

Supreme Court of Florida

No. AOSC15-18

IN RE: STANDARDS FOR ACCESS TO ELECTRONIC COURT
DOCUMENTS AND ACCESS SECURITY MATRIX

ADMINISTRATIVE ORDER

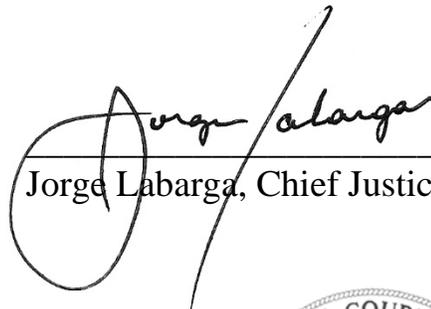
In March 2014, the Supreme Court adopted the Standards for Access to Electronic Court Records and the Access Security Matrix. See In re: Standards for Access to Electronic Court Records, Fla. Admin. Order No. AOSC14-19 (amended nunc pro tunc to March 19, 2014, on May 23, 2014). Since that time, the Access Governance Board, under authority of the Florida Courts Technology Commission (hereinafter “FCTC”), has made recommended changes to these two documents based on input from the clerks of court, private attorneys, public defenders, representatives of the media, and other interested entities.

The FCTC has approved the changes 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 FCTC now recommends approval and adoption by the Court of the amended Standards for Access to Electronic Court Records and the amended Access Security Matrix.

As a means for the judicial branch to continue to ensure responsible access to electronic records, the Court hereby adopts the amended Standards for Access to Electronic Court Records and the amended Access Security Matrix to supersede those adopted in AOSC14-19. The amended Standards for Access to Electronic Court Records and the Access Security Matrix are attached hereto and incorporated herein by reference.¹

DONE AND ORDERED at Tallahassee, Florida, on June 9, 2015.



Jorge Labarga, Chief Justice

ATTEST:



John A. Tomasino, Clerk of Court



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

Standards For Access To Electronic Court Records

May 2015

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. The standards also implement the Access Security Matrix, which governs remote internet and clerk's 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
3. Web-based portal for public viewing of replicated data and variable levels of security based on user role

Direct or web access to live production data is generally limited to court and clerk officers and authorized court and clerk's office staff. 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 appended to these standards governs access to electronic court records based upon user roles and applicable rules, statutes, and administrative policies. The matrix performs the following functions:

1. Establishes user groups
2. Establishes access levels
3. Assigns access level for each user group based on case type
4. Assigns access level for all docket codes

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

USER GROUPS

Access to electronic court records is determined by the user's role and applicable statutes, rules, and administrative policy. Access may be restricted to certain user groups based on case type, document type, or information contained within 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 rule and statutory requirements. Remote electronic access may be more restrictive than clerk in-house electronic access.

USER GROUPS	ACCESS PERMITTED	SECURITY REQUIREMENTS
Judges and authorized court and clerk's office personnel	<p>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.</p> <p>Access to records sealed pursuant to s. 943.059, F.S., is permitted judges to assist in performance of case-related adjudicatory responsibilities.</p>	In-house secure network and secure web access.
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.
General public	<p>All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order.</p> <p>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.</p>	None. Anonymous internet access permitted.

USER GROUPS	ACCESS PERMITTED	SECURITY REQUIREMENTS
Individuals registered for subscriber service	<p>All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order.</p> <p>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.</p>	Secure access through user name and password by written notarized agreement.
Attorneys of record	<p>For the purpose of rules 8.010 and 3.130, the Office of the Public Defender is considered the attorney of record at first appearance. 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.</p>	Secure access through user name and password by written notarized agreement. The gatekeeper is responsible for maintaining authorized user list.
Authorized state or local government agencies	<p>All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order.</p> <p>Access to social security numbers as permitted by s.119.071, F.S.</p>	Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list.

USER GROUPS	ACCESS PERMITTED	SECURITY REQUIREMENTS
<p>Certified law enforcement officers of federal or state law enforcement agencies, including state attorney's offices, and state attorney general's office</p>	<p>All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order.</p> <p>Access to social security numbers as permitted by s.119.071, F.S.</p> <p>Access to HIV test results as permitted by ss. 775.0877, 951.27, and 960.003, F.S.</p> <p>Access to sexually transmitted disease results as permitted by s. 384.29(1), F.S.</p> <p>Access to birth certificates as permitted by s. 382.013(5), F.S.</p> <p>Access to mental health records as permitted by s. 916.107(8), F.S.</p> <p>Access to addresses of domestic violence victims, and identities of victims of sexual and child abuse when originating from law enforcement as permitted by s. 119.071(2), F.S.</p> <p>Access to children and families in need of services records as permitted by s.984.06(3), F.S.</p> <p>Access to juvenile records as permitted by s. 39.0132(4)(a)(1), F.S.</p>	<p>Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining an authorized user list.</p>

USER GROUPS	ACCESS PERMITTED	SECURITY REQUIREMENTS
	<p>Access to juvenile delinquency records as permitted by s. 985.04, F.S.</p> <p>Access limited to law enforcement personnel who require access in performance of their official job duties.</p>	
<p>Department of Children and Families personnel, or authorized service providers of the agency.</p>	<p>All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order.</p> <p>Access to social security numbers as permitted by s. 119.071, F.S.</p> <p>Access to birth certificates as permitted by s. 382.013(5), F.S.</p> <p>Access to children and families in need of services records as permitted by s. 984.06(3), F.S.</p> <p>Access to juvenile records as permitted by s. 39.0132(3), F.S.</p> <p>Access to juvenile delinquency records as permitted by s. 985.04, F.S.</p> <p>Access to records is limited to agency personnel and service providers who</p>	<p>Secure access through user name and password by written notarized agreement. Agency gatekeeper is responsible for maintaining authorized user list.</p>

USER GROUPS	ACCESS PERMITTED	SECURITY REQUIREMENTS
	require access in performance of their official job duties.	
Commercial purchasers of bulk records.	<p>All records except those that are expunged or sealed, automatically confidential under rule 2.420(d)(1), or made confidential by court order.</p> <p>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.</p>	<p>Secure access through user name and password by written notarized agreement. Commercial purchaser gatekeeper is responsible for maintaining an authorized user list.</p>
Administrative	Access for administrative purposes only to manage accounts for an organization with multiple users	<p>Secure access to maintain and update user accounts. Gatekeeper can represent an agency under a single notarized agreement.</p>

ACCESS LEVELS

Access permitted to:

- 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

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. Requests for judicial orders will be reviewed by the clerk for redaction or application of security protocols consistent with these standards.

SECURITY

No sensitive security information should be presented on the user interface. Sensitive data shall be exchanged over trusted paths, or 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 cut and paste 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
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 and redacted version of the record.

Links online shall be encrypted where a user may not be able to cut and paste a URL and get back to a page. Link refresh times shall be limited and time out.

REDACTION

Redaction is the process of obscuring confidential information contained within a public record from view. Redacted portions of the 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 records 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 may not work in some circumstances, such as with handwritten text or poor quality images. There must be a process to review records that cannot be redacted by software. It is recommended that these records be made available upon request, so proper review and redaction can be completed before they are provided on-line for viewing. The default view for judges is the non-redacted version of the record.

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.

PERFORMANCE

Search parameters for internet access to electronic records will be limited to the following:

A. Public User

1. case type
2. case number
3. party name
4. citation number
5. date range

B. Authenticated Users may have more robust search features.

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.

Images are view only, and therefore cannot be modified. No search of images is allowed for internet public access. This type of search would invite bots, overburden the system, and weaken the security systems in place to protect confidential information. Internal users may search images if legally authorized to do so.

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.

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 access portal.

USER MAINTENANCE

Each state or local government agency or law office with personnel who access electronic records in a role that must be authenticated must assign a gatekeeper to notify clerk's office staff of employee or contractor changes. Each agency and law office must remove terminated employees or contractors and must accept responsibility for unauthorized access. The clerks must develop and maintain agreements clearly defining responsibilities for user maintenance.

ACCESS SECURITY MATRIX



Access Security
Matrix v4 May 2015.xl