Standards for Access to Electronic Court Records

April 2019

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 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.

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. Access will be changed to Registered User when the attorney's appearance is terminated in accordance with rule 2.505.	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 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.	Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list.

MATRIX USER ROLES	ACCESS PERMITTED	USER SECURITY REQUIREMENTS
	Access to social security numbers as permitted by ss. 119.071(5)(a)6.b. and 119.0714(1)(i), F.S.	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.
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.	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
	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.	
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.