Supreme Court of Florida

No. AOSC22-7

IN RE: ACCESS TO ELECTRONIC COURT RECORDS

ADMINISTRATIVE ORDER

In March 2014, the Supreme Court adopted the Standards for Access to Electronic Court Records (hereinafter "Standards") and the Access Security Matrix (hereinafter "Matrix") in *In re: Standards for Access to Electronic Court Records*, Fla. Admin. Order No. AOSC14-19 (amended May 23, 2014), to govern appropriate, differentiated levels of access to electronic court records.

Since then, the Florida Courts Technology Commission (hereafter "Commission") has recommended changes to the Standards and the Matrix, as necessary, based on applicable rules and statutes, and the Court adopted the most recent revisions through *In re: Access to Electronic Court Records*, Fla. Admin. Order No. AOSC21-45 (September 3, 2021).

In June 2021, the Florida Court Clerks & Comptrollers (hereinafter "FCCC") chose to voluntarily implement the Matrix into the Comprehensive Case Information System (hereinafter "CCIS"), a statewide electronic court case data system that is maintained by the FCCC. As a result of the changes to CCIS made by the FCCC in June 2021, several government users' access to confidential case information in CCIS was affected, which prompted several requests for amendments to the Standards and the Matrix to be submitted.

After thoughtfully reviewing all amendment requests, the Commission recommended that the Court create a separate user role for the Justice Administrative Commission (hereinafter "JAC"). Additionally, the Commission recommended that the JAC be required to establish policies and procedures to ensure that access to confidential records and information is limited to those individuals who require access to said records and information in the performance of their official duties.

The Commission also recommended that the Florida Department of Law Enforcement be added to the existing Certified Law Enforcement Officers of Federal and Florida State and Local

Law Enforcement Agencies, and Florida Department of Corrections user role on the Standards and the Matrix.

Moreover, since The Florida Bar (hereinafter "Bar") is an extension of the judicial branch, the Commission recommended that the Bar be provided with the same access as judges and authorized court and clerk's office personnel.

Additionally, the Commission recommended revising the access levels for the Office of Criminal Conflict and Civil Regional Counsel to allow attorney of record access to certain criminal and civil cases.

The Commission further recommended revising current access levels for other user types to ensure the appropriate access to case information was properly reflected on the Matrix.

Further, the Commission recommended that the Mortgage Foreclosure case type be consolidated into the Circuit Civil case type, and that Medical Malpractice be moved from the Circuit Civil Private (Sexual Abuse) case type to the Circuit Civil case type, and small claims access be expanded for certain users.

As a means for the judicial branch to continue to ensure responsible access to electronic court records, the Court hereby

adopts the amended Standards and 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 March 24, 2022.

AOSC22-7 03/24/2022

Chief Justice Charles T. Canady

AOSC22-7 03/24/2022

ATTEST:

AOSC22-7 03/24/2022

John A. Tomasino, Clerk of Court

AOSC22-7 03/24/2022

1. The Standards for Access to Electronic Court Records and the Access Security Matrix are also available on the Florida Courts website. See https://www.flcourts.org/Resources-Services/Court-Technology/Technology-Standards.

Standards for Access to Electronic Court Records

March 2022

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") 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 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.

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 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.

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 by court order;
C. All but expunged, or sealed under Ch. 943, F.S. or sealed by court order or confidential under Fla. R. Gen. Prac. & Jud. Admin. 2.420;
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.

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 §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. Access to records sealed pursuant to §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.
User Role 2 Florida State Attorneys' Offices and the Office of Statewide Prosecution	All records except those that are expunged or sealed, or, unless Level B access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. Access to Social Security numbers by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to HIV test results as permitted by §381.004(5)(c), F.S. Access to sexually transmitted disease results as permitted by §384.29(1), F.S.	Secure access through username and password by written notarized agreement. The agency gatekeeper is responsible for maintaining the 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 the performance of their official duties.**

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
	Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5, F.S. Access to mental health records as permitted by §§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 §119.0714(1)(h), F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S.	
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), Fla. R. Gen. Prac. & 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 in accordance with rule 2.505, Fla. R. Gen. Prac. & Jud. Admin.	Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining the authorized user list.

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
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), Fla. R. Gen. Prac. & 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 the 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), Fla. R. Gen. Prac. & Jud. Admin., 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 §28.2221(5)(a), F.S.	Secure access through username and password or in person at Clerks' offices.
User Role 6 General government and constitutional officers	All records except those that are expunged or sealed, or, unless Level "B" access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. 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 the 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 the performance of their official duties.**

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
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), Fla. R. Gen. Prac. & 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 §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 the Florida Department of Law Enforcement	All records except those that are expunged or sealed, or, unless Level "B" access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to HIV test results as permitted by §§381.004(2)(e), and 951.27 F.S. Access to sexually transmitted disease results as permitted by §384.29(1), F.S. Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S.	Secure access through username and password by written notarized agreement. The agency gatekeeper is responsible for maintaining the 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 the performance of their official duties.**

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
	Access to identities of victims of sexual and child abuse when originating from law enforcement as permitted by §119.0714(1)(h), F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. Access to juvenile records as permitted by §§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, or, unless Level "B" access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. 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 agency gatekeeper is responsible for maintaining the 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 the 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, or, unless Level "B" access is assigned to this role in the Access Security Matrix, those records automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to juvenile delinquency records as permitted by §985.04(1)(b), F.S.	Secure access through username 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 the 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. Gen. Prac. & 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 §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.
User Role 12 Florida Office of the Public Defender (Institutional Access only)	All records except those that are expunged or sealed; or, unless Level "B" access is assigned to this role in the Access Security Matrix, access may be denied to records or information automatically confidential under rule	Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list.

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
	2.420(d)(1), Fla. R. Gen. Prac. & 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 attorney of record at a defendant's first appearance as permitted by §985.045(2) and rules 8.010 and 8.165, Fla. R. Juv. P., for juvenile defendants and §27.51, F.S., 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.	**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 Office of Criminal Conflict and Civil Regional Counsel (Institutional Access only)	All records except those that are expunged or sealed; or, unless Level "B" access is assigned to this role in the Access Security Matrix, 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 Criminal Conflict and Civil Regional Counsel (OCCCRC) is considered the attorney of record at a party's first appearance in civil proceedings	Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list. **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 the performance of their official duties,**

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
	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. Access will be changed to User Role 6 when the OCCCRC is no longer the attorney of record or another attorney is assigned.	
User Role 14 Statewide Guardian ad Litem Office	All records except those that are expunged or sealed, or, unless Level "B" access is assigned to this role in the Access Security Matrix, automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order. Access to social security numbers as permitted by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5., F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. 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 authorized user list. **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.	
User Role 15 Justice Administrative Commission	All records except those that are expunged or sealed; or, unless Level "B" access is assigned to this role in the Access Security Matrix, access may be denied to records or information automatically confidential under rule 2.420(d)(1), Fla. R. Gen. Prac. & Jud. Admin., or made confidential by court order, depending upon the type of case and the language of the court order. Access to Social Security numbers by §§119.071(5)(a)6.b. and 119.0714(1)(i), F.S. Access to HIV test results as permitted by §381.004(5)(c), F.S. Access to sexually transmitted disease results as permitted by §384.29(1), F.S. Access to birth certificates as permitted by §§382.013(5) and 382.025(1)(a)5, F.S. Access to mental health records as permitted by §§394.4615(3)(b), 394.4655(3)4)(c), and F.S.	Secure access through username and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list. **The justice administrative commission 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 identities of victims of sexual and child abuse when originating from law enforcement as permitted by §119.0714(1)(h), F.S. Access to children and families in need of services records as permitted by §984.06(3), F.S. Access to juvenile records as permitted by §§39.0132(4)(a)(1) and 985.04(1)(b), F.S.	

INSTITUTIONAL ACCESS

Institutional Access applies to roles of the Florida 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.

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:

1. Level 1 -The system reads the images and uses the knowledge base to auto-redact suspect regions.
2. 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 the 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 username and password and have the ability to change their password using self-service within the web-based application.

Access Security Matrix -Workgroup Recommended Changes

(March 2022 v11)

User Role (Subscribers)

Key to access codes
A = All but expunged, or sealed under Ch. 943, F.S.
B = All but expunged, or sealed under Ch. 943, F.S., or sealed by court order
C = All but expunged, or sealed under Ch. 943 or confidential under Fla. R. Gen. Prac. & Jud. Admin. 2.420, or by court order
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

***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	1. Judges and authorized court and clerk's office personnel (Internal access by authorization)	2. Florida State Attorney's Offices and the Office of Statewide Prosecution	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 the Florida Department of Law Enforcement	9. Florida Attorney General's Office and Florida Department of Children and Families	10. Florida School Districts (Truancy)	11. Commercial purchasers of bulk records	12. Florida Office of the Public Defender (Institutional Access only)	13. Office of Criminal Conflict and Civil Regional Counsel (Institutional Access only)	14. Statewide Guardian ad Litem Office	15. Justice Administrative Commission	UCN	Applicable rules and statutes
County Criminal Appeals	P	A	B	B	C	D	C	D	B	C	C	D	B	B	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	B	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	C	D	C	AP	Rule 2.420(d)
Circuit Civil	P	A	B	B	B	C	C	C	B	C	C	D	C	C	C	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	B	D	B	CA	Rule 2.420(d), Chapter 119, F.S.& § 394.921(1)&(2), F.S.
Circuit Civil Private (Sexual Abuse)	VOR	A	B	B	D	D	D	D	B	D	D	D	D	D	D	D	CA	Rule 2.420(d)(1)(B)(xiii), §§119.071(2)(h), 119.0714(1)(h), & 28.2221(5)(a), F.S.
Circuit Civil - Trusts (Pre 2010)	P	A	B	B	B	C	C	E	B	C	C	E	C	C	C	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	C	C	C	B	C	C	D	C	C	C	C	CC	Rule 2.420(d) & Rule 1.210
Felony	P	A	B	B	C	D	C	D	B	C	C	D	B	B	C	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	B	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	C	A	B	B	B	G	G	G	B	G	G	G	B	B	G	B	CJ	§§985.04(1) & (2), 985.045(2), 985.036(1) & 985.11(3), F.S.
County Ordinance Infractions	P	A	B	B	B	D	C	D	B	C	C	D	C	B	C	C	CO	Rule 2.420
County Ordinance - Arrests	P	A	B	B	C	D	C	D	B	C	C	D	B	B	C	C	CO	Rule 2.420
Probate Formal Administration	P	A	D	D	D	D	D	E	D	D	D	E	D	D	D	D	CP	Rule 2.420; §§28.2221(5)(a) & 733.604 (b), F.S.
Probate Other	P	A	D	B	D	D	D	E	D	D	D	E	D	D	D	D	CP	Rule 2.420; §§28.2221(5)(a) & 735.201-302, F.S.
Criminal Traffic	P	A	B	B	C	D	C	D	B	C	C	D	B	B	C	B	CT	Rule 2.420(d) & (f)
Juvenile Dependency	C	A	B	B	C	G	G	G	B	B	G	G	G	B	B	B	DP	Rule 2.420(d), §§39.0132(3)&(4)(a), 39.822(3) & 27.511(6)(a), F.S.
Juvenile Truancy	C	A	B	B	B	G	G	G	B	B	B	G	G	B	B	B	DP	§984.06(3) & §27.511(6)(a), F.S.
Domestic Relations	P	A	B	B	B	D	C	E	B	C	C	E	C	B	C	C	DR	Rule 2.420(d), §§28.2221(5)(a), 61.043(1), 68.07, 382.025(1), 382.0195(1), 409.2563(2)(d) & 742.011, F.S.
Domestic Relations Adoption (FINAL)	C	A	G	D	D	G	G	G	G	G	G	G	G	D	G	G	DR	§§63.162(1)(2) & 63.022(4)(i), F.S.
DR Adoption (while open and pending)	C	A	G	B	D	G	G	G	G	G	G	G	G	B	G	G	DR	§§63.162(1)(2), 63.022(4)(i), & 27.511(6)(a), F.S.
Domestic Relations - Paternity - sealed	P	A	F	F	F	F	F	F	F	F	F	F	F	F	F	F	DR	§§742.011, 742.091, 742.16(9), 742.031(1), & 28.2221(5)(a), F.S.
DR Violence Injunctions (all) Before Service	C	A	B	B	G	G	G	G	D	G	G	G	G	G	G	G	DR	Rule 2.420(d)(1)(B)(xxiii), §§119.0714(1)(k)3 & 28.2221(5)(a), F.S.
DR Violence Injunctions (all but sexual) After Service	P	A	B	B	D	D	C	E	B	C	C	E	B	B	C	C	DR	Rule 2.420(d)(1)(B)(xxiii), §§119.0714(1)(k)3 & 28.2221(5)(a), F.S.
Parental Notice of Abortion	VOR	A	G	B	B	G	G	G	G	G	G	G	G	~~B~~	G	B	DR	Rule 8.805(b), Rule 8.835, Rule 2.420(d)(1)(B)(vii), §§390.01114(6)(e) & 390.01116, F.S.
Sexual Violence After Service	VOR	A	B	B	D	D	D	E	B	D	D	E	C	B	D	B	DR	Rule 2.420(d)(1)(B)(xiii) & (f), §119.071(2)(h)1 (b) or (c), F.S.
Termination of Parental Rights	C	A	B	B	G	G	G	G	B	B	G	G	G	B	B	B	DR	§§39.814(3) & (4), 39.822(3) & 27.511(6)(a), F.S.
Extradition	VOR	A	B	B	C	D	D	D	B	D	D	D	C	D	D	B	CF	Rule 2.420(d) & (f)
Guardianship/Guardian Advocate (Developmental Disabilities)	P	A	B	B	B	D	C	E	C	C	C	E	C	B	C	B	GA	§§744.1076, 744.3701, 393.12 & 27.511(6)(a), F.S.
Guardianship Miscellaneous/Professional Guardian	P	A	B	B	C	D	C	E	C	C	C	E	C	B	C	B	GA	§§744.1076, 744.3701, 744.2003 & 27.511(6)(a), F.S.
Non-Criminal Infractions	P	A	B	B	B	D	C	D	B	C	C	D	C	C	C	C	IN	Rule 2.420(d)
Juvenile Miscellaneous	C	A	B	B	G	G	G	G	G	G	G	G	G	B	G	G	DP	§§985.04(1) & (2), 985.045(2) & 27.511(6)(a), F.S.
Miscellaneous Firearms	P	A	B	B	B	D	C	D	B	C	C	D	B	B	D	C	MM	Rule 2.420(d), §§119 & 790.065(4), F.S.
Mental Health Miscellaneous	P	A	B	B	B	D	D	E	C	D	D	E	B	B	D	B	MH	Rule 5.900, §§393.11, 765.105, 916.107(3)(a), & 415.1051, F.S.
Baker Act	C	A	B	B	B	G	G	G	B	B	G	G	B	B	B	B	MH	Rule 2.420(d), §§394.459(8) & 394.4615, F.S.
Substance Abuse - Assessment/Treatment	C	A	B	B	B	G	G	G	B	B	G	G	G	B	B	B	MH	Rule 2.420(d), §§397.501(7), 397.6760 & 27.511(6)(a), F.S.
Tuberculosis/STD Treatment/Other Confidential	C	A	B	B	B	G	G	G	B	B	G	G	G	B	B	B	MH	§§392.55, 384.27 & 27.511(6)(a), F.S.
Incapacity	P	A	B	B	B	D	C	E	C	C	C	E	C	B	C	B	MH	Rule 2.420(d), §§744.3701, & 27.511(6)(a), F.S.
Misdemeanor	P	A	B	B	D	D	C	D	B	C	C	D	B	B	C	B	MM	Rule 2.420(d)
Misdemeanor - sexual cases	VOR	A	B	B	D	D	D	D	B	D	D	D	B	B	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	B	C	C	MO	Rule 2.420(d)
Municipal Ordinance Arrest	P	A	B	B	B	D	C	D	B	C	C	D	B	B	C	C	MO	Rule 2.420(d)
Misdemeanor-Misc	VOR	A	B	B	B	D	D	D	B	D	D	D	B	B	D	B	MM	Rule 2.420(d)
Parking	P	A	B	B	B	D	C	D	B	C	C	D	B	B	C	C	CO	Rule 2.420(d)

Access Security Matrix -Workgroup Recommended Changes

(March 2022 v11)

		User Role (Subscribers)																
Key to access codes A = All but expunged, or sealed under Ch. 943, F.S. B = All but expunged, or sealed under Ch. 943, F.S., or sealed by court order C = All but expunged, or sealed under Ch. 943 or confidential under Fla. R. Gen. Prac. & Jud. Admin. 2.420, or by court order 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		**1. Judges and authorized court and clerk's office personnel (Internal access by authorization)**	**2. Florida State Attorney's Offices and the Office of Statewide Prosecution**	**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 the Florida Department of Law Enforcement**	**9. Florida Attorney General's Office and Florida Department of Children and Families**	**10. Florida School Districts (Truancy)**	**11. Commercial purchasers of bulk records**	**12. Florida Office of the Public Defender (Institutional Access only)**	**13. Office of Criminal Conflict and Civil Regional Counsel (Institutional Access only)**	**14. Statewide Guardian ad Litem Office**	**15. Justice Administrative Commission**		*****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**
Small Claims	P	A	B	B	B	C	C	C	C	C	C	D	C	C	C	C	SC	Rule 2.420(d)
Traffic Infractions	P	A	B	B	B	D	C	D	B	C	C	D	B	B	C	C	TR	Rule 2.420(d)
Any case marked sealed	S	A	G	G	G	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	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	G	G	G		Case by case basis giving Party/Attorney access

Domestic Relations consists of Administrative Support Proceeding, Delayed Birth Certificate, Dissolution, Domestic Relations-Paternity, URESA/UIFSA, and Name Change
County Civil consists of County Foreclosure
Circuit Civil consists of Mortgage Foreclosure