Supreme Court of Florida

No. AOSC18-16

IN RE: ACCESS TO ELECTRONIC COURT RECORDS

ADMINISTRATIVE ORDER

The Florida State Courts System strives to promote public trust and confidence in the judicial branch by delivering timely, consistent, and useful information through traditional and innovative communication methods and safeguarding the security, integrity, and confidentiality of court data.

In re: Standards for Access to Electronic Court Records, Fla. Admin. Order No. AOSC14-19 (amended May 23, 2014), governs appropriate, differentiated levels of access to electronic court records and prescribes a process by which a clerk of court who wishes to provide court records online must develop and test in a pilot program its online electronic records access system and, when it demonstrates through such pilot program compliance with the Standards for Access to Electronic Court Records and the Access Security Matrix adopted by the Supreme Court, seek Supreme Court approval to provide online access to electronic court records. The clerks of court for three counties have completed the

pilot program and are seeking approval to provide online access to electronic court records.

Through AOSC14-19, the Supreme Court adopted the standards and the security matrix and subsequently amended the standards and security matrix in succeeding administrative orders. The Florida Courts Technology Commission (Commission) has recommended additional amendments to the standards and the security matrix.

NOW, THEREFORE, the Supreme Court takes the following actions.

Approval of Clerk of Court Requests

The clerks of court for Brevard, Monroe, and Wakulla counties have engaged in a pilot program for at least 90 days to test its online electronic records access system; submitted at least three monthly status reports to the Office of the State Courts Administrator; reported all incidents of inadvertent release and unauthorized access to confidential information, if any occurred; took the appropriate corrective actions necessary to address all reported incidents related to confidential information; and ensured compliance with the current version of the standards and security matrix.

In addition, each clerk of court submitted a certification request, consistent with AOSC14-19, and a written description of the steps, processes, or tools used to validate compliance with the standards and the security matrix. The Access

Governance Board (Board) of the Commission reviewed each request and recommended approval, and the Commission concurred with the recommendation of the Board.

Accordingly, the requests to provide online access to electronic court records submitted by Brevard, Monroe, and Wakulla clerks of court are hereby approved, subject to the following terms and conditions:

1. Within 90 days following the date of this order, each clerk of court must implement its online electronic records access system in accordance with the standards and the security matrix adopted by AOSC14-19 and amended by AOSC17-47.
2. Each clerk shall incorporate any future amendments or updates to the standards and security matrix into the clerk's existing online electronic records access system.
3. To ensure compliance with the standards or security matrix, each clerk of court shall provide the Supreme Court or its designee access accounts for all roles in the security matrix, if so requested.

Violation of any of these terms and conditions shall constitute grounds for revocation of the approval to implement online electronic records access in the respective county.

Amendments to the Access Security Matrix and the Standards for Access to Electronic Court Records

The Board received a request from the Florida Court Clerks & Comptrollers Technology Group to update the security matrix relating to mental health cases. Several mental health cases were excluded from the security matrix; thus, no security roles were attached. Based on statute, the Board modified the security matrix by adding Professional Guardian; Mental Health Miscellaneous; Substance Abuse Assessment/Treatment; and Tuberculosis/STD Treatment/Other Confidential case types. These updates also incorporate the changes made by Fla. R. Jud. Admin. 2.420(d)(1)(B), which includes new exemptions to public records law for non-court records that the clerks of court are required to protect.

A Realigning of the Standards and Matrix Workgroup was created to revise and edit the standards and security matrix to ensure the documents complement one another. Previously in the standards, several user roles were lumped into similar categories by statutory citations for access to specific types of records; a few user roles denoted rules and statutes that did not grant access to that specific role; and the default view for judges was the non-redacted version of the record. In the new version of the standards, the user roles are separated and renamed to be synonymous to those in the security matrix; relevant rules and statutes have been added to indicate access and certain rules and statutes are more specific as they relate to the user role, rules and statutes that did not grant access to specific user

roles have been removed; the Administrative user role has been deleted to eliminate ambiguity between an administrator and a gatekeeper; a gatekeeper is defined; the User Maintenance section is updated to allow clerks who currently use an online process to register users to use their online electronic records access system as opposed to registered user agreements; and the requirement for the default view for judges to see the non-redacted version of the record has been removed.

In accordance with its authority under Florida Rule of Judicial Administration 2.236 to "establish, periodically review, and update technical standards for technology used and to be used in the judicial branch to receive, manage, maintain, use, secure, and distribute court records by electronic means, consistent with the technology policies established by the supreme court," the Commission concurred with the Board's recommendations and submitted amended standards and an amended matrix for the Court's consideration.

As a means for the judicial branch to continue to ensure responsible access to electronic court records, the Court hereby adopts the amended Standards for Access to Electronic Court Records and the amended Access Security Matrix to

supersede those previously adopted. The amended standards and matrix are attached hereto and incorporated herein by reference.[1]

DONE AND ORDERED at Tallahassee, Florida, on June 21, 2018.

AOSC18-16 6/21/2018

Chief Justice Jorge Labarga

AOSC18-16 6/21/2018

ATTEST:

AOSC18-16 6/21/2018

John A. Tomasino, Clerk of Court

AOSC18-16 6/21/2018

1. The Standards for Access to Electronic Court Records and the Access Security Matrix are also available on the Florida Courts website. See http://www.flcourts.org/resources-and-services/court-technology/technology-standards.stml.

Standards for Access to Electronic Court Records

April 2018

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, which governs remote web-based and clerks' office access to electronic court records.

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.

ACCESS SECURITY MATRIX

The Access Security Matrix (the "Matrix") appended to these standards 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 (the "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.

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 sworn agreement is required or 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.

GATEKEEPER

In an effort to effectively manage access and ensure security, an agency may utilize a 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 duty imposed upon the gatekeeper by the Board.

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 rule 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 Judges and authorized court and clerk's office personnel	All court records, except those expunged pursuant to s. 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 performance of their official duties. Access to records sealed pursuant to s. 943.059(4), F.S., is permitted for judges to assist in 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 Florida State Attorneys' Offices	All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order. Access to Social Security numbers by ss. 119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to HIV test results as permitted by s. 381.004(5)(c), F.S. Access to sexually transmitted disease results as permitted by s. 384.29(1), F.S. Access to birth certificates as permitted by ss. 382.013(5) and 382.025(1)(a)5, F.S. Access to mental health records as permitted by ss. 394.4615(3)(b), 394.4655(3)4)(c), and F.S. Access to identities of victims of sexual and child abuse when originating from law enforcement as permitted by s. 119.0714(1)(h), F.S. Access to children and families in need of services records as permitted by s. 984.06(3), F.S. Access to juvenile records as permitted by ss. 39.0132(4)(a)(1) and 985.04(1)(b), F.S.	Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list. Each state attorney must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in performance of their official duties.

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
User Role 3 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), or made confidential by court order, depending upon the type of case and the language of the court order.	Secure access through user name and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list.
User Role 4 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), or made confidential by court order, depending upon case type and the language of the order.	Secure access on case-by-case basis. Access by notarized request to insure identity of party.
User Role 5 Public in Clerks' offices and registered users	All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order. 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, pursuant to s. 28.2221(5)(a), F.S.	Secure access through user name and password by written notarized agreement or in person at Clerks' offices.
User Role 6 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. Access to social security numbers as permitted by ss. 119.071(5)(a)6.b. and 119.0714(1)(i), F.S.	Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list. <u>Each agency must establish policies to ensure that access to confidential records and information is</u>

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
		limited to those individuals who require access in performance of their official duties.
User Role 7 General public (without registration agreement)	All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order. 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, pursuant to s. 28.2221(5)(a), F.S.	None. Anonymous web-based access permitted.
User Role 8 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. Access to social security numbers as permitted by ss. 119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to HIV test results as permitted by ss. 381.004(2)(e), and 951.27 F.S. Access to sexually transmitted disease results as permitted by s. 384.29(1), F.S. Access to birth certificates as permitted by ss. 382.013(5) and 382.025(1)(a)5., F.S. Access to identities of victims of sexual and child abuse when	Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining an authorized user list. Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in performance of their official duties.

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
	originating from law enforcement as permitted by s. 119.0714(1)(h), F.S. Access to children and families in need of services records as permitted by s. 984.06(3), F.S. Access to juvenile records as permitted by ss. 39.0132(4)(a)(1) and 985.04(1)(b), F.S.	
User Role 9 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. Access to social security numbers as permitted by ss. 119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to birth certificates as permitted by ss. 382.013(5) and 382.025(1)(a)5., F.S. Access to children and families in need of services records as permitted by s. 984.06(3), F.S. Access to juvenile records as permitted by ss. 39.0132(4)(a)(1) and 985.04(1)(b), F.S.	Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list. Each agency must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in performance of their official duties.

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
User Role 10 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. Access to social security numbers as permitted by ss. 119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to juvenile delinquency records as permitted by s. 985.04(1)(b), F.S.	Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list. Each school district must establish policies to ensure that access to confidential records and information is limited to those individuals who require access in performance of their official duties.
User Role 11 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. 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, pursuant to s. 28.2221(5)(a), F.S.	Secure access through user name and password by written notarized agreement. Commercial purchaser gatekeeper is responsible for maintaining an authorized user list.
User Role 12 Florida Public Defenders' Offices (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. The Office of the Public Defender is considered the	Secure access through user name and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list. Each public defender must establish 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
	attorney of record at a defendant's first appearance as permitted by s. 985.045(2) and rules 8.010 and 8.165, Fla. R. Juv. P. for juvenile defendants and s. 27.51 and rule 3.130, Fla. R. Crim. P. for adult defendants. Access will be changed to User Role 6 when the public defender is no longer the attorney of record or another attorney is assigned.	performance of their official duties.

ACCESS LEVELS

Access levels are defined as follows:

A. All but expunged, or sealed under Ch. 943;
B. All but expunged, or sealed under Ch. 943, or sealed under rule 2.420;
C. All but expunged, or sealed under Ch. 943 and sealed under rule 2.420, 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.

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

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 protection of confidential information. It is recommended that clerks advise commercial purchasers that court records are regularly updated, and encourage use of updated records.

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 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.

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 individual clerk, but links shall refresh no less than once every 30 minutes.

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. Other user roles with authenticated users may have more robust search features than general public users.

Non-confidential data or data accessed by an authenticated user may be viewed immediately. Some images may be "viewable on 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.

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.

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 user name and password, and have the ability to change their password using self-service within the web-based application.

ACCESS SECURITY MATRIX

Access Security
Matrix v8 April 2018.x

Access Security Matrix

(April 2018 version 8)

User Role (Subscribers)																
Key to access codes A = All but expunged, or sealed under Ch. 943 B = All but expunged, or sealed under Ch. 943 or sealed under rule 2.420 C = All but expunged, or sealed under Ch. 943 and sealed under rule 2.420; 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 H = No access See Access Details		1. Judges and authorized court and clerk's office personnel (Internal access by authorization)	2. Florida State Attorney's Offices	3. Attorneys of Record	4. Parties	5. Public in Clerks' offices and registered users	6. General Gov't and Const Officers	7. General public (without registration agreement)	8. Certified law enforcement officers of federal and Florida state and local law enforcement agencies, Florida Department of Corrections, and their authorized users	9. Florida Attorney General's Office and the Florida Department of Children and Families	10. Florida School Districts (Truancy)	11. Commercial purchasers of bulk records	12. Florida Public Defender's Offices (institutional access only)		*****VOR Statute List (F.S.):** 787, 794, 796, 800, 825, 827, 847, 921 VOR is at the case level ***Viewable on Request (VOR) - to ensure that information is properly removed prior to public access, some case types and document types have a special electronic security called viewable on request. Selecting an image of a court document in cases or documents coded viewable on request will not allow the user to view the record at that point. Instead, a request is generated to a clerk, who performs a second examination of the document to remove personal identification information and information about the victims of sexual or child abuse crimes. After the clerk has completed, the requestor then receives a notice that the document is available for viewing. Once a document has been requested and reviewed, it is available for all future access without requiring a request/review.
Case - Charge/Filing Description	**PRIVACY**													**UCN**	**Applicable rules and statutes**
County Criminal Appeals	P	A	B	B	C	D	C	D	B	C	C	D	B	AP	Rule 2.420(d) & (f)
County Criminal Appeals Sexual Abuse	VOR	A	B	B	D	D	D	D	B	D	D	D	B	AP	Rule 2.420(d) & (f); §119.071(2)(h), F.S.; Chs. 794, 796, 800, 827, & 847, F.S.
County Civil Appeals	P	A	B	B	B	D	C	D	B	C	C	D	C	AP	Rule 2.420(d)
Circuit Civil	P	A	B	B	B	D	C	D	B	C	C	D	C	CA	Rule 2.420(d) & Rule 1.210
Jimmy Ryce Act	VOR	A	B	B	D	D	D	D	B	D	D	D	B	CA	Rule 2.420(d); Chapter 119, F.S.; § 394.921(1)&(2), F.S.
Mortgage Foreclosure	P	A	B	B	B	D	C	D	B	C	C	D	C	CA	Rule 2.420(d) & Rule 1.210
Circuit Civil Private (Sexual Abuse & Medical Malpractice	VOR	A	B	B	D	D	D	D	B	D	D	D	D	CA	Rule 2.420(d)(1)(B)(xiii); §119.071(2)(h), F.S.; §119.0714(1)(h), F.S. & §28.2221(5)(a), F.S.
Circuit Civil - Trusts (Pre 2010)	P	A	B	B	B	D	C	E	B	C	C	E	C	CA	Rule 2.420(d)(1)(B); Chapter 119, F.S. & §28.2221(5)(a), F.S.
County Civil	P	A	B	B	B	D	C	D	B	C	C	D	C	CC	Rule 2.420(d) & Rule 1.210
County Foreclosure	P	A	B	B	B	D	C	D	B	C	C	D	C	CC	Rule 2.420(d) & Rule 1.210
Felony	P	A	B	B	C	D	C	D	B	C	C	D	B	CF	Rule 2.420(d) & Chapter 119, F.S.
Felony - sexual cases	VOR	A	B	B	C	D	D	D	B	D	D	D	B	CF	Rule 2.420(d)(1) & §119.071(2)(h)1.b or c, F.S., Chs. 794, 796, 800, 827, & 847, F.S.
Juvenile Delinquency	P	A	B	B	B	G	G	G	B	G	G	G	B	CJ	§985.04(1) & (2), F.S.; §985.045(2), F.S.; §985.036(1), F.S. & §985.11(3), F.S.
County Ordinance Infractions	P	A	B	B	B	D	C	D	B	C	C	D	C	CO	Rule 2.420
County Ordinance - Arrests	P	A	B	B	C	D	C	D	B	C	C	D	B	CO	Rule 2.420
Probate	P	A	D	D	D	D	D	E	D	D	D	E	D	CP	Rule 2.410; §28.2221(5)(a), F.S.
Probate Miscellaneous	P	A	D	D	D	D	D	E	D	D	D	E	D	CP	Rule 2.410; §28.2221(5)(a), F.S.
Criminal Traffic	P	A	B	B	C	D	C	D	B	C	C	D	B	CT	Rule 2.420(d) & (f)
Juvenile Dependency	P	A	B	B	C	G	G	G	B	B	G	G	G	DP	Rule 2.420(d); §39.0132(3)&(4)(a), F.S.
Juvenile Truancy	P	A	B	B	B	G	G	G	B	B	B	G	G	DP	§984.06(3), F.S.
Domestic Relations	P	A	B	B	B	D	C	E	B	C	C	E	C	DR	Rule 2.420(d); Chapter 119, F.S. & §28.2221(5)(a), F.S.
Domestic Relations Adoption (FINAL)	P	A	G	D	D	G	G	G	G	G	G	G	G	DR	§63.162(1)(2), F.S. & §63.022(4)(i), F.S.
DR Adoption (while open and pending)	P	A	G	B	D	G	G	G	G	G	G	G	G	DR	§63.162(1)(2), F.S. & §63.022(4)(i), F.S.
Domestic Relations - Paternity	P	A	B	B	B	D	C	E	B	C	C	E	C	DR	Rule 2.420(d); §742.011, F.S. & §28.2221(5)(a), F.S.
Domestic Relations - Paternity -sealed	P	A	F	F	F	F	F	F	F	F	F	F	F	DR	§742.011, F.S.; §742.091, F.S.; §742.16(9), F.S.; §742.031(1), F.S. & §28.2221(5)(a), F.S.
Delayed Birth Certificate	P	A	B	B	B	D	C	E	B	C	C	E	C	DR	Rule 2.420(d)(1)(B)(vi); §382.025(1), F.S.; §382.0195(1), F.S.& §28.2221(5)(a), F.S.
Name Change	P	A	B	B	B	D	C	E	B	C	C	E	C	DR	§68.07, F.S. & §28.2221(5)(a), F.S.
Dissolution	P	A	B	B	B	D	C	E	B	C	C	E	C	DR	Rule 2.420(d); §28.2221(5)(a), F.S.& §61.043(1), F.S.
Repeat Violence	P	A	B	B	D	D	C	E	B	C	C	E	B	DR	Rule 2.420(d)(1)(B)(xii); §741.30(8)(c)5b, F.S. & §28.2221(5)(a), F.S.
Administrative Support Proceeding	P	A	B	B	B	D	C	E	B	C	C	E	C	DR	§409.2563(2)(d), F.S. & §28.2221(5)(a), F.S.
Parental Notice of Abortion	VOR	A	G	B	B	G	G	G	G	G	G	G	G	DR	Rule 8.805(b); Rule 8.835; Rule 2.420(d)(1)(B)(vii); §390.01114(4)(e) & §390.01116
Sexual Violence	VOR	A	B	B	D	D	D	E	B	D	D	E	C	DR	Rule 2.420(d) & (f), Chapter 119.071(2)(h)1 (b) or (c), F.S. & §784.046(4), F.S.
Termination of Parental Rights	P	A	B	B	G	G	G	G	B	B	G	G	G	DR	§39.814(3) & (4), F.S.
URESA/UIFSA	P	A	B	B	B	D	C	E	B	C	C	E	C	DR	Rule 2.420(d) & §28.2221(5)(a), F.S.
Extradition	VOR	A	B	B	C	D	D	D	B	D	D	D	C	CF	Rule 2.420(d) & (f)
Guardianship/Guardian Advocate (Developmental Disabilities)	P	A	B	B	B	D	C	E	C	C	C	E	C	GA	§744.1076, F.S. & §744.3701, F.S.; & 393.12, F.S.
Guardianship Miscellaneous/Professional Guardian	P	A	B	B	C	D	C	E	C	C	C	E	C	GA	§744.1076, F.S.; §744.3701, F.S. & §744.2003, F.S.
Non-Criminal Infractions	P	A	B	B	B	D	C	D	B	C	C	D	C	IN	Rule 2.420(d)
Juvenile Miscellaneous	P	A	B	B	G	G	G	G	G	G	G	G	G	DP	§985.04(1) & (2), F.S. & 985.045(2), F.S.
~~Financial Miscellaneous~~ [Deactivated]	~~P~~	~~G~~	~~B~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~MM~~	~~Rule 2.420(d) & Chapter 119, F.S.~~
Miscellaneous Firearms	P	A	B	B	B	D	C	D	B	C	C	D	B	MM	Rule 2.420(d); Chapter 119, F.S. & §790.065(4), F.S.

Access Security Matrix

(April 2018 version 8)

User Role (Subscribers)															
Key to access codes A = All but expunged, or sealed under Ch. 943 B = All but expunged, or sealed under Ch. 943 or sealed under rule 2.420 C = All but expunged, or sealed under Ch. 943 and sealed under rule 2.420; 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 H = No access See Access Details		1. Judges and authorized court and clerk's office personnel (Internal access by authorization)	2. Florida State Attorney's Offices	3. Attorneys of Record	4. Parties	5. Public in Clerks' offices and registered users	6. General Gov't and Const Officers	7. General public (without registration agreement)	8. Certified law enforcement officers of federal and Florida state and local law enforcement agencies, Florida Department of Corrections, and their authorized users	9. Florida Attorney General's Office and the Florida Department of Children and Families	10. Florida School Districts (Truancy)	11. Commercial purchasers of bulk records	12. Florida Public Defender's Offices (institutional access only)		*****VOR Statute List (F.S.):** 787, 794, 796, 800, 825, 827, 847, 921 VOR is at the case level ***Viewable on Request (VOR) - to ensure that information is properly removed prior to public access, some case types and document types have a special electronic security called viewable on request. Selecting an image of a court document in cases or documents coded viewable on request will not allow the user to view the record at that point. Instead, a request is generated to a clerk, who performs a second examination of the document to remove personal identification information and information about the victims of sexual or child abuse crimes. After the clerk has completed, the requestor then receives a notice that the document is available for viewing. Once a document has been requested and reviewed, it is available for all future access without requiring a request/review.
Case - Charge/Filing Description	**PRIVACY**													**UCN**	**Applicable rules and statutes**
Baker Act and Mental Health Miscellaneous	P	A	B	B	B	D	D	E	C	D	D	E	B	MH	Rule 5.900; §394.4615, F.S.; §393.11, F.S.; §765.105, F.S.; §916.107(3)(a), §415.1051, F.S. & §394.459(8)
Substance Abuse - Assessment/Treatment	P	A	B	B	B	G	G	G	B	B	G	G	G	MH	Rule 2.420(d); §397.501(7), F.S. & §397.6760, F.S.
Tuberculosis/STD Treatment/Other Confidential	P	A	B	B	B	G	G	G	B	B	G	G	G	MH	§392.55, F.S. & §384.27, F.S.
~~Substance Abuse cases filed pre 10-1-2010 disabled~~ [Deactivated]	~~P~~	~~A~~	~~B~~	~~B~~	~~D~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~G~~	~~MH~~	~~§397.501, F.S.~~
Incapacity	P	A	B	B	B	D	C	E	C	C	C	E	C	MH	Rule 2.420(d) & §744.3701, F.S.
Misdemeanor	P	A	B	B	D	D	C	D	B	C	C	D	B	MM	Rule 2.420(d)
Misdemeanor - sexual cases	VOR	A	B	B	D	D	D	D	B	D	D	D	B	MM	Rule 2.420(d) & §119.071(2)(h), F.S.
Municipal Ordinance Infraction	P	A	B	B	B	D	C	D	B	C	C	D	C	MO	Rule 2.420(d)
Municipal Ordinance Arrest	P	A	B	B	B	D	C	D	B	C	C	D	B	MO	Rule 2.420(d)
Misdemeanor-Misc	VOR	A	B	B	B	D	D	D	B	D	D	D	B	MM	Rule 2.420(d)
Parking	P	A	B	B	B	D	C	D	B	C	C	D	B	CO	Rule 2.420(d)
Small Claims	P	A	B	B	B	D	D	D	D	D	D	D	C	SC	Rule 2.420(d)
Traffic Infractions	P	A	B	B	B	D	C	D	B	C	C	D	B	TR	Rule 2.420(d)
Any case marked sealed	S	A	G	G	G	G	G	G	G	G	G	G	G		Any case that has a SEALED Privacy at the case level
Any expunged case	E	H	H	H	H	H	H	H	H	H	H	H	H		Any case that has an EXPUNGED Privacy at the case level
Sealed Family Law Case	S	A	G	B	B	G	G	G	G	G	G	G	G		Case by case basis giving Party/Attorney access