encryption and authentication.
    5. The newest security standard is 802.11-2007 (sometimes referred to as WPA2), incorporating authentication by 802.1x standard. 802.1x supports authentication server or database service including Remote Authentication Dial-In User Service (RADIUS), LDAP, and Windows

domain, and Active Directory. Encryption in 802.11-2007 is strong AES.

6. Change the "out-of-the-box" settings – do not use default or null SSIDs or passwords. At a minimum, activate the default level of product security.
7. Set access point SSID broadcasting to "OFF".
8. Consider implementing VPN with strong encryption for wireless networks. Place access points outside of the firewall. Use VPN for connectivity to the intranet.
9. Implement MAC address authentication and tracking to control network security. Utilize monitoring software to limit network access based on the user's physical location and IP address, granting or denying access to services as needed.
10. Implement additional authentication if supported by the vendor (RADIUS, LDAP, etc.).
11. Monitor access logs or use network-based intrusion detection to detect unauthorized access or attacks.
12. All publicly accessible Wi-Fi must be outside the court's internal network.

- **Point-to-Point Wireless**. When implementing a wireless solution to connect remote locations, the following list of guidelines needs to be considered.

**Point-to-Point Wireless Guidelines**

1. Bandwidth/Network Requirements: Video Conferencing, Digital Court Recording ("DCR") Monitoring, VoIP, data volume, and latency.
2. Distance/Path: Line of sight is required.
3. Tower Locations and Access.
4. Security
    a. Physical security: Tower location and equipment need to be secure.
    b. Network security.
5. Availability: Uptime of 99.98% or better is recommended.
6. Management: Utilities should be Simple Network Management Protocol ("SNMP") compliant.
7. Warranty and Maintenance: Equipment, tower climbing, and maintenance should be included.
8. Each circuit should develop a practical and comprehensive wireless solution including a detailed IEEE 802.1x-based security plan.

Licensed bandwidth has oversight by the Federal Communications Commission ("FCC") and must adhere to FCC rules and regulations. Licensed bandwidth guarantees frequency ranges that are assigned to the associated license, preventing interference with other frequencies. Unlicensed bandwidth is not under the FCC oversight and carries the risk of interference

from competing wireless locations. Any interference issues must be negotiated on a case-by-case basis.

#### 7.3.1.10 Security Standards

Information Security encompasses many technical and non-technical areas. This section describes the comprehensive high-level technical security architecture strategy that should be addressed when defining Information Security requirements.

Information Security Standards are organized into four categories:

- Device Control
- Personnel Control
- Network Control
- Physical Security

These standards address the overarching Information Security needs and provide a framework for developing compliant Information Security Standards and Policies. Security standards shall comply with CJIS Security Policy under the U.S. Department of Justice, Federal Bureau of Investigation where applicable.

- **Device Control**
    1. Access Rights and Privileges: Computer-resident sensitive information shall be protected from unauthorized use, modification, or deletion by the implementation of access control rights and privileges.
    2. Anti-Virus Protection: Platforms that are susceptible to malicious code shall be equipped with adequate software protection when such protection is available.
    3. Authentication of Desktop Users: Desktop access shall be secured and authenticated using adequate security techniques.
    4. Backup Policy: Data storage devices shall undergo sufficient periodic backup to protect against loss of information.
    5. Business Continuity & Disaster Recovery: Formal business continuity and disaster recovery plan(s) shall be documented and implemented per applicable Florida State Courts policy and administrative rules.
    6. Transmission of Sensitive Data: Sensitive data (security management information, transaction data, passwords, and cryptographic keys) shall be exchanged over trusted paths, using adequate encryption between users, between users and systems, or between systems.
    7. E-mail Anti-Virus Protection: Proactive installation and management of software/hardware to safeguard against the injection of malware, viruses, or other code via e-mail or e-mail attachments is required.
    8. Platform Level Administration (Local): Local access to system console functions shall be restricted to appropriately authorized personnel.
    9. Platform Level Administration (Remote): Remote access shall be secured via adequate authentication and restricted to appropriately authorized personnel.
    10. System Administration Privileges: System administration privileges shall be locally granted only to appropriately authorized personnel.

- **Personnel Control**
    1. Acceptable Use Policy: Policies addressing the acceptable use of information technology shall be documented.
    2. Acceptable Use Training: All employees shall undergo training, briefing, and orientation as deemed necessary by the circuit to support compliance with all elements of established acceptable use and applicable information security policies and guidelines.
    3. Remote Access Policy: Where applicable, each circuit will maintain a written remote access policy.
    4. Sensitive and Exempt Data Handling: All employees with access to sensitive or exempt data shall be trained to handle the data in compliance with relevant guidelines. The Florida Department of Law Enforcement ("FDLE") establishes CJIS guidelines governing the access by any workstations to FCIC/NCIC data directly or through the Judicial Inquiry System ("JIS").
    5. Incident Response: Incident Response ("IR") procedures shall be developed and maintained. IR procedures will guide appropriate steps to take in response to breaches in devices, networks, and physical security.
- **Network Control**
    1. Network: Network security encompasses preventing unauthorized access to the LAN and WAN that will be used to access judicial services.
    2. Device Resistance: All critical devices within the perimeter network shall be resistant to attack by known threats for which there are available defenses.
    3. Network Audit Logs: Network audit logs shall provide sufficient data to support error correction, security breach recovery, and investigation. Network audit logs should be retained for a minimum of three months.
    4. Remote Access: All remote access methods providing access to critical systems shall be identified and inventoried. Remote access to the court's network and resources will only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted. Remote access logs should be recorded for a minimum of three months. A centralized point of access is preferred.
    5. Wireless Network Security and Management: All wireless networks and devices shall be locally authorized by each circuit and have adequate security configurations.
- **Physical Control**
    1. Physical Security Policy: Physical security policies shall adequately address information technology infrastructure.

#### 7.3.1.11 System Management Tools

A comprehensive set of management tools will be required to support an integrated information system environment. The system architecture and its components should support centralized monitoring and control. Characteristics of system management include:

- An application to provide complete systems and network management throughout the enterprise environments, preferably including Active Directory ("AD") monitoring, Structured Query Language ("SQL") (or equivalent) database monitoring, and detailed flexible reporting.
- Network management applications that are deployed and integrated to support network management requirements, including hub, switch, and router management. SNMP compliant hardware; when in a Windows environment, Windows Management Instrumentation ("WMI") compliance is required.
- Network management tools that have the ability to monitor across VLANs, WANs, and disparate network architectures, including wireless networks.
- Either IPv4/IPv6 are protocols. The tools should contain the ability to monitor, report, and block offending IP addresses or infected network segments.
- Network Quality of Service ("QoS") management utilities. Preference for SSH or SSL over telnet or HTML for network management tools.
- Traffic monitoring systems that utilize a learning mechanism establishing initial baselines that are time corrected and display anomalous traffic with reasonable swiftness. Rules-based equipment should allow for frequent base table updating.
- Desktop management tools deployed and integrated to support workstations, software distribution, desktop inventory control, and asset tracking of desktop configurations and installed software ("metering"). Ghost or equivalent imaging software, patch management (such as Windows Server Update Services ("WSUS")), and detailed, flexible reporting mechanisms.
- Server management tools should be SNMP compliant, have the ability to monitor server health, including disk, memory, process utilization, and when possible, power consumption, and when possible, support Lightweight Directory Access Protocol ("LDAP").

Change control applications should be utilized to help coordinate the activities (such as software code changes, testing and verification of the changes, and related documentation changes) that need to be performed by various organizations.

When evaluating system management tools administrators should consider the following criteria:

- For flexibility, site or enterprise licensing is preferred.
- "Agent-less" tools are not required but may be preferred.
- Robust reporting/metrics functionality is preferred and strongly recommended.

- E-mail/text alerts for virus monitoring should be available for all systems. Encryption should be required for some types of e-mail at rest and in route.
- Remote management of network, desktops, servers, provided software meets the established security standards is preferred.

A health report should be periodically generated, and contain the following information when possible:

- SNMP trap information.
- Login reports for both successful and failed attempts (wireless, RADIUS, VPN, etc.).
- Switch/router/hub changelogs.
- Wireless connections.
- Server health (average CPU load, RAM and disk utilization, etc.).
- Active Directory additions/deletions/changes.
- Restricted traffic attempts and perceived network anomalies.

#### 7.3.1.12 Audio and Video Teleconferencing

The following is a list of recommended guidelines that will serve as a baseline for video conferencing definition.

- **Digital Audio and Video Conference Standards**
    1. Must use the TCP/IP network protocol.
    2. Separate VLAN for video.
    3. Standard definition speed: 384K.
    4. High definition speed: 768K
    5. Duplex: Full (512 units = half).
    6. Network speed: 100Mbps (502 units = 10Mbps).
    7. Switch and codec: hard-coded speed/duplex.
    8. Video communications must support the H.264 SIP multimedia standards.
    9. Audio conferencing must support G.711 audio compression
    10. Low Resolution: Based on communications availability. H.323 standard should use a minimum of 256Kbps bandwidth per concurrent video session.
    11. QoS tag: DSCP AF41.
    12. Ports: 1719, 1720, 3230-3253 TCP/UDP

Any endpoint or Multi-Point Conference ("MCU") traversing the Internet should be considered "best effort", given the circuit's inability to manage all aspects of the connection, signal quality, and clarity.

#### 7.3.1.13 Cloud Video Conferencing

Support for cloud-based video conferencing is desirable.

#### 7.3.1.14 Court Reporting Technologies

Court Reporting standards shall comply with CJIS Security Policy under the U.S. Department of Justice, Federal Bureau of Investigation when applicable.

- **Reference**
  Technical and Functional Standards for Digital Court Recording (last updated April 2018).

#### 7.3.1.15 Technical Support

Skill sets needed to achieve technology objectives and provide support and maintenance should be defined by each circuit court.

On-call is required to support 24/7 operations.

#### 7.3.1.16 User Support Ratio

Minimum service level expectation in the court environment is to provide initial service within the same day or less as when the call for assistance was received, depending on the criticality of the environment (e.g., a case manager's printer error can be responded to the same day, but a network outage impacting first appearance or shelter hearings must be responded to more quickly).

Specialized technical services may require dedicated support staff depending on the environment. Specialized services may include:

- Network
- Security
- Audio Video
- ADA
- Communications
    1. Data
    2. Voice
- Training
- Web
    1. Internet
    2. Intranet
- Application Development
- Database Administration
- Server Administration

Other considerations: Geographic distribution of serviced sites will impact service levels. Multi-county or large county circuits must factor travel time into service level expectations. Additional staff may be required to meet service level requirements.

Funding for on-going training must be included with staff to maintain the skill sets required to support the environment.

#### 7.3.1.17 Courtroom Technology Standards

- **Courtroom – Hearing Room Technology Minimum Requirements**
  For criminal proceedings, courtrooms and hearing rooms need to have the infrastructure in place to deliver information and services to the courtroom. Information is vital whether it is information on a computer screen, a juror's

ability to hear the witness, or the ability to set up evidence presentation tools. For Civil proceedings, equipment may be used if available; otherwise, attorneys are responsible for providing the equipment needed for evidence presentation.

Posting a disclaimer on the circuit's website concerning the provided technology is recommended. An example is listed below:

> Courtroom technology is provided as a courtesy to the legal profession and court participants. While the court will make every effort to ensure the equipment is working properly, the court does not guarantee the reliability or availability of the equipment. It is presumed that anyone using courtroom technology is properly trained to do so. The court is not responsible to provide educational or technical support for these services. By using this technology, the user agrees to hold the court harmless for any equipment failure or corruption of data, for any court-related proceeding, and to not seek to delay/reschedule of court proceedings due to same. Finally, users agree to be prepared to proceed without using technology should the circumstances warrant such action.

- **Infrastructure**
  When building new courtrooms, plans shall include conduit and cable paths to support existing and future technology. Raised flooring is recommended for courtrooms to allow for easy access. Floor boxes can be used to support future expansion. If using floor boxes, industry-standard termination must be accommodated into the design of the floor boxes and wiring practices. See Figure 6 for a typical courtroom design.

- **Courtroom Technology Guidelines**
  1. DSP-based Sound Reinforcement System (1 system per courtroom) /ADA compliant hardware. Microphone locations should be discussed with Chief Judge to determine if hanging microphones, tabletop microphones, or if both types are needed in the courtrooms.
  2. ADA assisted listening devices.
  3. Video display(s).
  4. 1 pan/tilt/zoom camera (minimum).
  5. DCR (when applicable).
  6. LAN access for Judge and Clerk.

- **Recommended Optional Integrated Equipment**
  1. Touch panel control pad.
  2. Wireless presentation interface.
  3. Sidebar microphones.
  4. Gallery microphones.
  5. Video displays/Intelligent displays (capable of supporting different multi-media sources).
  6. Touch screen video displays (witness stand for evidence presentation).

7. 4 pan/tilt/zoom cameras (suggested camera options: judge, witness, courtroom, and evidence/jury. The evidence camera should be mounted in the ceiling at a location that allows evidence to be placed underneath for presentation.
8. Network access/Wi-Fi for participants.
9. Remote interpreting A/V equipment.
10. Video conferencing.
11. Teleconferencing.
12. Analog stereo audio, VGA, component, and HDMI inputs and/or wireless media display devices, display port, and other industry-standard connections.
13. Media plate
14. Remote technical support and control.
15. White noise cancellation for sidebar conferences.
16. Where needed, the microphones should be configured to work with the DCR.

- **Hearing Rooms Guidelines**
  While sound systems may not be needed in all hearing room types, other equipment is essential. These rooms shall include the following:
  1. ADA assisted listening devices.
  2. Video display(s).
  3. 1 camera.
  4. DCR (pre-wired if possible).
  5. LAN access for judge and clerk

- **Recommended Optional Hearing Rooms Equipment**
  1. Network access/Wi-Fi for participants.
  2. Wireless presentation interface.
  3. Remote interpreting A/V equipment.
  4. Video conferencing.
  5. Teleconferencing.
  6. Analog stereo audio, VGA, component, and HDMI inputs and/or wireless media display devices, display port, and other industry-standard connections. These inputs can be installed in a floor box or wall plate.
  7. Remote technical support and control.

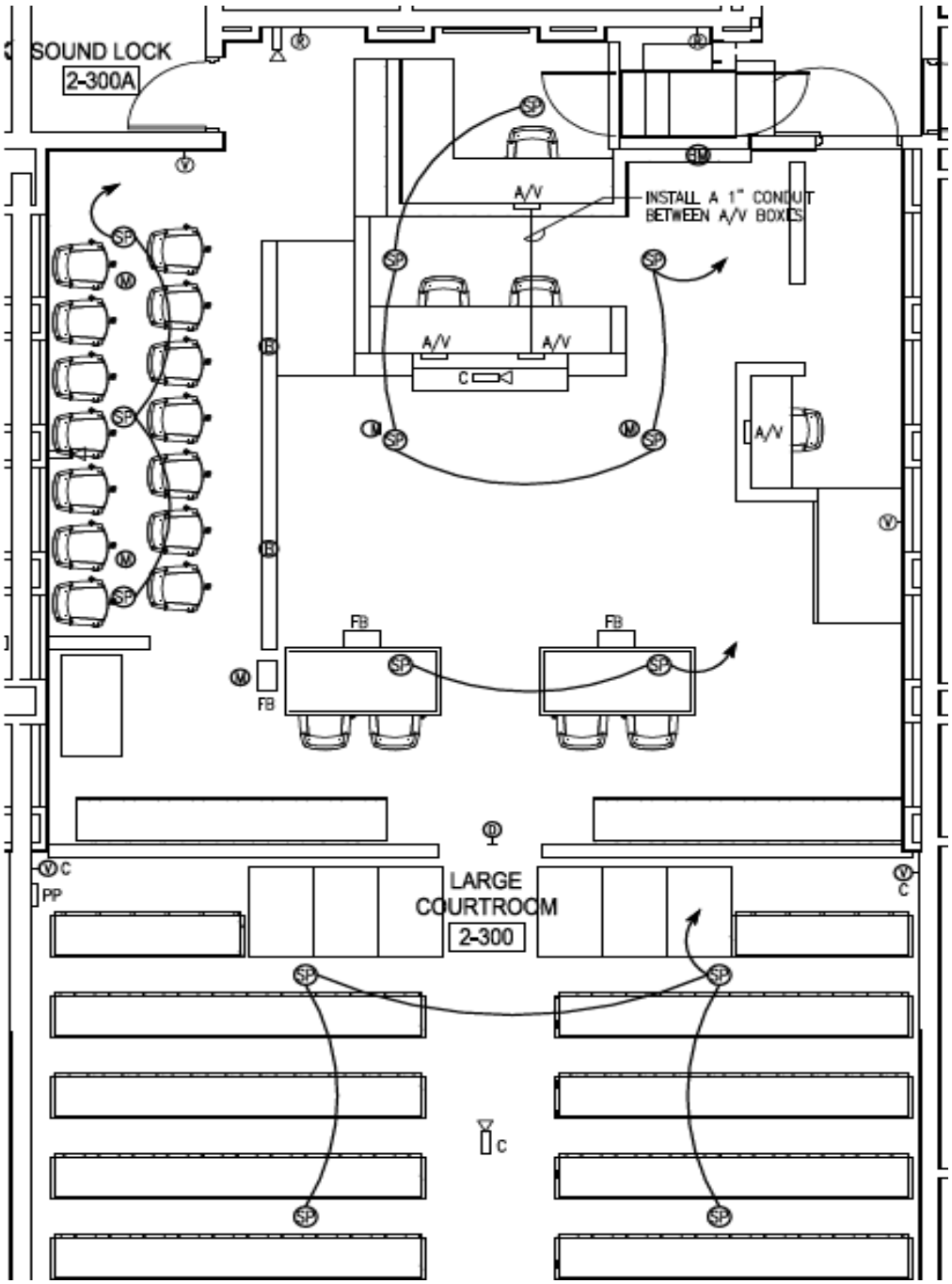
- **Optional Mobile Technology**
  If funding is unavailable for integrated courtroom technology solutions, mobile systems are recommended. Evidence presentation systems should be able to display a wide range of types/formats/sizes of physical and digital evidence used in today's courtrooms. An evidence presentation system should include (but not be limited to) the following support components:
  1. **Display**
     Mobile display (TV/LCD screen) or projector:
     A mobile display is recommended only for smaller settings and should support multiple resolutions with sufficient brightness.

A projector should support multiple resolutions with sufficient brightness for viewing in ambient light (will vary based upon projected image size) + projector screen.

The system should provide audio/video outputs compatible with the courtroom's integrated video displays/audio/DCR system (if applicable).

2. **Cables**
   Audio/video presentation systems should support prevailing audio/video transmission cable standards such as analog stereo audio, analog stereo audio, VGA, component, and HDMI.
3. **Physical Media**
   Audio/video presentation systems should support prevailing physical media standards such as CD (R/RW), DVD, (+R/RW), USB storage device (flash or HD), CompactFlash, SD/Smartmedia, Memory Stick, Blue-ray, and cell phone connectivity.
4. **Digital Audio/Video Standards**
   Audio/video presentation systems should support prevailing digital audio/video standards such as Audio CD, DVD, VCD, SVCD, WMV, Quicktime, Mpeg4, MP3, OGG.
5. **Overhead Projector**
6. **Document Camera**

***Figure 6. Courtroom Drawing***



AV INFRASTRUCTURE LEGEND:

PP — PRESS PLATE LOCATION. CONTRACTOR SHALL INSTALL A 8"x8"x3" DEEP JUNCTION BOX FLUSH IN WALL AT 18" AFF. INSTALL TWO 2" CONDUIT FROM THE PLATE TO THE CABLE TRAY ON THE 1ST LEVEL.

FB — FLOOR BOX/POCKET; INSTALL AN ACE BACKSTAGE 124SL FLOOR POCKET OR APPROVED EQUAL. THE FLOOR POCKET SHALL BE ABLE TO CONTAIN A MINIMUM OF 4 A/V GANGS, 1 DUPLEX RECEPTACLE, 2 RJ-45 CONNECTORS, AND TWO SPARE SINGLE GANG PLATES. EACH POCKET SHALL HAVE TWO 2" CONDUITS FOR FUTURE A/V CABLING AND ONE 1" CONDUIT SPARE. THESE CONDUITS SHALL BE INSTALLED TO THE CABLE TRAY ON THE 1ST LEVEL. A SEPARATE CONDUIT SHALL BE INSTALLED FOR THE DUPLEX RECEPTACLE AND A SEPARATE CONDUIT FOR THE RJ-45 CONNECTIONS. REFER TO THE TELECOM AND POWER PLANS FOR INFORMATION ON THESE SYSTEMS.

(SP) CEILING SPEAKER LOCATION; LOCATION IS APPROXIMATE AND SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO ROUGHING IN; A JUNCTION BOX SHALL BE INSTALLED AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE SPEAKER TO THE OTHER SPEAKERS ON THE SAME ZONE. THE HOMERUN CONDUIT FOR EACH ZONE SHALL BE INSTALLED TO THE CABLE TRAY ON THE 1ST LEVEL.

(M) CEILING HANGING MICROPHONE LOCATION; LOCATION IS APPROXIMATE AND SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO ROUGHING IN; A JUNCTION BOX SHALL BE INSTALLED AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE MICROPHONE TO THE CABLE TRAY ON THE 1ST LEVEL.

(B) BUTTON MICROPHONE LOCATION; LOCATION IN CASEWORK IS APPROXIMATE AND SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO ROUGHING IN; A STUB UP 3/4" CONDUIT SHALL BE INSTALLED IN THE CASEWORK. THE CONDUIT SHALL BE ROUTED TO THE CABLE TRAY ON THE 1ST LEVEL.

(BM) SIDEBAR BUTTON MICROPHONE LOCATION; LOCATION IN CASEWORK IS APPROXIMATE AND SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO ROUGHING IN; A STUB UP 3/4" CONDUIT SHALL BE INSTALLED IN THE CASEWORK. THE CONDUIT SHALL BE ROUTED TO THE CABLE TRAY ON THE 1ST LEVEL.

A/V — A/V PLATE LOCATION; INSTALL A 12" WIDE x 6" TALL x 3" DEEP JUNCTION BOX FLUSH IN CASEWORK. JUNCTION BOX SHALL BE LOCATED 18" ABOVE THE BOTTOM OF THE CASEWORK. INSTALL TWO 2" CONDUITS AND ONE 1" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL.

A/V CAMERA LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE WALL AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL. MOUNTING HEIGHT SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO INSTALL.

C — A/V CAMERA LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE CEILING AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL. MOUNTING HEIGHT SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO INSTALL.

(V) TV LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE WALL AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL. MOUNTING HEIGHT SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO INSTALL.

(V) C — TV LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE CEILING AT EACH LOCATION. INSTALL A 3/4" CONDUIT FROM THE JUNCTION BOX TO THE CABLE TRAY ON THE 1ST LEVEL. EXACT LOCATION SHALL BE COORDINATED WITH THE A/V CONTRACTOR PRIOR TO INSTALL.

(D) DCR LIGHT LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE WALL 12" ABOVE THE BOTTOM. INSTALL A 3/4" CONDUIT TO THE CABLE TRAY ON THE 1ST LEVEL.

(R) HEARING IMPAIRED IR LOCATION; INSTALL A JUNCTION BOX FLUSH IN THE WALL AT A HEIGHT TO BE DETERMINED BY THE A/V CONTRACTOR. INSTALL A 1" CONDUIT TO THE CABLE TRAY.

## 7.4 REQUIREMENTS FOR INTEROPERABILITY AND DATA EXCHANGE

New applications being developed must have web-based capabilities for record viewing. Any enhancements or upgrades to existing applications must include support for access through a web browser for viewing of records. To the extent possible, access to add, change, and delete information must migrate toward web-based interfaces. Scanning systems and other applications that directly interface with peripherals are more difficult to move to web-based applications, but it is possible. In addition, applications must include industry-standard application programming interfaces ("APIs") for standardized exchange of information.

The technical standards listed below have been developed across all industry sectors and have the joint backing of many software development companies (e.g., Microsoft, Oracle, Sybase, IBM) that have recognized that information exchange and the resulting gains in productivity and efficiency are critical strategic goals of improved system performance.

### 7.4.1 Software Applications

- Software applications must support the following standards when applicable:
    1. Presentation (for web-based applications)
        a. Standards compliant XHTML 1.0/HTML 4.01 and later
        b. Standards compliant Cascading Style Sheets 2.1 and later
    2. Application
        a. Service-Oriented Architecture ("SOA") should be applied to applications.
        b. Development processes such as Model-View-Controller ("MVC").
        c. The presentation layer should access information via a web service.
        d. Where possible, code should be executed on the server (server-side-code), not the client.
        e. eXtensible Markup Language ("XML").
        f. Simple Object Access Protocol ("SOAP")
        g. Web Services and/or Representational State Transfer ("REST") web services.
        h. JSON ("JavaScript Object Notation").
        i. American National Standards Institute Structured Query Language ("ANSI SQL").
        j. W3C ADA/508 compliance.
        k. Open Database Connectivity ("ODBC"), Java Database Connectivity ("JDBC"), OLEDB, Database Native Clients.
        l. Remote Procedure Call ("RPS")
    3. Storage
        a. American National Standards Institute Structured Query Language ("ANSI SQL").
    4. Security
        a. Security for all components of software applications should use industry-proven algorithms, techniques, platform-supplied infrastructure, and vendor-tested and supported technologies.

b. The Data Exchange Standards, adopted in May 2016, but the FCTC provides a Data Security Model standard to which applications should adhere when applicable.

### 7.4.2 Data Transmission

Protocols for transmission, between distinct entities, of data governed by this document must be generally available, nonproprietary, and protected by the most secure methods reasonably available to all participants. Each repository of data shall provide its data per this document, the Data Exchange Standards, and such other standards as may be adopted under the authority of the Supreme Court.

### 7.4.3 Database Standards

Database connectivity to some databases may not be possible due to driver/network restrictions at the location. Each participating agency/entity should collaboratively develop a plan governing the connection to, accessing, and formatting the data maintained in the particular database source. These databases should

- Be relational.
- Use ANSI SQL.
- Package appropriate database drivers with the database platform.
- Be secured using industry-proven algorithms, techniques, platform-supplied infrastructure, and vendor-tested and supported technologies.
- Be backed up per the Backup of Electronic Records standards in AOSC19-23.
- Have a tested recovery plan.

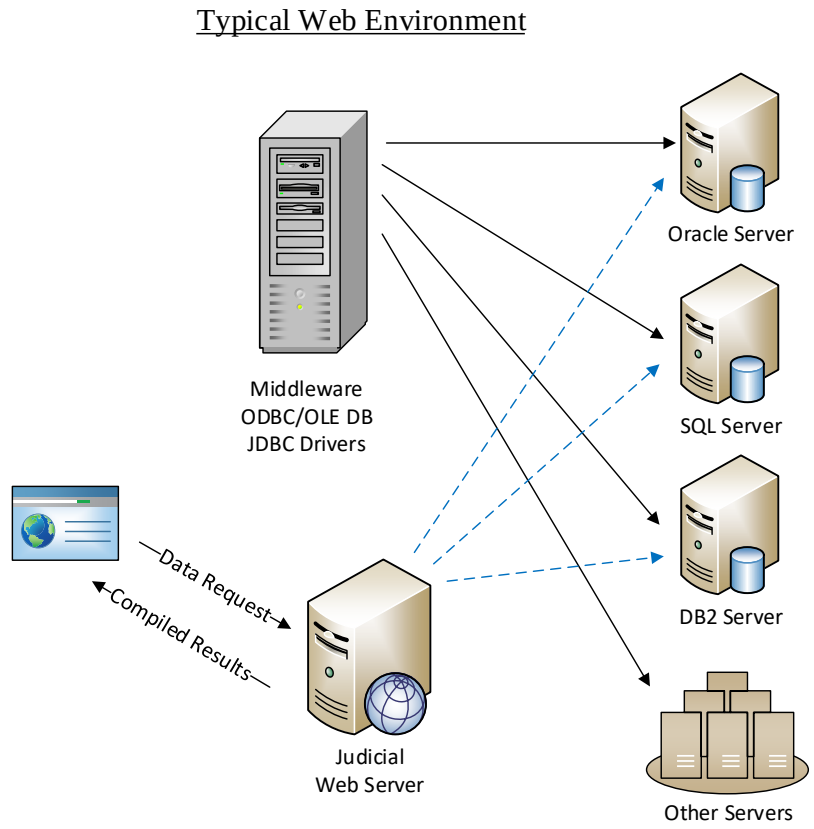
### 7.4.4 Database Connectivity

A detailed system architecture should be defined that will meet the business requirements of judicial applications. The system architecture should describe the structure and organization of the information systems supporting specific circuit/county/judicial location functions and provide the technical system specifications based on the functional requirements. It should describe the complete set of system and network infrastructure components that are installed or planned for installation. It should also include an approach to information sharing (database connectivity) and workflow coordination between business functions, external sources, and users of business information. Also, the architecture should define recommended drivers/middleware once the database and application development software for the system is finalized.

The communication technologies (database drivers) needed to allow transmittal and sharing of access to and utilization of information for various databases in the circuits may include:

- Open Database Connectivity (“ODBC”).
- Object Linking and Embedding (“OLE DB”).
- Java Database Connectivity (“JDBC”).
- Database Native Drivers.

*Figure 7. Conceptual Data Exchange Environment*




### 7.4.5 Archival Storage of Electronic Documents

Electronic document systems must accommodate the need to archive documents in a manner that will guarantee accurate reproduction of the original content in the present system as well as future systems and their storage format changes. Archival storage requirements of content must comply with the current records retention policy. Each system must consider and address the challenges of delivering documents seamlessly as changes occur over time. Archival storage formats used must be able to meet long-term rendering requirements as well as have a method to meet ADA requirements/accommodations. An industry-standard specifically developed for long-term archival purposes is PDF/A-2.

The Florida Supreme Court approved PDF/A-2 as the document storage format for electronic court documents in June 2019. AOSC19-23 outline the current document storage and backup of electronic records requirements.

## 7.5 CLOUD COMPUTING

There are unique opportunities and challenges with the advent of Cloud Computing. Cloud services are evolving at a fast pace that goes beyond file storage.

### 7.5.1 Approval Process

Due to the changing nature of cloud computing in the areas of storage and service offerings, moving to the cloud can be beneficial financially, but also carries many risks. Therefore, the chief judge shall be informed of benefits and potential risks and give approval before court records or court services are moved to a cloud service provider. Where applicable, cloud services must conform to CJIS standards.

### 7.5.2 Risks

One of the major risks with cloud computing involves the accessibility of data/services upon termination of the hosting agreement due to formatting or proprietary storage protocols implemented by the vendor. Care should be given to ensure the data is returned in the same format in which it was migrated. Security and integrity of the court data may be at risk when a contracted cloud service provider, who is also responsible for data security, is storing the data outside the monitoring capability of court/clerk staff. Care must be taken to ensure the security and integrity of court data and services. Security audits and reviews should be conducted preferably by an external, third-party entity. Security breaches should be properly and immediately reported to the Trial Court Administrator, Chief Judge, and the Chief Information Security Officer at the Office of the State Courts Administrator.

Because Service Level Agreements ("SLA's") can change often and with short notice, a plan must be in place to monitor and audit the impact that such changes to agreements could have and mitigate their impact.

### 7.5.3 Storage Restrictions

The location of cloud data storage is restricted based on the following classifications:

- Classification 1: Judicial Branch Records as defined in Florida Rules of Judicial Administration 2.420 (b)(1):
    1. Court Records
    2. Administrative Records
- Classification 2: Logs (e.g. temporary files such as computer activity logs, scheduling polls that are short-term files).

Data in both classifications must be available for a time period at least as long as the applicable records retention period by Florida law.

Data in classification 1 must reside within the United States. Data in classification 1 shall be encrypted, both in transit and at rest.

Data in classification 2 may be stored outside the United States, but the data must be stored in such a way as to facilitate copying of the data or a portion thereof in an amount of time

similar to the amount of time such duplication would take if the data were stored within the United States.

### 7.5.4 Data Encryption

Data encryption must be enabled for the storage of sensitive data in the cloud.

### 7.5.5 Best Practices

Best practices related to the security and integrity of data stored in the cloud should be followed either by practice (as identified in proposed cloud migration plans) or by contractual agreement. These include, but are not limited to:

- Any agreement should include a clause prohibiting the use of court data for any use without the express written consent of the governing jurisdiction.
- Any agreement should include a clause requiring law enforcement to work through the custodian of the record when requesting access to records rather than direct access.

### 7.5.6 Resources

- ISO 27018:2019 Compliant Cloud data privacy
- Security
  - Cloud Security Alliance: Cloud Control Matrix
  - PCI Security Standards
  - ISO/IEC 27001:2013
  - ISO/IEC 27002:2013
- Justice Partner Compliance
  - Criminal Justice Information Services (CJIS) compliance
  - Compliance with Justice Partner standards for current & future integrations
- Industry-verified conformity with global standards

# SECTION 8 DATA EXCHANGE

## 8.1 INTRODUCTION

The exchange of court data represents an extremely dynamic challenge for all involved. The demands of efficiency, timeliness, accuracy, and confidentiality combine to impose significant, often conflicting, demands on the exchange process. Traditionally, these challenges have been met locally with solutions targeted to the specific court data management system involved. However, if the court system is to keep pace with the evolving information age, a more global solution is required. The task of this specification is to define a sufficiently rigorous mechanism to standardize the transfer of data between two or more data systems while remaining flexible enough to tailor the exchange particulars required to the specific needs of those systems.

For purposes of this standard, interaction is being considered between the following entities:

- Clerks of court case maintenance/management systems and supporting systems (referred to as clerk CMS).
- Circuit court judicial viewer and/or Court Application Processing Systems (referred to as CAPS).
- State-level Judicial Data Management Services system (referred to as JDMS)

The decentralized nature of the relationships between county and circuit, circuit and state and county and state, and the variety of data management solutions deployed guarantees that the transfer of data between various entities within and outside of the court system is a complex matter. Multiple counties may maintain individual CMS's or may share the same CMS. Similarly, circuits may share a single CAPS among multiple counties within their jurisdiction or deploy individual CAPS as appropriate. Consequently, this standard must define a data transfer mechanism that satisfies the need to efficiently and effectively exchange data between court partners and that is independent of the complex relationships mentioned above while simultaneously guaranteeing the highest levels of security, resilience, and privacy of the data contained and shared among these systems.

However, it is not possible to compose a standard describing a limitless set of possible interactions. The intent of this standard is to define the mechanism by which a data transfer event is initiated and completed and to provide a description of the data package that is exchanged. It is not concerned with what must happen to a particular piece of data once it is received. Those details are left to the consuming system.

This Data Exchange Standard incorporates other existing, non-proprietary standards and specifications wherever possible. In particular, this standard has dependencies on the [ECF] (See Appendix A), [NIEM] (See Appendix A), [FIPS-180-2] (See Appendix B), and the World Wide Web Consortium (W3C) (See Appendix A). The terminology used in this standard to describe the components of the Data Exchange architecture conforms to a Service Oriented Architecture (SOA) (See Appendix B and C).

## 8.2 GOVERNANCE

Once the standard is approved, the Data Exchange Workgroup will schedule quarterly conference calls with at least one meeting in-person annually.

Changes to these standards must be approved by the Florida Courts Technology Commission ("FCTC") based on recommendations of the Data Exchange Workgroup before implementation. Requests for changes to these standards will be submitted to the Data Exchange Workgroup via the Office of the State Courts Administrator ("OSCA") and reviewed at the next scheduled meeting and a recommendation will be made to the FCTC.

Volusia County completed a pilot project testing the data exchanges. The documentation can be accessed at http://app02.clerk.org/menu/ccis/.

Nonconformance to these standards, once adopted, may be referred to the FCTC Compliance Subcommittee.

## 8.3 DATA EXCHANGE SECURITY

As noted in the Introduction section, version 1.0 of these standards will cover the exchange of data between local Case Maintenance Systems ("CMS"), Court Application Processing System ("CAPS") and state-level Judicial Data Management Services ("JDMS") systems and may include interactions with other state-level systems such as the Comprehensive Case Information System ("CCIS") as appropriate. Subsequent versions of this standard may expand upon and include data exchange between additional systems or stakeholders.

The Data Security Model should contain the following elements:

- Data Storage Encryption: All data stored electronically in locations other than those where the systems are located must also be encrypted, (e.g., an offsite backup facility). This also applies to any data extracted from the CMS with the intention of performing bulk transfers into other systems.
- Workstation Security: All end-user workstations or devices must maintain an up-to-date, industry-standard anti-malware system to protect the information being consumed by the end-user. This may be exempted only in the event that a business case has been developed showing that the end device cannot be kept current. In this event, the organization providing the data must be notified before the exchange.
- Mobile devices: No data may reside in mobile devices beyond the current session. If such a device is deployed or used for the "consumption" of information, a VPN solution must be deployed and managed by the courts.
- Cleaning Hard Disks: If at any moment a portable Hard Disk Drive or similar technology is used to transfer data among systems, the storage device must be sanitized using the DoD 5220.22-M approach.
- Firewalls: Firewalls are required when data must transport through an external network to reach its destination. This will be through a firewall specific source and destination (IP and port) defined in the firewall to prevent unintentional access to source/destination servers.

- User Credentials: When credentials (passwords) are necessary to access or transmit data among systems, the password should be a complex (upper, lower, numeric, and special character) combination password no shorter than 8 characters and renewable every 90 days. Provisions should be taken to deny the reuse of the previous 5 passwords.
- Security Updates: To mitigate vulnerabilities at the host and PC level, systems must have security updates applied frequently (preferably via automatic update); checks to ensure any system is not vulnerable should be performed before bringing it into production.

## 8.4 TRANSPORT

All data transport should be secured and encrypted in compliance with ECF 4.0.1, Section 5, Service Interaction Profiles, as augmented below. See Appendix B – [FIPS-180-2] and Appendix C).

- Data Exchange Protocol: Enhanced transport requirements shall be Secure HTTP (HTTPS) that consists of the standard HyperText Transfer Protocol (HTTP) layered on top of a secure Transport Level Security (TLS) session. To maximize security, any public-facing interface should be registered with a Certificate Authority ("CA); either a commercial service or maintained via the State Courts System. For the best security, 2048-bit (or more) key lengths should be used. For closed data center environments where communications occur between trusted servers, TCP may also be used (See Appendix A).
- Web Services: To ease implementation, the use of the Web Services Description Language ("WSDL") is strongly recommended, as it helps automate the creation of compliant interfaces for clients by providing a machine-readable description of the web service.

Data transport includes the transfer of data to the state and other repositories. For example, AOSC09-30, Statewide Standards for Electronic Access to the Courts, identifies the capability to transfer case and court activity data, both as single records and in bulk, to state-level data repositories as an essential capability of court data management systems. Transfers may be made for a wide variety of purposes including routine activity reporting, program and performance monitoring, resource allocation, court operations management, and data warehousing. The transfers may use a wide variety of data exchange scenarios, e.g., a data transfer initiated by a local data provider to a receiving state repository in response to changes within the underlying data being reported (event-push), or a transfer where the request originates from the repository to the local data management system (timed-pull). Consequently, the general web services capability established at either end of the data transfer should be capable of handling both types of transactions. The specific strategy, event-push or timed-pull, should be identified by the entity originating the transaction as part of the data request package definition.

It is recommended that data transfer occur using the lowest level, stable technology suitable for the task, in conformance to this standards document. However, it may be necessary to define alternate data transfer mechanisms, such as FTP or FTPS, in order to maintain compatibility with legacy reporting systems or when reporting is sufficiently short-term or is of such a nature as to

not justify the cost to develop a web services solution. The suitability of alternative transfer mechanisms should be determined by the entity originating the reporting requirement and approved by this standard's governing body.

While this data transfer standard is comprehensive, not all elements defined for a data request package may apply to a given exchange scenario. Since the data request may involve a large number of agencies, the entity originating the request should define a data transfer package description document detailing the format and content of the data being transferred and identifying the appropriate auditing and tracking elements as provided in this standard. This information may be included as part of the integration kit discussed below. If necessary, to ensure data transfer integrity, the service enabling the specific data transfer should provide for immediate, synchronous response to, for example, allow a service to initiate a transfer and the receiving service to signal success or failure of a transfer. (See Appendix C).

## 8.5 TRANSFER FRAMEWORK

The court system is adopting an enterprise standard for data management. Conformance to this standard requires the use of an SOA as the foundation for all data transfer. This approach views data exchange, not as a series of isolated data projects with each exchange subject to separate and unconnected rules. It is expected that data exchange projects can be built from a set of reusable modular components that can be mixed and matched as needed to provide the necessary functionality. The data exchange mechanism defined in this standard can serve as an architecture for data transfer in that the mechanism is capable of exchanging data between two endpoints.

The data transfer can be broken down into three types of information:

- Metadata describing the data being transferred.
- Sufficient tracking and auditing information to ensure reliable transmission, receipt, and messaging.
- The actual data to be transferred.

The integration toolkit discussed below will contain sufficient information to describe the data exchange. While some of the data needs can vary widely between jurisdictions, there are many types of common data exchanged, across all entities within the state. As specific data exchanges are defined, and appropriate integration kits built, it is planned that these standards will be expanded with a library of namespaces, XML Schemas, Major Design Elements (MDEs), and data dictionaries for common data exchanges (See Appendix C). This library will further help standardize data exchange within the court system and simplify the implementation of new exchanges across the state. Data Exchange Content Models will be developed to facilitate this standardization (See Appendix C and D.) In the context of web services, Major Design Elements (MDEs) is the conceptual representation of the exchange (See Appendix C) exposing a canonical set of core capabilities (See Appendix F). The Data Exchange architecture is divided into two principal elements:

- Core specifications that define the MIDEs and the operations and messages that are exchanged between the MDEs.

- Service Interaction Profiles (See Appendix C) are specifications that describe the communication infrastructures that deliver the messages between MDEs. Any Data Exchange MDEs will follow these two principal elements as formulated in the ECF 4.0.1 (or current) standard for data exchange. In addition, the data transfer framework components of:
    1. Meta description.
    2. Audit and tracking information.
    3. Data content is to be constrained through the use of namespaces and XML Schema Definition ("XSD") files.

Multiple namespaces can be included in one or more XML Schema Definition files that include all necessary constraints that are specific to the particular data transfer. The Data Exchange XML schemas are implementations of the data exchange content models (See Appendix C and D). They are the only normative representations of the messages.

## 8.6 INTEGRATION TOOLKIT

An integration toolkit should be provided for any implementation purposes. This toolkit consists of detailed documentation identifying:

- A plain language name for the integration toolkit.
- A Universally Unique Identifier (UUID) for the integration toolkit (mandatory element) – A UUID for the integration toolkit as agreed upon by the entities involved.
- A UUID for other existing or new data exchange specifications – This UUID allows versioning of the specification and promotes controlled upgrades and modifications between different data systems.
- A clear plain language description of the contents of the data being transferred including appropriate references to specifications if necessary.
- Example XML requests and responses, data dictionary (including the detailed description/format of each data element or attribute), references to appropriate business rules, relevant standards and definitions, XML schema definition files, theory of operation, Major Design Elements – (MDEs, and sample usage cases for each MDE (See Appendix C).

## 8.7 CONFORMANCE

Conformance to this standard does not apply to existing systems that are technically incapable, or it is cost-prohibitive to conforming to this standard and data exchanges.

# SECTION 9 GENERAL TECHNOLOGY

## 9.1 ADA AND TECHNOLOGY COMPLIANCE

Accessibility standards for electronic and information technology are covered by federal law, known as Section 508 of the Rehabilitation Act of 1973 (as amended), which lists standards necessary to make electronic and information technology accessible to persons with disabilities. These standards, together with the requirements of the Americans with Disabilities Act and Florida law, must be met. References to these requirements throughout this document will be noted as "Section 508, Florida law and the ADA".

All technology and information used to support the creation of an electronic case file and to provide access to court records will comply with statutes (federal and state), court rule, Administrative Order issued by the Supreme Court, court technology standards, and the Florida AeIT Bill [Accessible Electronic and Information Technology], s. 282.601-282.606. Fla. Stat.

Additionally, all technology applications submitted for approval include a "Statement of Accessibility/Certification."

A list of references regarding understanding the requirements of Section 508, Florida law and the ADA can be found in Appendix A to this part.

- Chapters 282.601-282.606, Fla. Stat.– The Florida Accessible Electronic and Information Technology Act
- Section 508 of the Rehabilitation Act of 1973 (as amended) – United States Federal Access Board: Electronic & Information Technology Accessibility Standards (http://www.access-board.gov/gs.htm)
- The Americans with Disabilities Act of 1990 (ADA)
- Florida Rules of Judicial Administration

Other reference sources of information may include:

- World Wide Web Consortium (W3C) Web Access Initiative Guidelines (http://www.w3.org/)
- ADA Best Practices Tool Kit for State and Local Governments – Chapter 5, Website accessibility Under Title II of the ADA: http://www.ada.gov/pcatoolkit/chap5toolkit.htm
- Section 508

## 9.2 REDACTION AND ADA COMPLIANCE

Redacted copies of electronic court documents are not required to retain the original document intelligence. These copies may be flattened to accommodate existing redaction workflow processes.

Custodians of electronic court documents are not responsible for adding ADA-compliance features to documents that they did not originate. However, custodians are required to follow acceptable ADA practices for access to court documents.

## 9.3 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.

## 9.4 ARCHIVAL REQUIREMENTS

Electronic records must be archived in a manner that protects the records from degradation, loss of content, or issues with software compatibility relative to the proper rendering of electronic records and in compliance with applicable law or Supreme Court guidelines.

## 9.5 BACKUP OF ELECTRONIC COURT RECORDS

Electronic court records custodians are responsible for the security, availability, and integrity of electronic court records (images and data) under their care. Custodians shall ensure that:

- Electronic court records in their care are securely backed-up and any backup data stored at a third-party location must also be encrypted. The custodian of the electronic court records shall have exclusive access to the encryption key. In instances where vendors are supporting appliances onsite and are required to maintain an encryption key, the custodian will have operational policies and procedures that serve as a control prohibiting vendor access without invitation and monitoring.
- The production data or backup copy will reside in a hardened (CAT 5) facility. If a hardened (CAT 5) facility is unavailable, a tertiary copy (redundant backup) will also be maintained in its own off-site, independent facility. The production electronic court records and at least one copy of the backup(s) shall not be housed in the same building.
- Agreements with third-party offsite vendors acknowledge the confidentiality of electronic court data they store and prohibit data mining and other access/use of the data for any purpose other than to make the data accessible to the custodian.
- All backup copies of court data must be readily available to the custodian for access and restoration.
- Random sample testing is performed annually to verify that data is accessible and recoverable.
- Any known breach, or other malicious events, is reported to the chief judge or his/her designee and the Chief Information Security Officer at the Office of the State Courts Administrator Office of Information Technology as part of the custodian's Computer Security Incident Response plan.
- All court backup data is stored in the United States.
- Physical and electronic data transfer processes conform to the confidentiality and security guidelines outlined in the Data Exchange Standards.

These standards are minimum standards. If a custodian stores court-related data from another jurisdiction or agency with stricter requirements, the custodian must comply with the stricter standards for that data.

## 9.6 COURT CONTROL OF COURT DOCUMENTS – DATA STORAGE

The production data or backup copy will reside in a hardened (CAT 5) facility. If a hardened (CAT 5) facility is unavailable, a tertiary copy (redundant backup) will also be maintained in its own offsite, independent facility. The production electronic court records and at least one copy of the backup(s) shall not be housed in the same building. All court backup data is stored in the United States. See Section 9.5, Backup of Electronic Court Records Standards for additional information.

## 9.7 DOCUMENT STORAGE FORMAT

Electronic court records custodians are responsible for the storage, processing, and accessibility of electronic court documents. Custodians shall ensure that:

- Electronic documents that are part of a court file (i.e., the record copy) are stored in the PDF/A format.
    1. This is a day-forward requirement.
    2. Upon implementation of the PDF/A requirement for incoming filings, existing electronic documents may remain in their current format(s) if the clerk CMS is capable of managing multiple file formats.
- The record copy of each electronic court document retains the original document intelligence (i.e., as filed with the Portal) except features that use a digital hash. For example, digital signatures and electronic notarizations may be flattened and the certificates invalidated as the document moves through the filing process.

# SECTION 10 NOTIFICATION BY CLERK OF SYSTEM MODIFICATION

| CONTACT INFORMATION | | | | | |
|---|---|---|---|---|---|
| Contact Person Name | | | Contact Person Phone | | |
| Contact Person E-mail | | | Agency Name | | |
| County | | Circuit | | Appellate | |
| Application Developer Name (Provide vendor name or designate In House) | | | | | |

| CHANGE INFORMATION | |
|---|---|
| Type of Change | ☐New Implementation ☐System Modification |
| Criticality of Change | ☐High ☐Medium ☐Low |
| Change Title | |
| Description of Change | |
| Justification for Change | |

| | |
|---|---|
| Effect of not implementing the change | |
| User Group(s) affected by the change | |
| Does the change affect the judiciary? | ☐Yes ☐No<br>If yes, has the change been approved by the chief judge or his/her designee? |
| Will the change require modifications to existing operating systems, databases, web services, or other system components? | ☐Yes ☐No<br>If yes, please describe how. |
| Will the change introduce new technology or tools? | ☐Yes ☐No |

| | |
|---|---|
| | If yes, please describe how. |
| Proposed schedule for the change | |

E-mail completed form to Lakisha Hall at halll@flcourts.org

# APPENDIX A. SYMBOLS AND ABBREVIATIONS

**CAPS**

Court Application Processing System

**CMS**

Case Maintenance System

**ECF**

Electronic Court Filing

**FCTC**

Florida Courts Technology Commission

**JDMS**

Judicial Data Management Services

**IEPD**

Information Exchange Package Documentation

**MDE**

Major Design Element

**NIEM**

National Information Exchange Model

**OASIS**

Organization for the Advancement of Structured Information Standards, *a non-profit consortium for open standards*

**OCR**

Optical Character Recognition

**PDF**

Portable Document Format

**PDF/A**

Portable Document Format/Archival

**SOAP**

Simple Object Access Protocol

**TCP**

Transmission Control Protocol

**XML**

eXtensible Markup Language

**W3C**

World Wide Web Consortium

**WSDL**

Web Services Description Language

**WS-I**

Web Services Interoperability Organization

# APPENDIX B. NORMATIVE REFERENCES


**[ECF Specification]**

*Electronic Court Filing Version 4.01, https://www.oasis-open.org/standards/, OASIS, May 2013.*

**[FIPS 180-2]**

*Secure Hash Standard*, http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf, National Institute for Standards and Technology, August 2002.

**[Genericode]**

A. B. Coates, *Code List Representation (Genericode) 1.0*, http://docs.oasisopen.org/codelist/ns/genericode/1.0/, OASIS Committee Specification, December 28, 2007

**[NIEM]**

*National Information Exchange Model 2.0*, http://niem.gov, US DOJ and DHS, 2007.

**[NIEM Guide]**

*NIEM Implementation Guidelines*, http://www.niem.gov/implementationguide.php, US DOJ and DHS, 2007.

**[NIEM Techniques]**

*Techniques for Building and Extending NIEM***,** http://www.niem.gov/topicIndex.php?topic=techPDF, Georgia Tech Research Institute, August 2007.

**[Namespaces]**

T. Bray, *Namespaces in XML*, http://www.w3.org/TR/1999/REC-xml-names-19990114, January 14, 1999.

**[RFC2046]**

N. Freed, *Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types*, http://www.ietf.org/rfc/rfc2046.txt, IETF RFC 2046, November 1996.

**[RFC2119]**

S. Bradner, *Key words for use in RFCs to Indicate Requirement Levels*, http://www.ietf.org/rfc/rfc2119.txt, IETF RFC 2119, March 1997.

**[RFC4122]**

Leach, et al., *A Universally Unique IDentifier (UUID) URN Namespace*, http://www.ietf.org/rfc/rfc4122.txt, IETF RFC 4112, July 2005.

**[Schema Part 1]**

H. S. Thompson, D. Beech. M. Maloney, N. Mendelsohn, *XML Schema Part 1: Structures Second Edition*, http://www.w3.org/TR/2004/REC-xmlschema-1-20041028/, W3C Recommendation, October 28, 2004.

**[Schema Part 2]**

P. Biron, A. Malhotra, *XML Schema Part 2: Datatypes Second Edition*, http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/, W3C Recommendation, October 28, 2004

**[SOA-RM]**

MacKenzie, et al., *Reference Model for Service Oriented Architecture 1.0*, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm, OASIS Public Review Draft 1.0, February 10, 2006.

**[UBL]**

*Universal Business Language Version 2.1 30 May 2011*. 30 May 2011. Committee Specification Draft 02 / Public Review Draft 02. http://docs.oasisopen.org/ubl/prd2-UBL-2.1/UBL-2.1.html J. Bozak, T. McGrath, G. K. Holman (editors), *Universal Business Language 2.0*, OASIS Standard, December 12, 2006.

**[XML 1.0]**

T. Bray, *Extensible Markup Language (XML) 1.0 (Third Edition)*, http://www.w3.org/TR/REC-xml/REC-XML-20040204, W3C Recommendation, February 4, 2004.

**[XMLENC]**

D. Eastlake, J. Reagle, *XML Encryption Syntax and Processing*, http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/, W3C Recommendation, December 2002

# APPENDIX C. TERMS AND DEFINITIONS

**Annotation**

A note that is added to a document by the creator. Annotations can be easily hidden and moved, possibly affecting the content of the document.

**Asynchronous Response**

A message transmission returned at some time interval after the end of an operation, i.e., there is no immediate (synchronized) response between the communicating endpoints. Asynchronous transmissions use data flow parameters as opposed to synchronous transmissions that use a clock signal to keep the data flow synchronized. (See the terms Message and Message Transmission).

**Attachment**

Information transmitted between MDEs that is of an arbitrary format and is related to the message(s) in the transmission in a manner defined in the standard. An attachment may be in XML format, non-XML text format, encoded binary format, or un-encoded binary format. (See the terms Message and Major Design Element (MDE)).

**Bookmark**

A link connecting to a specific target in a document. Bookmarks usually indicate the document structure, but may also include sensitive words and phrases.

**Callback message**

A message transmission returned by some operations sometime after the operation was invoked (asynchronously). (See the terms Message and Message Transmission).

**Case Maintenance System (CMS)**

An electronic system used by Clerks to perform their court-related statutory duties, to include the major business functions outlined in the Consolidated Case Maintenance System Standards.

**Case Management**

A systematic administration and allocation of resources, including judicial attention and leadership, time, court staff, court technology, and the resources or parties and communities, directed to enhancement of the quality, timeliness, and efficiency of the judicial system. Case management develops and maintains reasonable and achievable policies and practices, identifies, collects and organizes critical case information, responds appropriately to characteristics of cases and parties, organizes the movement of cases, ensures that necessary activities and events occur, marshals and prioritizes court and community resources, promotes reasonable and consistent expectations, provides critical information to judicial leaders and court managers, and promotes accountability and ongoing improvement (TCP&A, 2001).

**Content Model**

Describes the information components used in the messages defined and how the information is organized. The data exchange content models will be the result of a detailed analysis of the data requirements to support the particular data exchange.

**Core Messages**

Defined by the core specifications which define the MDEs and the operations and messages that are exchanged between MDEs. These are required messages for the particular MDEs. (See the terms Message and Major Design Element (MDE)).

**Court Application Processing System (CAPS)**

A computer application designed for in-court and in-chambers use by trial judges, their staff, and Court Administration personnel to access and use electronic case files and other data sources in the course of managing cases, scheduling and conducting hearings, adjudicating disputed issues, and recording and reporting judicial activity.

**Data Element**

Required information identified by rule, statute, forms, and any other pertinent information describing the activity of the court system either organizationally or in relation to activity within a specific court division.

**Digital Signature**

A specific type of electronic signature created using a mathematical algorithm (e.g., encrypted hash value) routinely used to validate the authenticity of a signer's identity creating a virtual fingerprint that is unique to a person and the integrity that the message has not been altered.

**Docketing**

The process invoked when a court receives a pleading, order, or notice, with no errors in transmission or in the presentation of required content and records it as a part of the official record. (See the term Progress Docket).

**Docket Number**

An alphanumeric number used by the clerks to identify a specific entry in a case docket.

**Document Intelligence**

Information and metadata that is created during the lifecycle of a document. This includes viewable text, appearance, and hidden information such as document identifiers, tags such as those used to make the document ADA compliant, and other metadata.

**Dots Per Inch (DPI)**

The measure of spatial printing, video or image scanner dot density, in particular the number of individual dots that can be placed in a line within the span of one (1) inch.

**E-Filing Portal (Portal)**

The central electronic court filing facility that accepts court documents for filing in Florida courts, transmits them to the clerks, and can effectuate automated service via e-mail upon all registered attorneys and parties associated with a case.

**Electronic Filing**

The automated transmission of legal documents from an attorney, party, or self-represented litigant to a court.

**Electronic Filing Envelope**

Data accompanying submitted documents which identify a submitted document, the filing party, and other sufficient information for entry in the court's docket or register of actions.

**Electronic Notarization**

A process whereby a notary affixes an electronic signature and notary seal using a secure public key to an electronic document.

**Electronic Signature**

A digitized signature that shows intent to sign a document. Acceptable electronic signature formats include “s/”, “/s”, or “/s/”.

**Encryption**

The process of converting information or data into a form that is unintelligible to prevent unauthorized access.

**Encryption Key**

A random string of bits generated specifically to scramble and unscramble data to ensure that every key is unpredictable and unique.

**Exhibits**

Documentary evidence.

**File Format**

A file representation of a document (e.g., Word, PDF, PDF/A).

**Filer**

Any person who files a document into a court record, excluding the clerk of court or designee of the clerk, a judge, magistrate, hearing officer, or designee of a judge, magistrate, or hearing officer.

**Flatten**

Removing original document intelligence.

**Framework**

A conceptual description of the components and other elements from which a working system can be built. A framework defines the boundaries of the system to be built and may constrain the operation of the components within. Depending on design considerations, the description of each component or element will vary in detail as necessary to clearly set boundaries and ensure the components work properly together.

**Gatekeeper**

An employee of an agency who adds, updates, and deletes user or agency information.

**Hyperlink**

An icon, graphic, or text that points to a specific document or a specific element within a document.

**Institutional Access**

Applies to roles of the Office of Public Defender and the Office of Criminal Conflict and Civil Regional Counsel in cases where they are appointed or are the presumptive attorney of record. Institutional users, including paralegals, legal assistants, and other staff are allowed to view assigned cases as if they were the "attorney of record."

**Major Design Element (MDE)**

A logical grouping of operations representing a significant business process supported by the standard. Each MDE operation receives one or more messages, returns a synchronous response message, and optionally sends an asynchronous response message back to the original sender. (See the terms Message and Synchronous Response).

**Message**

Information transmitted between MDEs that consists of a well-formed XML document that is valid against one of the defined message structure XML schemas. A message may be related to one or more attachments in a manner defined in the standard. (See the term Attachment).

**Message Transmission**

The sending of one or more messages and associated attachments to an MDE. (See the terms Attachment and Message). Each transmission must invoke or respond to an operation on the receiving MDE, as defined in the standard. (See Receiving MDE).

**Metadata**

Data that describes or gives information about other data.

**Operation (or MDE Operation)**

A function provided by an MDE upon receipt of one or more messages. The function provided by the operation represents a significant step in the business process. A sender invokes an operation on an MDE by transmitting a set of messages to that MDE, addressed to that operation. An operation will have an operation signature. (See the terms Message, Operation Signature, and Major Design Element (MDE)).

**Operation Signature**

A definition of the input message(s) and synchronous response message associated with an operation. Each message is given a name and a type by the operation. The type is defined by a single one of the message structures defined. (See the terms Message and Synchronous Response).

**Optical Character Recognition (OCR)**

The electronic conversion of typed, hand-written, or printed text into a digital format using photoelectronic devices and computer software so the text can be edited or searched.

**Progress Docket**

A list of each pleading, motion, or other paper and any steps taken by the clerk in connection with each action, appeal, or other proceedings before the court. (See the term Docketing).

**Proposed Order**

Draft of an order prepared by a party/parties for review and/or consideration by the court.

**Rasterize**

Converting an image into pixels to print, display, or store the image in a bitmap file format.

**Receiving MDE**

The MDE that receives the request with the operation invocation performs the operation and sends the response. (See the terms Major Design Element (MDE) and Operation).

**Redaction**

Permanently remove information from the document that is identifying or otherwise sensitive.

**Scanning**

The process of converting a paper document or picture into a digital copy using a device (e.g., scanner, phone, tablet) that has a camera or document scanner that uses charge-coupled or contact image technology. (See the terms OCR and DPI).

**Searchable PDF**

A PDF that contains a bitmapped image of a document with textual content that can be searched.

**Sending MDE**

The MDE that sends the request including the operation invocation and receives the response with the results of the operation. (See the terms Major Design Element (MDE) and Operation).

**Service Interaction Profiles**

Specifications that describe communication infrastructures that deliver messages between MDEs. (See the terms Message and Major Design Element (MDE)).

**Service-Oriented Architecture**

A design pattern based on distinct pieces of software providing application functionality as services to other applications via a protocol. It is independent of any vendor, product, or technology. The W3C defines it as a set of components that can be invoked and whose interface descriptions can be published and discovered.

**Synchronous Response**

A message transmission returned immediately (synchronously) as the result of an operation. Every operation has a synchronous response. (See the terms Message and Message Transmission).

**Viewable on Request (VOR)**

A public document with a high probability of containing confidential information, protected by an additional layer of security, requiring additional review by a clerk of court employee for the redaction of confidential information. Once a VOR has been requested and reviewed, a copy of

the document is updated to a public status and is made publicly available, electronically, or in person.

# APPENDIX D. DATA EXCHANGE CONTENT MODELS

Data exchange content models describe the information components used in all of the messages defined (See the term Message in Appendix C). The data exchange content models will be the result of a detailed analysis of the data requirements to support the particular data exchange. During the modeling process, common items of data will be identified by a process of normalization to identify aggregates based on functional dependency. Where appropriate, these will be generalized so that they can be re-used to support the various messages. The data exchange content models will be used for the following purposes:

- Facilitate the identification of the reusable components, i.e., the data structures that are common across the Data Exchange messages (See Appendix E).
- Aid in understanding the information requirements of the total scenario.
- The source from which the object classes are derived and documented in the Data Exchange XML Schemas (See the normative references for Schema Part 1 and Schema Part 2 in Appendix B).

To facilitate comprehension, several particular data exchange content model diagrams will be developed. Each diagram will represent a logical grouping of components and display both the attributes and object classes belonging to the components in the grouping. The scope of each diagram will be arbitrary and will not hold any significance beyond the diagrams.

# APPENDIX E. DATA EXCHANGE MESSAGES

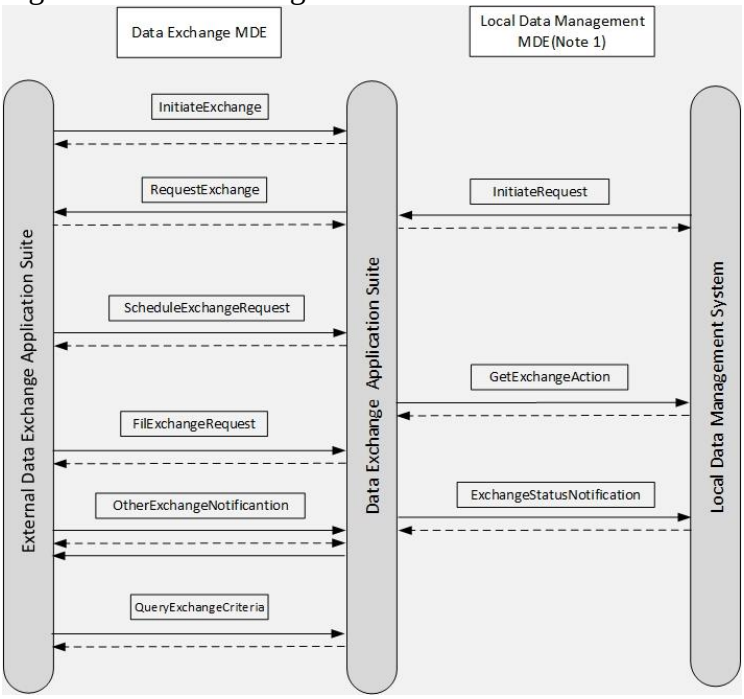
The key principles that shall guide the design of the Data Exchange message (see the term Message in Appendix C) structures are:

- Interoperability: The Data Exchange message structures shall provide a means for exchanging data among all types of court information systems.
- Completeness: The Data Exchange message structure format shall provide for all the elements for the particular data exchange.
- Simple implementation: The design should foster rapid implementation.
- Simple XML and portable structure: The core messages in a data exchange will be formatted as XML documents (See Appendix C).
- Familiarity: The data elements and code values shall be meaningful.
- Interdisciplinary utility: The design should be usable by a broad range of court-related applications.

# APPENDIX F. DATA EXCHANGE CAPABILITY MODEL

This data exchange standard advances a common set of exchange capabilities that should be built upon to define a specific data exchange. The below general methods describe a minimal set of capabilities that each exchange must implement. However, implementation details are left to the individual exchange which need not define methods with these specific names. Refer to Figure 8. for a representative diagram.

Figure 8. Data Exchange MDE Reference




**InitiateExchange**
The Data Exchange MDE must allow for an external data source to initiate data exchange at any time. The initiation action for this method includes the direct transfer of data from the external data source to the Data Exchange MDE as part of the Initiate Exchange message. The Data Exchange MDE must respond synchronously with a message denoting receipt of the data or failure of the transfer. Failure messages must include a reason for failure if such a reason is identifiable by the Data Exchange MDE.

**RequestExchange**
The Data Exchange MDE may request an exchange of data from another Data Exchange MDE. The receiving MDE must respond synchronously with the data requested, an error message, or by invoking the ScheduleExchangeRequest operation on the consuming Data Exchange MDE to schedule a date/time when the request will be filled. The RequestExchange message must include a unique identifier for the request that must be used through subsequent operations.

**ScheduleExchangeRequest**
The Data Exchange MDE may satisfy a RequestExchange action by scheduling a date and time when the requested data will be provided. Messages must use the unique identifier established during the original RequestExchange operation.

**FillExchangeRequest**
The Data Exchange MDE must resolve a ScheduleExchangeRequest operation by providing the data originally requested by invoking the FillExhangeRequest operation on the requesting Data Exchange MDE. The FillExchangeRequest must use the unique identifier associated with the original RequestExchange operation. The message must contain the data requested. The Data

Exchange MDE must respond synchronously with a message denoting receipt of data or failure of the transfer. Failure messages must include a reason for failure if such a reason is identifiable by the Data Exchange MDE.

**OtherExchangeNotification**
The Data Exchange MDE must define a capability to establish arbitrary data exchanges. The complexity of court data exchange will necessitate specialized exchanges between local data providers. The OtherExchangeNotification operation should provide a mechanism for meeting this local exchange need through the appropriate message namespaces while remaining compliant with this specification.

**QueryExchangeCriteria**
A Local Data Exchange MDE may obtain the necessary exchange criteria parameters from a Data Exchange MDE by invoking the QueryExchangeCriteria operation. The invocation of the QueryExchangeCriteria must include a specific exchange UUID for which to receive criteria as the exchange of different data products may impose different limitations. The Data Exchange MDE returns a machine-readable WSDL describing specific limitations associated.

The following methods should not be exposed for general consumption. They are intended to provide management capabilities to local and/or internal data management systems authorized to interact with a specific instance of a Data Exchange MDE. In particular, the implementation details of the Local Data Management MDE is left to the specific jurisdiction. While it is expected that the accepted method of interaction with the Data Exchange MDE is via a web services protocol, the interaction between the Local Data Management MDE need not be constructed as a web service. This element of the diagram intends to illustrate the functionality that the Data Exchange MDE needs to define. For example, the Data Exchange MDE must have the functionality to enable a local, authorized data management system to initiate a request for data via the Data Exchange MDE. However, while the request for data may be accomplished via web services, the initiation could be accomplished by different means such as another web service, a locally defined message queue, or even a simple set of scheduled jobs.

**InitiateRequest**
The Local Data Management MDE may invoke this operation on the Data Exchange MDE to retrieve data from an external data provider. The Data Exchange MDE must respond synchronously reporting the date/time that the data was requested (via the RequestExchange operation) and the unique identifier for the request. The Data Exchange MDE must respond asynchronously with the requested data, the date/time the data is scheduled to be provided, or an error message indicating failure of the data transfer.

**GetExchangeAction**
The Data Exchange MDE may invoke the GetExchangeAction on the local data management MDE if that system provides for it. The Local Data Management MDE must respond synchronously with a method, location, or mechanism to store or process the data received from the Data Exchange MDE.

**ExchangeStatusNotification**
The Data Exchange MDE must define a capability to exchange status and other relevant information with the Local Data Management MDE through appropriate messages and namespaces.