Best Practice:

ELECTRONIC VIEWING AND RELEASE OF COURT RECORDS

(Category: _____)

I. Background and Purpose: On March 19, 2014, in AOSC14-19, the Supreme Court lifted the moratorium on online viewing of electronic court documents that had been in place since 2004. AOSC14-19 supersedes the order that provided interim access – AOSC07-49 – and defines standards about online viewing as well as user groups and security levels. The order contains a number of technical requirements, Standards for Electronic Access to Court Records (Standards), and a complex security matrix, Access Security Matrix (Matrix), designed to balance reasonable online viewing for the public and an individual's right to privacy.

The order provides for a permissive clerk application process. Each clerk who wishes to provide online viewing must apply to the FCTC for approval of its remote electronic viewing system. Each clerk has 120 days from the date of their application approval letter to implement their online viewing systems. The 90-day pilot period begins when implementation is finished. Upon conclusion of the pilot, each clerk will need to apply for final certification.

It is important that each clerk who chooses to provide online viewing of court records does so in as consistent a manner as possible, so that customers are presented with a similar experience and are provided the same viewing abilities consistently throughout the state. This Best Practice is intended to provide guidelines to achieve that consistency.

II. Recommendations: The Best Practices Committee, appointed by the President of the Florida Court Clerks and Comptrollers (FCCC), recommends that the following guidelines are implemented by the Clerks of the Circuit Court in the State of Florida in compliance with legal requirements set out in the Florida law.

A. Consider Utilizing the Best Practice Reference Guide for FCTC Security Matrix.

1. **Reference Guide**: The attached Reference Guide spreadsheet reorganizes the FCTC Security Matrix by division and provides additional explanations.

2. **Criminal Charges Protected Tab**: This tab provides a list of the charges that apply to criminal cases involving sexual violence or child abuse, to determine what cases fall under those categories on the matrix. Each clerk's office in criminal cases will need to create a method of identifying what criminal cases involve sexual violence or child abuse. A preliminary set of statutes is also included on the Case Level Tab in the Reference Guide Matrix. Also consider whether victim information will be filed in Jimmy Ryce Act cases and, if so, how to protect that information.

   Some offices also opt to apply the protection of a victim's identity information in sexual offenses or child abuse criminal cases to plaintiffs or petitioners in civil cases, see the discussion of this under the Exceptions section. Civil cases involving these protections will involve either injunction cases or negligence cases. This can provide some inconsistency between clerks' offices.

3. **Security Roles Tab**: This tab compares the users in the Matrix and the Standards and explains the remote viewing capabilities each type of user has, ranging from the public to the courts and clerks.

4. **Documents to Protect Tab**: This tab provides a comprehensive list of document descriptions with the associated protection levels, viewing permissions and explanations derived from the county in which the Matrix was originally implemented. The Standards refers to a list of documents, which is not on the FCTC Matrix. Review the Confidential Records BP for additional information about what documents require protection.

B. Requirements for Remote Electronic Viewing of Court Records:

1. **Authentication:** A user's role must be authenticated for enhanced viewing. In order to be assigned a login account, users must register with the pertinent clerk's office and provide verifiable identification by notarization. Users with enhanced, remote viewing permissions must have a user name, password, and the ability to independently change their password within the clerk's system.
2. **Search Parameters:** Search parameters for the general public user group is limited to case type, case number, party name, citation number, and date range. Clerks may add a filter feature to the search results and provide authenticated users with more robust search options.
3. **Security:** Confidential information must be blocked from viewing and information must be exchanged only over trusted paths or through the use of adequate encryption. The cut and paste of workable links is prohibited; hyperlinks must not include authentication credentials; and only replicated records can be used for the viewing by the general public. Authentication is required for enhanced viewing permissions and bulk data transfers must be monitored to protect against abuse by automated search programs.
4. **User Maintenance:** Clerks must develop and maintain agreements clearly defining responsibilities for user maintenance. Gatekeepers/Administrative [Users] must be designated by government agencies where staff members are authenticated users. Gatekeepers/Administrative [Users] are required to immediately notify a clerk's office of employee or contractor changes, to promptly remove accounts for terminated employees or contractors and to accept all consequences for unauthorized use of records.
5. **Judicial Signatures:** The Standards require that judicial orders be provided to a requestor only after redaction OR application of security protocols to protect the judicial signature. Orders filed via either the Florida E-Portal or judicial viewers are trusted and secure delivery systems and such orders may be released without the redaction of judicial signatures as those security protocols are consistent with those required by the *Standards.* Judicial viewers, in particular, require an electronic signature of a judge [to] be accompanied by a date, time stamp, and case number which must appear as a watermark through the signature to prevent copying the signature to another document as well as appear unobscured below the signature. §8.5 of CAPS Functional Requirements Version 3.0. Clerks may release paper orders without redacting a judicial signature if the office has developed a security policy similar to the chain of custody requirements for evidence in order to ensure the protection of judicial signatures.

C. Identify and Protect Confidential Cases, Documents and Information

1. Protecting against the unauthorized release of confidential records is a key component of implementing a remote viewing system. Neither the *Standards for Electronic Access to Court Records* in AOSC14-19 nor the incorporated Security Matrix promulgates confidentiality requirements beyond those currently in law.
2. Clerks should review the FCCC's Best Practice on Confidential Records and ensure that their online systems protect confidential information or records listed in Fla. R. Jud. Admin. 2.420 (d)(1)(B) and (c) 1-6 or protected by court order.

3. Establish a policy for adding new charges or updating FDLE table to determine whether any of the added or revised charges involve the list of protected statutes. FCCC, in its annual legislative review, should identify legislation that would affect the Reference Guide and provide recommendations for updating the Matrix and Standards.
4. Set a policy for viewing progress dockets on cases where victim information is protected depending on whether or when rules were in place to limit information on dockets about victims that might identify a victim in cases where victim identification information is protected. For example, if your office set a policy prohibiting victim information from being on docket lines in sexual battery cases in 2010, prohibit viewing of pre-2010 docket lines after 2010.
5. Sealed Civil Orders: Decide what the effect of an order sealing a civil case (not under FS 943.059, FS 943.0585, or Fla. R. Crim. P. 3.692) or sealing a document is on viewing permissions, for example, whether the party names are protected, based on the wording of the order.

D. User Roles and User Role Definitions

1. **Attorney General**, the chief legal officer for Florida as established by Art. IV, §10, Fla. Const., including assistant attorney generals as defined in FS 16.08 is entitled to view some confidential information, but not sealed or expunged records. The agency must submit a written agreement for secure viewing permission with each clerk; designate a gatekeeper to maintain an authorized user list; and establish a local security policy to ensure that confidential information is only viewed by those individuals who require this information in the performance of their official duties. This can be a single agreement for all clerks' offices.
2. **Attorney of record**
   a. An attorney who has appeared in a case under Fla. R. Jud. Admin. 2.505(e). Only attorneys admitted to The Florida Bar or are admitted Pro Hac Vice can appear in a Florida case. Federal attorneys may have attorney of record viewing rights, see definition of Federal attorney in Definitions section. When an attorney of record's status as such terminates, be sure the attorney's viewing rights as attorney of record are also terminated. Consider whether attorneys listed in the signature block, but not signing the pleading, are attorneys of record for purposes of heightened viewing rights.
   b. Ordinarily an attorney of record will have a Florida Bar number and attorneys appearing pro hac vice will have a pro hac vice number assigned by The Florida Bar. Since clerks are required to confirm that attorneys of record are in good standing with The Florida Bar weekly, The Florida Bar number will be needed for registration and verification.
   c. Enhanced viewing rights for an attorney of record terminate upon the occurrence of any the events listed in Fla. R. Jud. Admin. 2.505(f) (e.g., attorney is automatically terminated as attorney of record after case closed for 30 days, if no notice of appeal filed). Accordingly, unless a clerk's programming can distinguish differing viewing rights based on party and corresponding attorney, documents which could otherwise be viewed by one party, but not another, should either be protected or identified as a VOR document.
   d. Although attorneys of record are permitted to view many confidential documents on the cases on which they are the attorney of record, the Access Governance Board has clarified that only redacted versions of documents with redactions can be viewed online, regardless of the security role of the viewer. The Access Governance Board will recommend the following language to the FCTC: *Viewing of court documents through a web-based application is defined by a security matrix. The Matrix is based upon only*

redacted information being available on the web. When a document is presented for viewing on the web, it should be redacted pursuant to applicable rules and statutes.

e. The Standards and Matrix use the permissive "may" when authorizing clerks to allow viewing of confidential information to attorneys of record, because some clerk's offices may not have the ability to provide some users with protected documents and others with unprotected documents. Each office can evaluate their resources and determine whether they can offer this service. The Protected Documents Tab identifies which documents can be viewed by attorneys of record.
f. Attorneys of record are also permitted to view most confidential paper records, if they exist. The attorney's right to view records depends on the viewing rights of his or her client.
g. In estate and guardianship cases, an attorney of record for purposes of viewing confidential reports is limited to an attorney who has appeared for the personal representative or guardian case as authorized in Fla. Prob. R. 5.030.
h. An attorney who has filed a motion to intervene is not an attorney of record until an order authorizing the attorney's client to intervene has been entered.
i. Support staff may only use their attorneys' login credentials, for which the attorney is responsible, as authorized by the attorney.
j. A Public Defender is considered the attorney of record at first appearance. Fla. R. Juv. P. 8.010, and Fla. R. Crim. P. 3.130.
k. The Task Force should request that the FCTC add a provision that allows attorneys to view information, with client consent, without appearing in a case as an attorney of record.
l. Attorneys must submit a written notarized agreement to each clerk to obtain secure viewing permission. There is no authorization in either the Standards or the Matrix for law firm gatekeepers.
m. Limited appearances are being addressed by RJA committee.

3. **Clerks of Court** as established in Art. V, §16, Fla. Const., and clerk personnel as defined in FS 27.01, are permitted to view all court records, except expunged records. The Standards document includes "Judges and authorized court and clerk's office personnel" as a single category of viewing permissions and requires each office to establish a local security policy to ensure that confidential information is only viewed by those individuals who require this information in the performance of their official duties. Some clerks may want to conduct periodic audits with random checks to make sure that protections are in place.
4. **Commercial Purchasers of Bulk Records** can register and view family and probate images as well as view social security numbers, if a clerk's office has the capability of protecting the SSN's from viewers without authorization to view SSN's. A commercial purchaser is a company that performs a qualified commercial activity in this state and makes a verified (see FS 92.525) written request for the social security number complying with FS 119.071(5)(a) 7. A qualified commercial activity means the permissible uses set forth in the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq.; the Fair Credit Reporting Act, 15 U.S.C. ss. 1681 et seq.; or the Financial Services Modernization Act of 1999, 15 U.S.C. ss. 6801 et seq., or verification of the accuracy of personal information received by a commercial entity in the normal course of its business, including identification or prevention of fraud or matching, verifying, or retrieving information. It does not include the display or bulk sale of social security numbers to the public or the distribution of such numbers to any customer that is not identifiable by the commercial entity. FS 119.071(5)(a) 7.a.(I).

5. **Department of Children and Families**, as defined in FS 39.0016 (including community-based care lead agency acting on behalf of Department), is permitted to view some confidential court records, as authorized by law. The agency must submit a written agreement for secure viewing permission with each clerk; designate a gatekeeper to maintain an authorized user list; and establish a local security policy to ensure that confidential information is only viewed by those individuals who require this information in the performance of their official duties. This can be a single agreement for all clerks' offices.
6. **Gatekeepers/Administrative [Users]** are designated by an agency or other entity to govern that organization's users and determine the remote viewing rights of individual organization users within the parameters assigned to that organization. As a registered user, they can also view family and probate images. To obtain secure authorization, agencies/entities must complete the required registration process for its user group—a single notarized agreement is sufficient. The agency principal and/or designee (with proof of designation) can appoint that agency's gatekeeper. Some offices require agency letterhead to be included with the registration agreement to show that authority, though each office must decide how to determine gatekeeper appointment authority.
7. **Judges, Authorized Court Personnel, and Judicial Assistants,** including hearing officers, magistrates, and other judicial staff, are permitted to view all confidential information, except for records that are expunged. Each office is required to establish a local security policy to ensure that confidential information is only viewed by those individuals who require this information in the performance of their official duties. The Matrix labels this group as "Judges, JA's, Court Personnel, Clerk Personnel." Clerks may wish to request their Court Administrator's Office to verify judicial users.
8. **Law Enforcement Agency personnel/Certified Law Enforcement Officers** are permitted to view some confidential court records as authorized by law, but not sealed or expunged records. Agencies must submit a written agreement for secure viewing permission and designate a gatekeeper to maintain an authorized user list and establish a local security policy to ensure that confidential information is only viewed by those individuals who require this information in the performance of their official duties. Definition: an agency or unit of government or any municipality or the state or any political subdivision which has constitutional or statutory authority to employ or appoint persons as officers and private entities contracting with state or county to operate a non-juvenile detention facility. See FS 943.10 (4) and (1) for full definition of law enforcement officer. This can be a single agreement for all clerks' offices.
9. **Parties**, persons or entities named in a case, are entitled to view the documents in their cases including most, but not all, confidential information. When a party is dismissed their "party" status is discontinued, meaning they no longer are entitled to enhanced viewing rights and the clerk must ensure that access is turned off. An intervenor does not become a party until an order authorizing intervention is entered. In some cases, such as dependency cases, a party may cease to be a party and is not entitled to confidential information. Non-party status extends to the non-party's attorney. Need notarized registration agreement and method to verify party is on case. Viewing rights of this role is the same whether the party is attorney-represented or is self-represented.
10. **Public Internet (Anonymous)** are members of the public and can view court information and images without having to set up a user name and password. They are prohibited from viewing any confidential information, nor can they view family or probate images, though

some clerks interpret FS 28.2221(5)(a) to include both information and images. Refer to the FS 28.2221 section in the Legal References, Application section below.

11. **Public in Clerk's Office** is a user role that allows viewing at the same level as Registered Users, while remaining anonymous with no registration required. They can view non-confidential family and probate images available as well as all other non-confidential. These users can view records on the clerk's website as long as those records are replicated records, so that the records cannot be altered or damaged. The Standards' "General Public" incorporates this category.
12. **Public Defenders** are attorneys as defined in FS 27.50, including assistant public defenders as defined in FS 27.53. Because Public Defenders are not governmental agencies, the viewing rights are as an attorney of record, where applicable. There is also, therefore, no provision for a gatekeeper.
13. **Regional Counsel** are attorneys appointed as authorized in FS 27.511, including both appointed regional staff and attorneys hired by regional counsel. Viewing rights are as an attorney of record.
14. **Registered users** (public, non-attorney of record) are not entitled to confidential information, but can view otherwise public probate and family images. Need notarized registration agreement. Each user must submit a written notarized agreement to obtain secure viewing permission.
15. **School Board (matrix)** district school superintendents authorized to file a truancy petition under FS 1003.27 and personnel assigned to performing these duties as directed and authorized by a superintendent are authorized to view truancy cases. Personnel viewing authorization is regulated by a gatekeeper. This can be a single agreement for all clerks' offices.
16. **State and Local Government Agency** and **General Government and Constitutional Officers personnel** can view some confidential information, as authorized by law, but not expunged records. Each agency's viewing permissions must be reviewed on a case-by-case basis, with each clerk evaluating an agency's authority to view the information requested by the agency. Definition: any state, county, district, authority, municipality, constitutional office, department, division, board, bureau, commission, or other separate unit of government created or established by law, including county school boards. See FS 110.107 and 165.031, and ch. 125. The six constitutional officers are: Attorney General, Chief Financial Officer, Governor/Lieutenant Governor, Secretary of State, State Treasurer/Insurance Commissioner/Fire Marshal. Each officer has state agencies, offices, or departments under their command. Agencies must submit a written agreement for secure viewing permission; designate a gatekeeper to maintain an authorized user list; and establish a local security policy to ensure that confidential information is only viewed by those individuals who require this information in the performance of their official duties. For statewide agencies, this can be a single agreement for all clerks' offices.
17. **State Attorneys,** as defined in FS 27.01, including assistant state attorneys as defined in FS 27.151, are permitted to view some confidential information, but not sealed or expunged records. Because State Attorneys are not governmental agencies, the viewing rights are as an attorney of record, where applicable. There is also, therefore, no provision for a gatekeeper.

E. Other Definitions

1. **Anonymous Remote Viewing**: internet viewing by members of the public who are not registered with the clerk's office.

2. **Confidential**: information which the clerk has an independent duty to keep protected as confidential under Fla. R. Jud. Admin 2.420, with no court order required.
3. **Federal Attorneys**: United States Attorneys represent the United States federal government in United States district and circuit courts. Each U.S. Attorney is the chief federal law enforcement officer of his or her judicial district. This includes assistant United States attorneys. U.S. Attorneys and their offices are overseen by the Executive Office for United States Attorneys of the Department of Justice. Personnel viewing authorization is regulated by a gatekeeper.
4. **Federal Law Enforcement Officer**: The federal government of the United States empowers a wide range of law enforcement agencies to maintain law and public order related to matters affecting the country as a whole. The Department of Justice, which handles most law enforcement duties at the federal level, includes the United States Marshals Service (USMS), the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), the Bureau of Alcohol, Tobacco, Firearms and Explosives (BATFE), Federal Bureau of Prisons (BOP), and the Department of Homeland Security (DHS), which includes elements of the U.S. Coast Guard and the U.S. Transportation Security Administration. There is also U.S. Customs and Border Protection (CBP) which includes the Office of Air and Marine, the Office of Border Patrol, and the Office of Field Operations. There are dozens of other federal law enforcement agencies under other executive departments, as well as under the legislative and judicial branches of the federal government.
5. **Matrix**: Spreadsheet designed to implement the Standards for Viewing Court Documents for programming purposes. A Florida Supreme Court approved spreadsheet that governs remote Internet and Clerk's office viewing of electronic court records. This "living document" applies to both electronic and paper records, establishes user groups and assigns access levels based on case type and docket codes.
6. **Online Remote Viewing**: This is any program or web application that allows viewers to view case information and/or case images from a location away from the physical buildings where clerks maintain offices. Case information/images that can be viewed in a clerk's office is not considered remote online view, whether the viewing is via an internet web app or is viewed via a system that is not on the internet.
7. **Public**: Everyone except judges, clerks, parties with regard to their cases, attorneys of record, and other entities designated under the Standards as having additional viewing authorization or permissions. This includes General Public as used in the Standards and Public Internet (Anonymous) on the Matrix.
8. **Redaction**: The process of protecting a portion of a document that is determined to be confidential, either by the court or by the clerk so that the non-confidential information on the image can be viewed and the confidential information cannot be viewed.
9. **Sealing**: the process of protecting an entire document or file that is determined by the court to be confidential or to be sealed.
10. **Security Levels:** Permission granted to a user group for the electronic viewing of court record images and data. Authorization levels range from permission to view images in all but expunged or sealed cases to no viewing rights of any kind.
11. **Standards for Electronic Access to Court Records:** A Florida Courts Technology Commission (FCTC) document that establishes the statewide technical and operational requirements for the electronic viewing of court records.
12. **Viewable on Request (VOR):** An electronic security code applied to certain case types and documents in order to ensure confidential or unauthorized information is removed prior to

public viewing. When an image is coded as VOR, the user will not immediately view the record but will instead generate a request to a Clerk. The Clerk then performs a second examination of the document to remove personal identification information and data relating to victims of certain crimes. After the second inspection, the requestor receives notification the document is available for view and the VOR designation is removed for all future remote viewing requests.

13. **Viewing Methods:** A procedure to retrieve electronic court documents and data. The three authorized techniques are through (1) direct access via application to live data, (2) web-based application to replicated or live data with security; and (3) a web-based portal of replicated data with various levels of security based on user roles.

III.Exceptions

- **A.** Local administrative orders may be inconsistent. Clerk's offices will need to review local administrative orders and decide, with the input of the judiciary, how to address the inconsistencies and how to field questions from other users about discrepancies between their security levels and those of other clerks' offices.
- **B.** Address processes outside of the matrix, why consistency might not be fully achieved.
- **C.** Sexual Victim Information for cases involving sexual offenses is expressed in criminal terms in the statute. Some offices extend the protection of identification information to plaintiffs in civil cases who were victims in an underlying criminal case.
- **D. Case types/data not addressed by the matrix**:
  - **1.** Insurance receivership cases, these cases are only filed in Leon County.
  - **2.** Qui tam cases filed only in Leon County. FS 68.083(8)(complaint and information held by department pursuant to investigation of violation of FS 68.082 is confidential, but may be disclosed by department to law enforcement agency, and is no longer confidential once investigation completed, unless information otherwise protected by law)
  - **3.** Gestational Surrogacy cases have similar confidentiality protections to adoption cases. Fla. R. Jud. Admin 2.420(d)(1)(B)(xiv)
  - **4.** Family Services for Children (CINS/FINS cases), Fla. R. Jud. Admin 2.420(d)(1)(B)(xvii)
- **E. Case types/Data/Information Confidential on Matrix, but not in Fla. R. Jud. Admin. 2.420(d)(1)(B) or (c)1-6**:

  The following **Civil** case types or documents that are either included in the FCTC Matrix or have traditionally have been protected by some offices, but are not included in Fla. R. Jud. Admin. 2.420(d)(1)(B) or (c)1-6 and clerks' offices should consider require an order determining these to be confidential before protecting them from viewing. This section is being included for informational purposes, but is still open for review, discussion, and comment. **FOR TASK FORCE DISCUSSION, SEE SEPARATE OPTIONS DOCUMENT.**
  - **1.** Attorney fee contingency contract cases, R. Regulating Fla. Bar 4-1.5(f)(4)(D)(counsel shall apply to court…and this aspect of the file may be sealed)
  - **2.** Disciplinary actions concerning nurses, FS 464.018
  - **3.** Qui tam cases (Leon only), FS 68.083
  - **4.** Paternity where mother marries purported father – entire file after clerk receives written notice and marriage certificate showing mother has married purported father, FS 742.091, per FS 63.089(8) (the record of proceedings….shall be sealed against public inspection).
  - **5.** Crash reports, FS 316.066(3)(c) (held by agency)
  - **6.** Federal tax returns – FS 192.105(1), 26 USC 6103
  - **7.** Jury notes, FS 40.50 (court, bailiff shall promptly destroy), recommend preventing jury notes from getting in file.
  - **8.** Photo, video, audio of killing, FS 406.136

9. Mediation reports, FS 44.102(3) (exempt from requirements of 119), Fla. R. Med. 10.360 requires mediator to maintain confidentiality of all information revealed during mediation, nothing about it being protected in court file
10. Involuntary Commitment of Sexual Predators cases – psychological, drug, alcohol, treatment, medical, victim impact statements and reports in CA ICCSVP cases – FS 394.921, forensic evaluations only cover defendants who have been charged with a felony and have been found to be incompetent to proceed; except that victim information is protected. Forensic reports in rule refer to ch. 916
11. Autopsy records –FS 406.135 (… held by a medical examiner)
12. Neurological Birth Defect claim information (furnished to association), FS 766.305(3)(claimant shall furnish to association information…which shall remain confidential and exempt under provisions of s. 766.315(5)(b)); FS 766.315(5)(b) (claim file in possession of association confidential or exempt)

F. Gestational surrogacy is on the List of 22, but not on the matrix. Fla. R. Jud. Admin. 2.420(d)(1)(B)(xiv), FS 742.16(9)(all "papers and records" are confidential, shall only be indexed in name of petitioner, name of child shall not be noted on any docket index or other record outside the court file)

G. Criminal case (CF, MM, CT, and CJ) documents not on the List of 22
   a. Crash reports (not for public view for 60 days) – FS 316.066(2)(held by the agency)
   b. Criminal history information – 28 CFR 2021(c); MOUs with FDLE
   c. Clinical Records, FS 916.107(8) statutory reference only covers evaluations of defendants charged with a felony and found to be incompetent to proceed, this is also the citation on the List of 22– Fla. R. Jud. Admin. 2.420(d)(1)(B)(viii) (any record derived from a mental health evaluations)
   d. DNA test results – FS 760.40(2)(a)
   e. Driving histories – FS 119.0712(2); MOUs with DHSMV
   f. Investigative subpoenas – FS 119.071(2)(c)1.("received by a criminal justice agency")
   g. Wireless applications/orders – FS 119.071(2)(a); FS 934.09(8)(c)

H. DR cases
   a. Guardian ad Litem reports filed in chapter 39 cases Fla. R. Jud. Admin. 2.420(d)(1)(B)(iii), no separate listing for guardian ad litem reports in other DR cases.
   b. Injunctions – sexual offense/child victim identification information – Fla. R. Jud. Admin. 2.420(d)(1)(B)(xiii), FS 119.071(2)(a) (redact victim identifying information, refer to discussion below under exceptions)
   c. Paternity – DNA test results – FS 760.40(2)(a)

IV.Legal References, Application

A. Standards vs Matrix Discrepancies: AOSC14-19 provides a Standards document and the Matrix is an implementation of the AO and Standards created to simplify programming of any remote electronic system. To the extent that there is any discrepancy, the Standards should control. Differences are noted in this best practice as well as in the Reference Guide.

B. Florida Rule of Judicial Administration 2.420 requires clerks to designate and maintain the confidentiality of any information contained within a court record that is described in either Fla. R. Jud. Admin. 2.420(d)(1)(A) or in 2.420(d)(1)(B). Subsection (d)(1)(A) covers information in Fla. R. Jud. Admin. 2.420(c)(1)-(c)(6), which covers arrest and search warrants, drafts of judicial opinions, and other judicial administrative information). Fla. R. Jud. Admin. 2.420(d)(1)(B) includes a "list of 22" items, each having statutory citations. Notably, information made confidential by Federal and Florida Law or court rule in subsections (c)(7) and (8), **only includes**

the items on the 2.420 list. Further, subsection (d)(3) provides a mechanism for filers to follow when they want subsection (c)(7-8) items determined confidential on a case by case basis. Additionally, subsection (j) provides a mechanism to view confidential records by court order.

C. **AOSC14-19** establishes Standards for remote online viewing and the incorporated Matrix implements those standards for programming purposes. The Florida Supreme Court also adopted AOSC14-569, which incorporates the technology standards of AOSC14-19 into Fla. R. Jud. Admin. 2.420 (the additional language in 2.420(a) "Scope and Purpose"). AOSC14-19 has some prospective language about transitioning from the moratorium "release" language of AOSC07-49 to the new standards, however the Standards and Matrix adopted in Fla. R. Jud. Admin. 2.420 do not include the AOSC14-19 transitional language.

D. **FS 28.2221(5)(a),** prohibiting records of cases governed by the Florida Rules of Family Law, the Florida Rules of Juvenile Procedure, or the Florida Probate Rules from being placed on a publicly available Internet website, has been interpreted by some counties to only include images and, by some others, to also include all information. The pilot county for online viewing provided information, but not images in these cases, and this system was approved by the FCTC. In addition, the Court, via the Standards, only limits viewing of images of these case types for anonymous public (non-registered users) remote users. Further, the legislative history of HB 1679 reflects that the Legislature only intended to prohibit Clerks from placing images or copies of records from such cases on a publicly available Internet website, not information about such cases. See Final Legislative History HB 1679 (2002), pp. 13 and 14. Since the Standards and Matrix only allow for images in these case types to be viewed by registered users, the images are not "publicly available" and, thus, do not violate the legislative mandate.

E. **FS 28.24**(12)(e)(1) provides that "[a]ll court records and official records are the property of the State of Florida and the clerk of court is designated the custodian of all court records. This declaration does not address whether the legislature or the courts, which are both part of "the State of Florida," have the right to determine what records are to be maintained as confidential.

F. **FS ch. 119** provides that providing access to public records is a duty of each agency, FS 119.01(1), which is defined as any state, county, district, authority, or municipal officer, department, etc., of government created or established by law. FS 119.011(2) Information in court files, court records, and Official Records is specifically addressed in FS 119.0714 and the opening section provides, "Nothing in this chapter shall be construed to exempt from §119.07(1) a public record that was made part of a court file and that is not specifically closed by order of court…." and then provides a list of exceptions such as: criminal intelligence information, social security numbers, confessions, identity of confidential informants, bank numbers, etc. The creation of a separate statute to cover court records indicates legislative intent that the other provisions of chapter 119 do not apply to court records.

G. **Applicability of statutory confidentiality provisions** and Fla. R. Jud. Admin. 2.420.

1. Times Pub. Co. v Ake, 660 So. 2d 255 (Fla. 1995), finds that the Court has exclusive jurisdiction over its records and that legislative regulation of court records is without effect. The clerk, when acting in the exercise of his duties derived from article V is acting as an arm of the court and, as such, is immune from the supervisory authority of the legislature… and access to judicial records under [clerk] control is governed exclusively by Fla. R. Jud. Admin. 2.051 [now 2.420].

2. Fla. R. Jud. Admin. 2.420(d)(1), which imposes a duty on clerks, excludes subsection (c)(7-8) from the list of documents that the clerk has an independent duty to protect, Fla. R. Jud. Admin. 2.420(d)(3), (e), (f), and (g) provide a mechanism for filers to protect (c)(7-8) information, and Fla. R. Jud. Admin. 2.420(j) provides a mechanism for those who cannot view confidential information.

3. Chapter 119, as applied to court records, limits ch. 119 exemptions to those in FS 119.0714. Some offices argue that the language in FS 119.0714 was created before the Ake decision in 1995 and that Ake and the subsequently enacted Fla. R. Jud. Admin. 2.420 supersede this statutory section, and so that only the chapter 119 exemptions selected by the Court as part of the "22" are the clerks' responsibility to maintain as confidential.
4. Other statutes make some court records confidential or exempt from release. Some clerks have historically protected these court records statutes, though not included in the Fla. R. Jud. Admin. 2.420 "List." Examples are listed in section III.E above. Each office will need to determine whether to protect only the Fla. R. Jud. Admin. 2.420(c)(1-6) and (d) list or include other statutory protections, considering the potential impact of inconsistency among clerks.
5. The Florida Supreme Court, in In re Amendments to Florida Rule of Judicial Administration 2.420 and the Florida Rules of Appellate Procedure, 31 So.3d 756, 762 (Fla. 2010), held that "New subdivision (d) sets forth the procedure for the clerks of court to designate court records as confidential under subdivisions (c)(1) through (c)(8) and *limits the subdivision (c)(7) and (c)(8) records that must be automatically designated as confidential to a finite set of nineteen [now 22] statutory exceptions*. It also provides a mechanism for the filer to seek a judicial determination of confidentiality as to subdivision (c)(7) and (c)(8) records that are not automatically designated confidential by the clerk." The Court termed the then "nineteen" exceptions as type I information which requires the clerks to automatically designate and maintain them as confidential. Further, the Court held that "New subdivision (d)(3) applies to what the Access Committee refers to as type II information which is information that may be confidential under (c)(7) or (c)(8), but that is not automatically confidential under the new rule." *Id. at 763*.

H. The **minimization rule**, Fla. R. Jud. Admin. 2.425, provides that "information filed with the court must be limited to the following format:…" This rule does not direct the clerk to identify or protect any of this information. There are exceptions to the minimization rule such as: (a) the name of a minor in any order relating to parental responsibility, time-sharing, or child support, (b) an account number which identifies the property alleged to be the subject of a proceeding, (c) the birth date of a minor whenever it is necessary for the court to establish or maintain subject matter jurisdiction, etc. Subsection (e) of the rule Provides "[t]his rule does not affect the application of constitutional provisions, statutes, or rules of court regarding confidential information or access to public information."

V.Communication

1. Clerks should consider public expectations for viewing court records when communicating on these issues:
   a. While the public may think all Clerks are the same, Clerks should be prepared to explain the differences based on size, budget, and other factors, i.e., whether they have in-house IT staff; whether electronic redaction is deployed; whether scanning is fully deployed and to what extent back-scanning has been achieved; etc.
   b. Clerks should be prepared to explain the evolution of their offices from a paper to electronic world. If some Clerks are not able to provide remote electronic viewing as envisioned by AOSC14-19 at this time, they should be prepared to show their proactive efforts in addressing issues regarding timeliness of records being docketed, scanned, in electronic or paper case files, etc.
   c. As custodians of court records, Clerks should explain their duty to balance the right to public viewing of records against keeping specific records as confidential.

2. If your office already has electronic viewing in place, but has to make changes as a result of AOSC14-19, consider communication by newsletter or other means to alert users to upcoming changes and why those changes are necessary.
3. If your office is not currently providing remote electronic viewing, consider communication to customers, or use of a standard response if questions are posed, about your current circumstances and how that may or may not change in the future.
4. Meet with judicial partners – judges, sheriff, State Attorney, Public Defender, etc. – to discuss the changes and how they may affect local viewing capabilities.