JUDICIAL COUNCIL
OF CALIFORNIA
TECHNOLOGY COMMITTEE

www.courts.ca.gov/jctc.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

Open to the Public (Cal. Rules of Court, rule 10.75(c)(1))
THIS MEETING WILL BE CONDUCTED BY TELECONFERENCE
THIS MEETING WILL BE RECORDED

Date:	November 9, 2015
Time:	12:00 noon - 1:00 p.m.
Public Call-in Number:	1-877-820-7831 Passcode: 3511860

Meeting materials will be posted on the advisory body web page on the California Courts website at least three business days before the meeting.

Agenda items are numbered for identification purposes only and will not necessarily be considered in the indicated order.

I. OPEN MEETING (CAL. RULES OF COURT, RULE 10.75(C)(1))

Call to Order and Roll Call

Approval of Minutes
Approve minutes of the August 20, 2015 and September 15, 2015, Judicial Council Technology Committee meetings.

II. PUBLIC COMMENT (CAL. RULES OF COURT, RULE 10.75(K)(2))

Written Comment
In accordance with California Rules of Court, rule 10.75(k)(1), public comments about any agenda item must be submitted by November 6, 2015, 12:00 noon. Written comments should be e-mailed to jctc@jud.ca.gov or mailed or delivered to 2255 N. Ontario Street, Suite 220, Burbank, California 91504, attention: Jessica Craven. Only written comments received by November 6, 2015, 12:00 noon will be provided to advisory body members prior to the start of the meeting.

III. DISCUSSION AND POSSIBLE ACTION ITEMS (ITEMS 1–6)

Item 1

Chair Report
Provide update on activities of or news from the Judicial Council, advisory bodies, courts, and/or other justice partners.

Presenter: Hon. Marsha G. Slough

Item 2

E-Signature Standards and Guidelines: Update to the Trial Court Records Manual (Information)

Review a proposal to update the Trial Court Records Manual with standards and guidelines governing electronic signatures by judges and courts. These standards and guidelines were developed by the Court Executives Advisory Committee and the Information Technology Advisory Committee to implement Government Code section 68150(g).

Presenter: Mr. Patrick O'Donnell, Managing Attorney, Legal Services

Item 3

Update/Report on Information Technology Advisory Committee (ITAC)

An update and report on ITAC will be provided; this will include the activities of the workstreams.

Presenter: Hon. Terence L. Bruiniers, Chair, Information Technology Advisory Committee

Item 4

Report on Information Security Framework Workstream: Final Deliverables (Action Required)

Review the proposal to accept the final deliverables of the Information Security Framework Workstream, which includes How to Use the Information Systems Controls Framework and Information Security Framework Checklist documents, and decide whether to recommend that these be submitted to the Judicial Council for review.

Presenters: Hon. Terence L. Bruiniers, and Mr. Robert Oyung, Executive Sponsor, Information Security Framework Workstream for ITAC

Item 5

Update on Civil Case Management System (V3) Replacement Budget Change Proposal

An update and report on the work related to the civil case management system (V3) replacement budget change proposal.

Presenter: Mr. Richard D. Feldstein, JCTC member

Item 6

Update on Sustain Justice Edition Case Management System

An update and report on the work related to the Sustain Justice Edition case management system.

Presenter: Mr. Richard D. Feldstein

IV. ADJOURNMENT

Adjourn

JUDICIAL COUNCIL
OF CALIFORNIA
TECHNOLOGY COMMITTEE

www.courts.ca.gov/jctc.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

MINUTES OF OPEN MEETING

August 20, 2015
10:00 a.m. - 12:00 p.m.

Advisory Body Members Present:	Hon. James E. Herman, Chair; Hon. David De Alba, Vice-Chair; Hon. Daniel J. Buckley; Hon. Ming W. Chin; Hon. Emilie H. Elias; Hon. Gary Nadler; Mr. Mark Bonino; and Mr. Richard D. Feldstein
Others Present:	Mr. Curt Soderlund; Mr. Mark Dusman; Mr. Zlatko Theodorovic; Ms. Diana Earl; Ms. Lucy Fogarty; Ms. Renea Stewart; Ms. Jessica Craven; Ms. Kathy Fink; Mr. David Koon; Ms. Tara Lundstrom; Ms. Katherine Sher; and Ms. June Agpalza

OPEN MEETING

Call to Order and Roll Call

The vice-chair called the meeting to order, took roll call, and advised that no public comments were received.

Approval of Minutes

The members unanimously approved the minutes of the July 21, 2015 Judicial Council Technology Committee meeting.

DISCUSSION AND ACTION ITEMS (ITEMS 1–9)

Item 1

Chair Report (No Action Required)

Update: Hon. James E. Herman, Chair of the Judicial Council Technology Committee (JCTC), thanked all members for attending, presented a special acknowledgement to the Vice-Chair, Hon. David De Alba, and thanked staff for their service.

Item 2

Update on V3 Case Management System Budget Change Proposal (BCP)

Update: Mr. Richard Feldstein provided an update on the work of the joint JCTC and Trial Court Budget Advisory Committee (TCBAC) working group related to the potential BCP for the replacement of the V3 case management system.

Discussion: The committee discussed the work completed to date, as well as the next steps.

Item 3

E-Service: California Rules of Court, rules 2.251 and 8.71 (Action Required)

Update: The committee reviewed the public comments and final proposal to amend rules 2.251 and 8.71 to authorize electronic service on consenting courts.

Discussion: The committee discussed the report and asked questions to clarify the process.

Action: The committee voted to approve the proposal.

Item 4

Phase I of the Rules Modernization Project: California Rules of Court, titles 2, 3, 4, 5, 7, and 8 (Action Required)

Update: The committee reviewed the public comments and final proposal to make technical, non-substantive amendments to the rules in titles 2, 3, 4, 5, 7, and 8.

Discussion: The committee discussed the report.

Action: The committee voted to approve the proposal.

Item 5

Public Access to Electronic Court Records in the Appellate Courts (Action Required)

Update: The committee reviewed the public comments and final proposal to introduce new rules to address public access to electronic court records in the appellate courts.

Discussion: The committee discussed the report.

Action: The committee voted to approve the proposal.

Item 6

E-Signature Standards and Guidelines: Update to the Trial Court Records Manual (Action Required)

Update: The committee reviewed the electronic signature standards and guidelines that would be circulated for comment to the trial courts. The standards and guidelines would be included in the *Trial Court Records Manual*.

Discussion: The committee discussed the standards and guidelines, as well as the next steps.

Action: The committee voted to approve the proposal.

Item 7

Update on Contract for California Court Technology Center

Update: Mr. Mark W. Dusman, Chief Information Officer and Director, Information Technology provided an update on the contract for the California Court Technology Center.

Discussion: The committee discussed the update.

Item 8

Update on California Law Enforcement Telecommunications System (CLETS) and California Court Protective Order Registry (CCPOR)

Update: Ms. Renea Stewart, Senior Manager, Information Technology provided an update on the CLETS and CCPOR in relation to operations and budget impacts.

Discussion: The committee discussed the update.

Item 9

Update on Work of Information Technology

Update: Mr. Mark W. Dusman provided an update on the current and upcoming work and activities of the Information Technology office including the office's budget.

Discussion: The committee discussed the update.

ADJOURNMENT

There being no further business, the meeting was adjourned.

JUDICIAL COUNCIL OF CALIFORNIA

TECHNOLOGY COMMITTEE

www.courts.ca.gov/jctc.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

MINUTES OF OPEN MEETING

September 15, 2015
8:30 a.m. - 9:30 a.m.

Advisory Body Members Present:	Hon. James E. Herman, Chair; Hon. Ming W. Chin; Hon. Gary Nadler; Mr. Mark Bonino; and Mr. Richard D. Feldstein
Advisory Body Members Absent:	Hon. David De Alba, Vice-Chair; Hon. Daniel J. Buckley; and Hon. Emilie H. Elias
Liaison Members Present:	Hon. Marsha G. Slough; and Hon. Terence L. Bruiniers
Others Present:	Mr. Curt Soderlund; Mr. Mark Dusman; Mr. Zlatko Theodorovic; Ms. Diana Earl; Ms. Lucy Fogarty; Ms. Renea Stewart; Ms. Jessica Craven; Ms. Kathy Fink; Mr. David Koon; Ms. Tara Lundstrom; Ms. Katherine Sher; and Ms. June Agpalza

OPEN MEETING

Call to Order and Roll Call

The chair called the meeting to order, took roll call, and advised that a public comment was received.

DISCUSSION AND ACTION ITEMS (ITEMS 1–9)

Item 1

Chair Report (No Action Required)

Update: Hon. James E. Herman, Chair of the Judicial Council Technology Committee (JCTC), thanked all members for attending, welcomed the new chair of the JCTC, Hon. Marsha G. Slough, and new vice-chair of the JCTC, Hon. Daniel J. Buckley, and provided a final chair report.

Item 2

Update/Report on Information Technology Advisory Committee (ITAC)

Update: Hon. Terence L. Bruiniers, Chair of ITAC provided an update on the advisory committee's work. He presented on the activities of the workstreams including a review of the membership of the Next Generation Hosting Strategy, Data Exchange, and E-Filing Workstreams.

Action: The committee voted to approve the membership of the Next Generation Hosting Strategy, Data Exchange, and E-Filing Workstreams and to forward the membership rosters to the Judicial Council's Executive and Planning Committee.

ADJOURNMENT

There being no further business, the meeting was adjourned.

Judicial Council Technology Committee Open Meeting

November 9, 2015

Call to Order and Roll Call

- Welcome
- Open Meeting Script
- Approve minutes

Hon. Marsha G. Slough, Chair, Judicial Council Technology Committee

JUDICIAL COUNCIL OF CALIFORNIA

Chair Report

Hon. Marsha G. Slough

JUDICIAL COUNCIL
OF CALIFORNIA

Update/Report E-Signature Standards and Guidelines: Update to the Trial Court Records Manual

Mr. Patrick O'Donnell, Managing Attorney, Legal Services

JUDICIAL COUNCIL OF CALIFORNIA

Update/Report on Information Technology Advisory Committee (ITAC)

Hon. Terence L. Bruiniers, Chair, Information Technology Advisory Committee

JUDICIAL COUNCIL OF CALIFORNIA

Action: Report on Information Security Framework Workstream: Final Deliverables

Hon. Terence L. Bruiniers, and Mr. Robert Oyung, Executive Sponsor, Information Security Framework Workstream for ITAC

JUDICIAL COUNCIL OF CALIFORNIA

Update on Civil Case Management System (V3) Replacement Budget Change Proposal

Mr. Richard D. Feldstein, JCTC member

JUDICIAL COUNCIL OF CALIFORNIA

Update on Sustain Justice Edition Case Management System

Mr. Richard D. Feldstein

JUDICIAL COUNCIL OF CALIFORNIA

Adjourn

All

JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue · San Francisco, California 94102-3688

www.courts.ca.gov

REPORT TO THE JUDICIAL COUNCIL

For business meeting on: December 11, 2015

Title
Court Records: Electronic Signature Standards and Guidelines - Update to the Trial Court Records Manual

Recommended by
Court Executives Advisory Committee
Mr. Richard D. Feldstein, Chair

Information Technology Advisory Committee
Hon. Terence L. Bruiniers, Chair

Judicial Council of California
Mr. Martin Hoshino, Administrative Director

Agenda Item Type
Action Required

Effective Date
January 1, 2016

Date of Report
November 30, 2015

Contact
Tara Lundstrom
415-865-7650
tara.lundstrom@jud.ca.gov

Josely Yangco-Fronda
415-865-7626
josely.yangco-fronda@jud.ca.gov

Executive Summary

The Court Executives Advisory Committee (CEAC) and the Information Technology Advisory Committee (ITAC) recommend updating the *Trial Court Records Manual* to include new standards and guidelines governing the use of electronic signatures by trial courts and judicial officers. These standards and guidelines implement Government Code section 68150(g), which authorizes electronic signatures by a court or judicial officer "in accordance with procedures, standards, and guidelines established by the Judicial Council." The update also includes new sections in the *Trial Court Records Manual* that (1) outline the various provisions in the Code of Civil Procedure, Penal Code, and California Rules of Court that authorize electronic signatures submitted to the courts by attorneys, parties, and law enforcement officers; and (2) state the effect of digitized signatures created by scanning paper court records. Lastly, the update contains technical changes to align the manual with intervening legislative and form changes.

Recommendation

The Court Executives Advisory Committee and the Information Technology Advisory Committee recommend that the Judicial Council, effective January 1, 2016, update the *Trial Court Records Manual* to:

1. Add standards and guidelines governing the use of electronic signatures by judicial officers and the courts, to implement Government Code section 68150(g);
2. Add an overview of the various provisions in the Code of Civil Procedure, Penal Code, and California Rules of Court that authorize electronic signatures submitted to the courts by attorneys, parties, and law enforcement officers
3. Add a section regarding the effect of digitized signatures created by scanning paper court records; and
4. Make technical changes.

Previous Council Action

For over 20 years, Government Code section 68150(a) has authorized the preservation of trial court records in electronic form. (Stats. 1994, ch. 1030.) With the enactment of Assembly Bill 1926 in 2010, this provision was expanded to allow superior courts to create and maintain court records in electronic form. (Stats. 2010, ch. 167.) Electronic court records were to be subject to rules adopted by the Judicial Council establishing standards and guidelines for their creation, maintenance, reproduction, and preservation. (See Gov. Code, §§ 68150(a) and (c).) The Judicial Council sponsored AB 1926 to facilitate the transition by courts to paperless case environments.

Effective January 1, 2011, the Judicial Council adopted rule 10.854 to implement AB 1926. This rule tasked Judicial Council staff—in collaboration with the trial court presiding judges and court executives—with preparing, maintaining, and distributing a manual providing standards and guidelines for the creation, maintenance, and retention of trial court records, consistent with the Government Code and the rules of court and policies adopted by the council. The first version of this manual, known as the *Trial Court Records Manual,* was approved by the council at the same time that it adopted rule 10.854.

Judicial Council staff—in collaboration with the trial court presiding judges and court executives—are also responsible for periodically updating the *Trial Court Records Manual* to reflect changes in technology that affect the creation, maintenance, and retention of court records. (Cal. Rules of Court, rule 10.854(c).) Proposed changes must be made available for comment from the trial courts before the manual is updated or changed. (*Ibid.*) Since it was first issued, the council has twice updated the *Trial Court Records Manual.*

Rationale for Recommendation

This proposal updates the *Trial Court Records Manual* to implement Government Code section 68150(g) by adding a new section to the manual that establishes standards and guidelines governing the use of electronic signatures on court-created records. In addition, new sections are

added to (1) outline the various provisions in the Code of Civil Procedure, Penal Code, and California Rules of Court that authorize electronic signatures submitted to the courts by attorneys, parties, and law enforcement officers and (2) state the effect of digitized signatures created by scanning paper court records. Lastly, the update contains technical changes to align the manual with intervening legislative and form changes.

Electronic signatures on court-created documents

As part of the effort to modernize the management of trial court records, AB 1926 authorized the use of electronic signatures by courts and judicial officers. The bill added subdivision (g) to Government Code section 68150, which provides as follows:

> Any notice, order, judgment, decree, decision, ruling, opinion, memorandum, warrant, certificate of service, writ, subpoena, or other legal process or similar document issued by a trial court or by a judicial officer of a trial court may be signed, subscribed, or verified using a computer or other technology *in accordance with procedures, standards, and guidelines established by the Judicial Council pursuant to this section*. Notwithstanding any other provision of law, all notices, orders, judgments, decrees, decisions, rulings, opinions, memoranda, warrants, certificates of service, writs, subpoenas, or other legal process or similar documents that are signed, subscribed, or verified by computer or other technological means pursuant to this subdivision shall have the same validity, and the same legal force and effect, as paper documents signed, subscribed, or verified by a trial court or a judicial officer of the court.

(Gov. Code, § 68150(g), italics added.) This proposal implements Government Code section 68150(g) by updating the *Trial Court Records Manual* to include standards and guidelines for the use of electronic signatures by courts and judicial officers.

This year, the Legislature enacted AB 432, which added new section 34 to the Code of Civil Procedure, effective January 1, 2016. Similar to Government Code section 68150(g), new Code of Civil Procedure section 34 provides that electronic signatures by courts and judicial officers are as effective as original signatures. AB 432 also defines the term "electronic signature" in Code of Civil Procedure section 17(b)(3) as "an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record."

To implement Government Code section 68150(g) and Code of Civil Procedure section 34, this update adds a new section 6.2.1 to the *Trial Court Records Manual* to establish standards and guidelines governing electronic signatures by the court and judicial officers. The standards and guidelines are loosely modeled on the Uniform Electronic Transactions Act and New York State's Electronic Signatures and Records Act Guidelines.

Purpose, drafting principles, and definitions. A new section 6.2.1.A states the purpose of the standards and guidelines and lists the principles that motivated the drafters. These principles include that the standards should not be more restrictive than those for traditional 'wet' signatures; that they should consider how the signature is being applied when setting the level of authentication required; that they should allow for flexibility in the method of applying and the appearance of the signature; and that they should, wherever possible, avoid requiring specific proprietary tools. A new section 6.2.1.B provides definitions applicable to the standards and guidelines, including a definition for "electronic signature" that mirrors the definition that will be added by AB 432 to Civil Code of Procedure section 17.

Format of electronic signatures. The format of electronic signatures are stated in new section 6.2.1.C. Electronic signatures may be in the form of (1) a digitalized image of the person's signature, (2) an "/s/" followed by the person's name, or (3) any other electronically created method of indicating with clarity the name of the person whose signature is being affixed to the document.

Guidelines governing intent, attribution, and verification. A new section 6.2.1.D provides guidelines to ensure (1) that the signer intended to sign the document, (2) that the electronic signature is attributable to an authorized person, and (3) that the electronic signature can be verified. To demonstrate intent, it must be clear to a person, when presented with the opportunity to sign a document, that the person is being asked to sign the document electronically. To ensure that the signer is authorized to sign, the document must be presented for an electronic signature only to an authorized person or someone authorized to execute the signature on that person's behalf. An electronic signature may be attributed to a person if it was the act of the person (or the act of someone authorized to sign on that person's behalf), which may be shown in any manner, including the efficacy of the security procedure applied when the signature is executed or adopted. And lastly, the identity of the signer must be capable of verification. Courts are instructed to retain any data relevant to verifying electronic signatures, such as the signer's identity and the date and time that the signature is executed or adopted.

This section also provides a 'practice tip' to recommend that courts consider designing their business practices and technology systems—such as workflows, pop-up screens, and access and security procedures—to facilitate compliance with these guidelines.

Signatures under penalty of perjury. A new section 6.2.1.E governs signatures required by law to be made under penalty of perjury. Electronic signatures may be made under penalty of perjury if the electronic record includes the electronic signature, all of the information as to which the declaration pertains, and a declaration under penalty of perjury by the person who submits the electronic signature that the information is true and correct.

Legal effect of electronic signatures. In accordance with Government Code section 68150(g) and Code of Civil Procedure section 34, a new section 6.2.1.F of the manual states that electronic

signatures by courts and judicial officers have the same effect as original signatures on paper documents.

Acceptable security procedures. Acceptable security procedures for identity verification are addressed in a new section 6.2.1.G. This section provides that all systems used in the capture, application, and storage of electronic signatures and documents should align, to the extent possible, with the data and information security guidelines recommended in *How to Use the Information Systems Controls Framework: A Guide to California Superior Courts.* Application of the framework ensures that access is limited to authorized individuals and that original files and documents have not been altered or modified since they were created.

In addition, this section recognizes both real-time digitized signatures and system-applied signatures as acceptable procedures for verifying identity. Real-time digitized signatures are defined as graphical images of a handwritten signature, where the signature is captured by means of a digital pen, pad, or other device that converts the physical act of signing into a digital representation of the signature and applies that digital representation to a document, transaction, or database entry. User authentication for real-time digitized signatures is similar to the authentication of traditional 'wet' signatures.

System-applied signatures are defined as electronic signatures applied to documents, transactions, or databases through the use of a computer, software, or application following an affirmative action (e.g., clicking on a check box) by the signer or someone authorized to act on his or her behalf. Four methods of user identification are recognized for system-applied electronic signatures: (1) password or PIN, where the user is authenticated through a password or PIN either tied directly to the application of the signature or used to gain access to the computer application, database, or network; (2) symmetric cryptography, where the user is authenticated using a cryptographic key that is known to the system and the signer; (3) asymmetric cryptography (digital certificates), where the user is authenticated using both public and private keys; and (4) biometrics, where the user is authenticated using biometrics such as voice, fingerprint, or retina.

Scanned signatures. A new section 6.2.1.H is added to address digitized signatures that are created when courts convert their paper records into electronic records by scanning. This section provides that the digitized signatures of judicial officers and courts created by scanning have the same validity and the same legal force and effect, as their original signatures.

Examples of court-created documents that may be electronically signed. A new section 6.2.1.I provides a list of various court documents that may be signed electronically by a court or judicial officer. The list is provided for illustrative purposes only and is not intended to suggest that a signature is required on any of the identified documents, unless a signature is otherwise mandated by statute or rule. Examples provided include judgments, orders after hearings, minute orders, notices, abstracts of judgment, arrest and search warrants, and certificates of service, among others.

Electronic signatures on documents submitted to the courts

A new section 6.2.2 is added to the *Trial Court Records Manual* to address the statutes and rules that authorize electronic signatures on documents submitted to the courts by attorneys, parties, and law enforcement officers. This legal authority includes (1) Code of Civil Procedure section 1010.6 and rule 2.257, which govern the use of electronic signatures on electronically filed documents in civil cases; (2) Penal Code sections 817 and 1526, which provide the procedures required to authorize the electronic signatures of law enforcement officers on probable cause declarations for arrest and search warrants; and (3) Penal Code section 959.1, which authorizes the digitized facsimile of a defendant's signature on Notices to Appear issued in traffic and criminal cases for infraction and misdemeanor violations.

Signatures on scanned documents

This proposal also adds a new section 6.2.3 to address digitized signatures that are created when courts convert their paper records into electronic records by scanning. This section provides that these digitized signatures have the same validity and the same legal force and effect, as the original signatures. It largely duplicates the language proposed for section 6.2.1.H that is specific to the scanned signatures of judicial officers and courts. This language is duplicated here to clarify that it also applies to electronic signatures on documents that were submitted to the courts.

Technical changes

Since the *Trial Court Records Manual* was last updated two years ago, the Legislature has enacted various bills amending the statutes governing which trial court records are confidential. This update revises the manual to reflect these changes in the law. It also makes minor technical changes that include eliminating references to the former Administrative Office of the Courts and replacing references to obsolete forms.

Comments, Alternatives Considered, and Policy Implications

Comments

Section 6.2 of this update was circulated to the trial courts for comment from September 8 to 25, 2015. Three courts submitted responses. The technical changes were not circulated because they update the manual to conform to existing law and to make non-substantive revisions.

Superior Court of Imperial County. The Superior Court of Imperial County pointed to the requirement in California Code of Regulations section 22002(a) that a digital signature must be under the "sole control of the person using it." The court perceives a conflict between California Code of Regulations section 22002(a) and this proposal, which recognizes that an electronic signature may be applied by someone authorized to sign documents on behalf of another. To comply with California Code of Regulations section 22002(a), the court's practice is to have the initials of the actual signer notated after the signature when signing on behalf of another.

California Code of Regulations section 22002(a) implements Government Code section 16.5, which authorizes digital signatures on "any written communications with a public entity." Government Code section 16.5 was enacted by the Legislature in 1995. It instructed the Secretary of State to adopt conforming regulations, which are provided in California Code of Regulations section 22000 et seq.

Enacted by the Legislature in 2010, Government Code section 68150(g) provides express authorization for electronic signatures by judges and courts. It directs the Judicial Council to adopt implementing procedures, standards, and guidelines. To the extent that there is any conflict with Government Code section 16.5 and California Code of Regulations section 22000 et seq., the committees' position is that Government Code section 68150(g), as the more recently enacted and specific statute, controls.

In drafting the proposed update, the committees decided to adopt an expressly more expansive approach to allow authorized persons to execute the signature on the person's behalf. This approach recognizes the common practice where judges authorize clerks to sign documents on their behalf. Although the electronic signature will not necessarily reflect the identity of the person who executed or applied the signature, the standards and guidelines contemplate that courts would be able to verify the identity by retaining relevant data.

Because the advisory committees recognize the potential benefit of the court's practice of applying different signatures depending on the identity of the signer, they decided to include a 'practice tip' to suggest that other courts may want to consider adopting this practice.

Superior Court of Los Angeles County. The Superior Court of Los Angeles County noted that the update contemplates that a person electronically filing a document with the court must keep the original signature and may be asked to produce the document bearing the original signature at any time. The court explained that these requirements may act as a disincentive to electronic filing, especially for agencies and other high frequency filers who must store these signed records. In contrast, when a paper document is filed with the court, the court may scan and preserve the document and image of the signature in electronic form. The court proposed similarly allowing the signatures on electronically filed documents to be maintained as a scanned image.

To the extent that the update addresses signatures on documents electronically filed into the courts, it restates the requirements in Code of Civil Procedure section 1010.6(b)(2)(B) and California Rules of Court, rule 2.257(a), for signatures made under penalty of perjury on electronically filed documents. The statute and rule provide that any person or attorney who electronically files a document must keep the printed form bearing the original signature and make it available upon request, if the signature is made under penalty of perjury. The advisory committees appreciate the burden that this may place on government agencies and other high frequency filers and may consider whether to propose legislative and rule amendments to change this requirement in 2016.

Superior Court of Riverside County. The Superior Court of Riverside County posed various questions requesting clarification of the proposal. Regarding the guideline in section 6.2.1.D—which provides that the identity of the signer must be capable of verification and that courts "should retain any data relevant to verifying the signature, such as the identity of the person who executed or adopted the signature and the date and time that the signature was executed or adopted"—the court questioned what data would need to be retained, what constitutes a valid verification, and in what manner verification must be made.

A valid verification would occur when the court is able, after the electronic signature has been applied, to identify the signer and ascertain when the signature was executed or adopted. Specifying precisely what data should be retained and in what manner the verification should be made is beyond the scope of this proposal, as circulated. The advisory committees did not intend to limit the courts in how they implement this guideline. Instead, they envisioned that courts would work with their technology staff and any vendors to ensure that their technology systems are capable of identifying the signer and verifying when the signature was executed or adopted by retaining any relevant data. However, to assist the courts, the committees decided to include a 'practice tip' that describes various types of data that courts may consider retaining.

The Superior Court of Riverside County also asked whether certain electronically signed court-generated documents, such as writs and exemplifications, would be accepted by law enforcement both locally and in other jurisdictions outside of California.

By complying with the proposed electronic signature standards and guidelines, documents that are electronically signed by judges and courts will satisfy the requirements of Government Code section 68150(g), which recognizes that these documents have "the same validity, and the same legal force and effect" as paper documents bearing original signatures. This statutory authorization is broadly worded to apply to "[a]ny notice, order, judgment, decree, decision, ruling, opinion, memorandum, warrant, certificate of service, writ, subpoena, or other legal process or similar document issued by a trial court or by a judicial officer of a trial court."

The advisory committees sympathize with the court's concern that electronically signed documents may not initially be recognized as valid. However, it is beyond the scope of this proposal, as circulated, to address how courts might work with justice partners and other outside parties to ensure that electronically signed documents are recognized as having "the same validity, and legal force and effect" as paper documents bearing original signatures.

Lastly, the Superior Court of Riverside County requested clarification on the language in section 6.2.2.B, which provides that "[w]hen a document to be filed requires the signature, not under penalty of perjury, of an attorney or self-represented party, the document shall be deemed signed by that attorney or self-represented party if *filed* electronically." (Italics added.) The court questioned whether this language should instead read "if *signed and filed* electronically."

The advisory committees recognize that the language in section 6.2.2.B is unclear as to whether the document must be signed before it is electronically filed. Section 6.2.2.B restates the language in Code of Civil Procedure section 1010.6(b)(2), as well as rule 2.257 of the California Rules of Court. Because this language is copied directly from the statute and rule, the advisory committees decline the invitation to revise the update at this time. In the future, the committees may consider whether to propose amending the statute and rule to clarify any ambiguity.

Alternatives Considered

Because Government Code section 68150(g) requires that the Judicial Council establish implementing standards and guidelines, CEAC and ITAC did not consider alternatives to this proposal to adopt these standards and guidelines as part of the *Trial Court Records Manual.*

Implementation Requirements, Costs, and Operational Impacts

Potentially significant costs could be incurred by individual courts in implementing this proposal as they might be required to procure new technology systems and equipment for capturing the electronic signatures of judicial officers and court officials. These initial costs, however, may be outweighed by the cost savings and efficiency gains that would be realized by allowing judicial officers and courts to use electronic signatures. Because implementation is voluntary, each court would determine if the benefits outweigh the costs in deciding whether to use electronic signatures on court-generated documents. Updating the manual, which is in electronic format and posted online, would result in only minimal costs to the branch.

Attachments

1. Chart of comments, at pages 10–14
2. Update to the *Trial Court Records Manual*, at pages ***

Trial Court Records Manual Version 4
Court Executive Advisory Committee and Information Technology Advisory Committee
Input and Recommendation

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Comment	Committee Response
1.	Superior Court of Imperial County By: Terri Darr Court Financial Officer	Under the California Code of Regulations, a digital signature is an acceptable technology if it meets the criteria set out in section 22002 (a). One of the criteria is that it is under the sole control of the person using it. Page 10 of the September 8, 2015 memo, 2nd bullet says, "When a document is to be signed electronically, it must be presented only to an authorized person or to someone authorized to execute the signature on the person's behalf". The JC guidelines allow the electronic signature to be shared which appears to be a conflict with the California Code of Regulations. Today, when signing on behalf of someone else, we notate our initials after the signature, exposing that the signature does not belong to the signer. I understand that there are certain documents that may be electronically signed in mass, and perhaps the proposed language is meant to address this situation. With the advent of mobile technology, documents can be signed electronically by the owner of the electronic signature.	The advisory committees appreciate the court's input. California Code of Regulations section 22002(a) implements Government Code section 16.5, which authorizes digital signatures on written communications with public entities. Government Code section 68150(g) expressly authorizes electronic signatures by judges and courts. It also directs the Judicial Council to adopt implementing procedures, standards, and guidelines. As the more recently enacted and specific statute, the committees' position is that Government Code section 68150(g) controls over Government Code section 16.5 and California Code of Regulations 22002(a). In drafting the proposed update, the committees decided to adopt an expressly more expansive approach to allow authorized persons to execute the signature on the person's behalf. This expansion was included to recognize the common practice where judges authorize clerks to sign documents on their behalf. In response to the court's comment, the advisory committees decided to include a 'practice tip' to suggest that other courts may also want to consider adopting different signatures depending on who is applying the signature.
2.	Superior Court of Los Angeles By: Tricia Penrose Senior Administrator	Throughout these updates to the TCRM a person filing a document electronically to the court must keep the original signature and may be requested to produce the document with the original signature at any time. If the original is filed	The advisory committees appreciate the court's input, but decline the invitation to revise this proposal at this time. To the extent that the update addresses signatures on documents electronically filed into the courts, it only restates the

Trial Court Records Manual Version 4
Court Executive Advisory Committee and Information Technology Advisory Committee
Input and Recommendation

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Comment	Committee Response
		with the court we would scan and preserve the image of the signature as the original. In some instances this may be counterproductive as an incentive to e-file because the filer now has to retain the original document, when if filed the court would scan and destroy. This may be especially true for high frequency filers like agencies that would have to store these signed records. Perhaps allowing for a scanned image of the signed document to be retained may help.	requirements in Code of Civil Procedure section 1010.6(b)(2)(B) and California Rules of Court, rule 2.257(a), for signatures made under penalty of perjury on electronically filed documents. The statute and rules provide that anyone who electronically files a document must (1) keep the printed form bearing the original signature if the signature is made under penalty of perjury and (2) make the printed form available upon request. This year, the Legislature enacted Assembly Bill 1519, which slightly modifies these requirements for local child support agencies. Amended Family Code section 17400(a)(3) allows local child support agencies to maintain original signed pleadings by way of an electronic copy in the Statewide Automated Child Support System and requires the agencies to keep the original signed pleadings only for the time period stated in Government Code section 68152(a). The Judicial Council is required to adopt implementing rules by July 1, 2016. This legislative change does not directly affect the courts or this update. To the extent that any implementing rule amendments modify the general signature rules duplicated in the update, they will be added to the next update. Next year, the advisory committees may consider whether to propose additional legislative and rule amendments to change the requirements for signatures on electronically filed documents.

Trial Court Records Manual Version 4
Court Executive Advisory Committee and Information Technology Advisory Committee
Input and Recommendation

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Comment	Committee Response
		On page 8, it looks like they are adding "Creation" to the title of section 6 of the TCRM. However, that is already part of section 4 titled "Creation, Filing, and Retrieval of Records. Section 6 doesn't have anything to do with the creation of a file.	The advisory committees agree with the suggestion to change the title to better reflect the contents of section 6. They decided to recommend the following title: "Storage, Maintenance, and Electronic Signing of Records."
3.	Superior Court of Riverside County By: Marita Ford Senior Management Analyst/PIO	On page 4, third paragraph, it states "Courts would be instructed to retain any data relevant to verifying electronic signatures, such as the signer's identity and the date and time that the signature is executed or adopted." And similarly on page 10, 4th bullet, it states "… the court should retain any data relevant to verifying the signature …". Questions • What data would need to be retained; and • What constitutes valid verification?	The advisory committees thank the court for its comments. In full, section 6.2.1.D provides that the "[t]he identity of the person who executed or adopted the electronic signature must be capable of verification. If a document is signed electronically, the court should retain any data relevant to verifying the signature, such as the identity of the person who executed or adopted the signature and the date and time that the signature was executed or adopted." Specifying precisely what data should be retained is beyond the scope of this proposal, as circulated. The advisory committees did not intend to limit the courts in how they implement this guideline. Instead, they envisioned that courts would work with their technology staff and any vendors to ensure that their technology systems retain data sufficient to identify the signer and when the signature was executed or adopted. However, to assist the courts, the committees decided to include a 'practice tip' that describes various types of data that courts may consider retaining. A valid verification would occur when the court is able to identify the signer and ascertain when the signature was executed or adopted, after the signature has been applied.

Trial Court Records Manual Version 4
Court Executive Advisory Committee and Information Technology Advisory Committee
Input and Recommendation

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Comment	Committee Response
		On page 9, paragraph D, it states that "Electronic Signatures Must Be … Capable of Verification." <u>Question</u> • In what manner must verification be made?	Specifying in precisely what manner the verification must be made is beyond the scope of this proposal, as circulated. The committees did not intend to limit the courts in how they implement this guideline. Instead, they envisioned that courts would work with their technology staff and any vendors to ensure that their technology systems are capable of identifying the signer and verifying when the signature was executed or adopted.
		On page 12-13, under examples of court-created documents: <u>Questions</u> • Would the electronically signed writs be accepted by each individual sheriff's department for enforcement; and • Would the electronically signed exemplifications be accepted in jurisdictions outside of our state?	By complying with the proposed electronic signature standards and guidelines, documents that are electronically signed by judges and courts will satisfy the requirements of Government Code section 68150(g), which recognizes that these documents have "the same validity, and the same legal force and effect" as paper documents bearing original signatures. This statutory authorization is broadly worded to apply to "[a]ny notice, order, judgment, decree, decision, ruling, opinion, memorandum, warrant, certificate of service, writ, subpoena, or other legal process or similar document issued by a trial court or by a judicial officer of a trial court." It is beyond the scope of this proposal, as circulated, to address how courts might work with justice partners and other outside parties to ensure that electronically signed documents are recognized as having "the same validity, and legal force and effect" as paper documents bearing original signatures.

Trial Court Records Manual Version 4
Court Executive Advisory Committee and Information Technology Advisory Committee
Input and Recommendation

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Comment	Committee Response
		Clarification on Section 6.2.2, B, (A) "When a document to be filed requires the signature, not under penalty of perjury, of an attorney or self-represented party, the document shall be deemed signed by that attorney or self-represented party if filed electronically." Question If the document is filed electronically with no signature at all (electronic or not) is it deemed signed? Or should it read "if signed and filed electronically"? Same question for Section 6.2.2,b B, (b).	Sections 6.2.2.B restates the language in Code of Civil Procedure section 1010.6(b)(2) and rule 2.257 of the California Rules of Court. Because this language is copied directly from the statute and rule, the advisory committees decline the invitation to revise the proposed update. In the future, the committees may consider whether to propose amending the statute and rule to clarify any ambiguities.

Trial Court Records Manual

EFFECTIVE JANUARY 1, 2011

REVISED JANUARY 1, ~~2014~~2016

JUDICIAL COUNCIL OF CALIFORNIA

ADMINISTRATIVE OFFICE OF THE COURTS

Trial Court Records Manual

Effective January 1, 2011

Revised January 1, ~~2014~~2016

JUDICIAL COUNCIL OF CALIFORNIA
ADMINISTRATIVE OFFICE OF THE COURTS

CONTENTS

1. Introduction 1

1.1 Background 1
1.2 Purpose of Records Management 3
1.3 Purpose of the Manual 4
1.4 Life Cycle of a Record 5
1.5 Key Definitions 6

2. Statutes and Rules of Court Governing Trial Court Records Management 7

2.1 California Government Code 7
2.1.1 Signatures on Electronically Created Court Documents 7
2.2 California Rules of Court 7

3. Records Management Administration 9

3.1 Application of Standards 9
3.2 Responsibility for Effective Records Management 9
3.3 Duties and Responsibilities of Records Managers 9
3.4 Records Management Training 10

4. Creation, Filing, and Retrieval of Court Records 11

4.1 Court Record Creation Process 11
4.1.1 Filing Papers in Court: Methods of Filing 11
4.1.2 Filing Papers in Court: Form and Format Requirements 17
4.1.3 Filing Papers in Court: Role of Civil Fees and Fee Waivers 18
4.2 Numbering Schematic for Court Records 20
4.3 Filing Systems for Court Records Maintained in Paper Format 21
4.3.1 Numerical Filing Systems by Case Numbers 21
4.3.2 Alphanumeric Filing Systems by Case Numbers 21
4.3.3 Terminal Digit Filing Systems by Case Numbers 22
4.4 Electronic Format Filing Protocols 23
4.4.1 E-Filing Overview 23
4.5 Court Record Location Tracking 23
4.5.1 Paper Record Tracking 23
4.5.2 Electronic File Tracking and Security 25

5. Record Classification 26

5.1 Standard Record Classifications 26
5.1.1 Case Record Classification 26
5.1.2 Prefiled Records 28

5.1.3 Lodged Records....28
5.1.4 Exhibits....28
5.1.5 Juror Records....28
5.2 Confidential and Sealed Records....28
5.3 Subpoenaed Records and Documents....29

6. Storage, Maintenance, and ~~Security~~ Electronic Signing of Records.... 30

6.1 Industry Standards for Storage of Paper and Electronic Records....30
6.1.1 Recommended Standards for Paper Records Storage Facilities....30
6.1.2 Recommended Standards for Managing Microfilm....31
6.1.3 Electronic Records....32
6.1.3.1 Process Review....33
6.1.3.2 File Format Best Practices....33
6.1.3.3 Color Palettes....36
6.1.3.4 Digital Imaging and Scanning Best Practices....37
6.1.3.5 Technology Refresh....41
6.1.3.6 Data Backup and Storage....42
6.1.3.7 Retention and Destruction....44
6.1.3.8 References....45
6.2 ~~Security and Protection~~Electronic Signatures: Standards and Guidelines....45
6.2.1. Electronic Signatures on Court-Created Records....45
6.2.2. Electronic Signatures on Documents Submitted to the Courts....50
6.2.3. Signatures on Scanned Documents....56

7. Exhibits Management .... ~~46~~57

7.1 Receiving, Handling, and Transfer of Exhibits in Criminal Cases....~~46~~57
7.2 Receiving, Handling, and Transfer of Exhibits in Civil Cases....~~46~~57
7.3 Protocols for Dangerous and Biohazard Exhibits....~~47~~58
7.3.1 Exhibits That Pose a Security, Storage, or Safety Problem....~~47~~58
7.3.2 Exhibits That Are Toxic....~~47~~58
7.3.3 Dangerous or Deadly Weapons, Poisonous Drugs, Explosives, or Any Property Prohibited by Law and Biological Material for DNA Testing....~~48~~59
7.4 Protocols for Cash Value, Historical Value, Narcotics, Sensitive Photographs, Private Property....~~48~~59
7.4.1 Exhibits Composed of Money or Currency of Unknown Ownership....~~48~~59
7.4.2 Exhibits Composed of Stolen or Embezzled Money or Currency....~~49~~60
7.4.3 Exhibits Composed of Property Other Than Money or Currency That Is Unclaimed....~~49~~60
7.4.4 Exhibits Composed of Property Value That Is Unclaimed....~~49~~60
7.4.5 Exhibits Composed of Photographs of Minors Deemed Harmful....~~49~~60
7.5 Death Penalty Exhibits....~~50~~61

8. Public Calendars, Indexes, and Registers of Action Minimum Standards .... ~~51~~62

8.1 Minimum Content for Court Calendars, Indexes, and Registers of Action 5162
8.2 Historical Data Fields Restrictions 5263

9. Disaster Recovery Planning and Procedures 5364

9.1 Planning for a Disaster 5364
9.2 Response to Disasters 5364
9.3 Disaster Recovery 5364

10. Public Access to Court Records 5566

10.1 Public Access to Trial Court Records 5566
10.1.1 Paper Court Records 5566
10.1.2 Electronic Court Records 5566
10.2 Remote Electronic Access Allowed in High-Profile Criminal Cases 5667
10.3 Confidential and Sealed Records 5767
10.3.1 Confidential Records 5767
10.3.2 Sealed Records 6576
10.4 Fees and Fee Waiver Guidelines for Requested Records 6576
10.5 Judicial Administrative Records 6576

11. Retention, Preservation, and Destruction of Court Records 6677

11.1 Retention, Preservation, and Destruction Practices 6677
11.1.1 Court Records Sampling Program 6778
11.2 Inactive Records Storage 6879
11.3 Cases Accepted for Review by the Supreme Court 6980
11.4 Schedule of Records Retention and Destruction and Special Case Type Characteristics 7081
11.4.1 Records Retention and Destruction Schedule under Government Code Sections 68152 and 68153 7081
11.4.2 Records Retention and Destruction Schedule for Other Case Types 8798
11.4.3 Records Retention and Destruction Schedule for Prefiled and Juror Records 8899

Appendices 89100

Appendix 1—Court Records Designated Confidential by Statute or Rule 90101
Appendix 2—Rotational Assignment for Longitudinal (100%) Sample 102113

Index 104115

1. Introduction

This Trial Court Records Manual (TCRM) has been developed by court administrators for court administrators and is published ~~by the Administrative Office of the Courts~~ under the direction of the Judicial Council of California. The vision of the court administrators and ~~AOC~~ Judicial Council staff who drafted the TCRM is to encourage and embrace input and participation from trial court leaders and subject matter experts in every court so that the TCRM is not only a reference manual of laws and rules governing court records management but also a repository for our best ideas and programs.

This TCRM is not considered final or complete; additional content will be drafted for subsequent versions and distributed to trial court leaders for comment as those versions become available.

As the Judicial Council adopts, and the trial courts begin to implement, new policies for the creation, maintenance, retention, and destruction of electronic records, the TCRM seeks to address the issues and challenges that trial courts will encounter with archival and current paper records, as well as to describe the new policies, business practices, and technology considerations that will lay a solid foundation for managing electronic records in the future. As the trial courts' business model changes with the advent of new technologies, courts are encouraged to develop strategic solutions that will position them to adapt to emerging trends in paperless records management.

To assist users in distinguishing between mandatory requirements and optional features of court records management programs, this icon precedes sections containing optional ideas, programs, and best industry practices. Sections **not** preceded by this icon contain mandatory requirements. Sections containing mandatory requirements typically contain links to the relevant statutes or rules.

This manual will be revised and updated periodically. Users are encouraged to submit in writing questions or suggestions for improving the TCRM to

Court Executives Advisory Committee
c/o ~~Administrative Office of the Courts~~Judicial Council of California
~~Judicial Council and Court~~ Leadership Services Division, Trial Court Liaison
455 Golden Gate Avenue, 5th Floor
San Francisco, CA 94102-3688

1.1 Background

The Judicial Council of California began developing and maintaining an overall records management framework for California courts to satisfy the needs of the courts for case processing and of historians and archivists for historical and research purposes served by court records, as well as the expectations of the public and litigants to provide reasonable confidentiality of court records. Many of the existing statutes, rules of court, and standards

include permissive minimums for court records retention and other options for court records management that allow courts significant latitude in applying them.

For many years, the management of trial court records has been costly and cumbersome because of several statutory and operational factors. These factors include the cost of transporting, preserving, and storing paper files and converting them to microfilm or microfiche; the outdated technologies allowed by statute to manage nonpaper records; the lack of staff resources dedicated to managing records; inadequate storage space near the courthouse to enable convenient access to records; and mandates for notification and destruction of records that are impractical and time-consuming.

The path to the current status has had many twists and turns. Prior to unification, trial court records were maintained by the county clerk, who served, by law, as the clerk of court. Municipal and justice court records were the responsibility of each court's clerk. Over time the clerk of court duties were transferred to the trial court executive officers. This was essentially complete across the state when the courts were merged at the end of the 1990s. However, at this point, there needed to be a merger of the records management systems of the two levels of court. Shortly after unification, primary funding for trial courts was shifted from the counties to the state. In addition to changing the source of funding, the change expanded the discretion of each trial court as to how to manage its records in terms of staffing, equipment, and, to a lesser extent, facilities. All of these transitions have changed the opportunities and challenges facing trial courts in establishing and maintaining an appropriate records management program.

The next stage of court records management involves the transition from paper records to records that are created and may exist only in electronic form. This involves both case management systems and document management systems containing document images. Some information in the future may exist only in electronic form and may consist only of data in fields of a case management system and not as a form readily converted to paper. A comprehensive records management system must contemplate and enable the shift to electronic records.

In December 2009, the Judicial Council of California's Court Executives Advisory Committee and Court Technology Advisory Committee cosponsored a proposal for Judicial Council–sponsored legislation to amend Government Code sections 68150 and 68151 pertaining to the creation, maintenance, retention, and destruction of trial court records. The proposed amendments were intended to give more latitude to the trial courts to manage and retain court records using modern technologies and to transfer the oversight of such activities from the Legislature to the Judicial Council and the trial courts. The court records legislation was introduced as Assembly Bill 1926 (Evans) in 2010. It amended the law on court records management, effective January 1, 2011, to authorize the council to adopt rules to establish guidelines for the creation, maintenance, reproduction, and preservation of court records.

The changes to the Government Code required the adoption of new California Rules of Court to establish standards and guidelines for the creation, maintenance, reproduction, and preservation of trial court records. In October 2010, the council adopted new rules 10.850

and 10.854, and amended rule 10.855. Rule 10.850 references the existing Government Code section 68151 on the definition of "court records." Rule 10.854 directs the Judicial Council's Administrative ~~Office~~ Director ~~of the Courts~~ to develop and distribute standards and guidelines for managing trial court records by creating a TCRM. The rule also provides direction for the content of the TCRM and mandates its periodic update. Rule 10.855 is modified to include requirements in the TCRM for court records preserved as part of the comprehensive, systematic, and subjective sampling programs. The new and amended rules became effective on January 1, 2011. On the same date, the initial version of this manual became effective.

1.2 Purpose of Records Management

The provision of a complete, accurate, and accessible court record, created and available in a timely manner, fulfills one of the judiciary's basic roles. The court record not only provides a record of the court's decisions but also educates the public and establishes societal norms for behavior governed by the law. The purpose of developing a TCRM is to assist the trial courts in establishing a comprehensive records management program that meets the expectations of the courts and the public regarding this fundamental role.

The establishment and continued operation of a comprehensive records management program is the responsibility of the court's executive officer. The National Association of Court Management (NACM) Core Competency Curriculum Guidelines on Essential Components identifies what court executives should know and be able to do regarding the court record. The key abilities are described as follows:

- Manage the court record-keeping function to produce a complete, accurate, and timely record of judicial actions and decisions.
- Establish court records management policies and practices, including records preparation, records retention, public access, and privacy protections.

A comprehensive records management program covers the creation, maintenance, retention, and destruction of trial court records. Each component may have several elements and objectives.

The CREATION of the court record involves two sets of information. One set includes documents and other information provided by the parties to aid the court in making its decisions, for example, pleadings, motions, exhibits, and so forth. The litigants, the appellate courts, and the public must be able to see all the information the court considered in making its decision, except what has been sealed or is subject to rules protecting the confidentiality of the information. The second set is the documentation of what the court did and decided. This includes matters related to calendaring and case management, as well as decisions of the court and juries. For litigants and the public to know what they can, and cannot, do, they need clear information about what the court found the law to be and how it was applied in this case.

The MAINTENANCE of the court record addresses the continued existence and accessibility of the record. The record must be kept in a manner that ensures its completeness and availability both during the life of an active case and after it is closed, where the result may still be relevant to the parties and the public. It must also be kept in a manner that allows easy and convenient access to those wanting to see it. The court should be able to find the record easily when the record is needed. Making copies of the record should also be convenient and inexpensive. Finally, the format in which the record is kept should allow ready access over time, despite changes in technology, in particular, obsolescence of equipment and software required to access electronic forms of a record.

Another aspect of maintenance is preserving the record's integrity; the court record should be the whole record and nothing but the record. The system for maintaining court records should minimize the risk of misfiling, loss, or damage of the court record or any of its parts.

Finally, good records management involves controlling who has access to the record or its component parts. There may be portions of the record that, by law or judicial decision, are accessible only to certain individuals, parties, or groups of individuals based on their role in the justice system. A good records management program should provide convenient and timely access to those allowed to see information, and prevent access by those not authorized to see it.

The RETENTION of the court record relates to how long it must be available to the public. Some court records must be retained indefinitely; others have a limited "shelf life" and need not be retained.

The DESTRUCTION of the court record is the final stage of a records management program. When the existence of a court record is no longer required, based on passage of time or a policy decision, the record should be properly destroyed. Whether the record ceases to exist, or becomes accessible only to certain groups, is a policy decision that the records management program must correctly implement.

The goal of this TCRM is to provide direction to the court executive and staff on ways to develop and improve their records management system to fulfill the objectives of faithfully executing all custodial responsibilities pertaining to the court record.

1.3 Purpose of the Manual

The purpose of the TCRM is twofold. First and foremost, it contains the statutory and rule requirements with which all trial courts must comply to meet minimum standards to execute their important responsibilities pertaining to managing paper and electronic court records. Second, the TCRM is intended to be a resource guide for court administrators and records staff to help them develop records management programs that best serve their local courts. It includes a broad, though perhaps not exhaustive, list of topics that all courts are encouraged to address to ensure that they have comprehensive and effective local records management programs.

The optimal way to use the TCRM is in electronic form, as there are hyperlinks to reference materials, statutes, and other source documents throughout this publication. ~~AOC~~ Judicial Council staff will make every effort to regularly refresh and update links so that the TCRM is a current and relevant resource for records management staff.

In addition to providing a resource that will contain all of the relevant statutes, rules, requirements, industry standards, and many best practices for court records management, the TCRM will also include a retention and destruction table for court records that is organized in a simple, readable format and includes links to the underlying authority for record retention in every case type.

1.4 Life Cycle of a Record

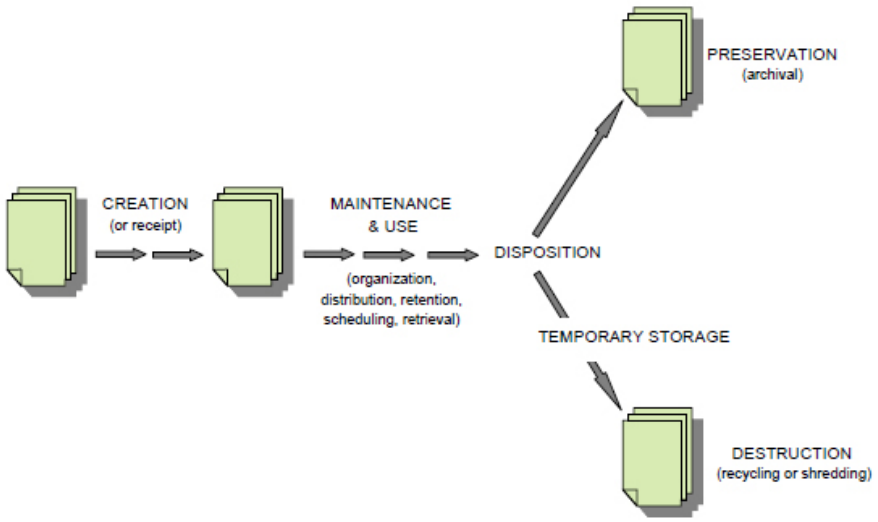
Courts often make the fundamental error of viewing records management only as the sampling, archiving, and destroying of case files in accordance with various statutes and rules of court. This manual is predicated on an expanded definition of records management that encompasses the complete life cycle of court documents from initial filing to final storage and destruction. As documents travel down this path, they will need to be transported to various court locations and viewed by multiple staff members, parties to the case, and others for various purposes. Archiving and destruction is just one step in the process.

Records management typically begins with document management. A comprehensive and effective records management program addresses the numerous issues and questions that arise in the life cycle of court documents. Here are just a few examples:

- How are documents to be captured and processed when initially filed?
- Who will need to access them at various points in the adjudication process?
- What method will be used to organize, store, and retrieve documents as cases are processed and disposed?
- What resources are necessary to track and manage individual documents and case file locations and security?
- How are electronic technologies used to access documents in place of the movement and viewing of physical files?

Courts that develop clear and comprehensive answers to these issues and questions are well positioned to have an effective document management system. The manner in which documents are captured and managed at the beginning and middle portions of their life cycle can often determine the ease and efficiency by which they are finally archived and destroyed. More importantly, extensive savings in staff time and financial resources can be achieved through a well-designed, comprehensive documents management program that also enables greater access to court records and services by staff, judicial officers, case parties, and other members of the general public.

Records Life Cycle



1.5 Key Definitions

Court Record
Any document, paper, or exhibit filed by the parties to an action or proceeding; any order or judgment of the court; and any item listed in Government Code section 68151(a), excluding any reporter's transcript for which the reporter is entitled to receive a fee for any copy. The term does not include the personal notes or preliminary memoranda of judges or other judicial branch personnel. (Cal. Rules of Court, rule 2.502.)

Electronic Record
A computerized court record, regardless of the manner in which it has been computerized, is a term that includes both a document that has been filed electronically and an electronic copy or version of a record that was filed in paper form. The term does not include a court record that is maintained only on microfiche, paper, or any other medium that can be read without the use of an electronic device. (Cal. Rules of Court, rule 2.502.)

Records Management
The systematic control of recorded information required to operate a court's business, including creation, active maintenance and use, inactive storage, and final disposition.

2. Statutes and Rules of Court Governing Trial Court Records Management

This section lists the principal statutes and rules of court that relate to trial court records.

2.1 California Government Code

Sections 68150 to 68153
Government Code sections 68150 through 68153 prescribe how trial court records are to be maintained and preserved, specify how long different types of records must be preserved, and provide procedures for the destruction of records.

2.1.1 Signatures on Electronically Created Court Documents

Government Code section 68150(g) provides that any notice, order, judgment, decree, decision, ruling, opinion, memorandum, warrant, certificate of service, or similar document issued by a trial court or judicial officer of a trial court may be signed, subscribed, or verified using a computer or other technology. ~~Future versions of this manual will contain procedures, standards, or guidelines for signing, subscribing, and verifying court documents by electronic means.~~Section 6.2.1 of this manual provides standards and guidelines for signing, subscribing, and verifying court documents by electronic means.

Section 68511.2
Government Code section 68511.2 provides that the Judicial Council shall provide by rule for the photographic, microphotographic, mechanical, or electronic entry, storage, and retrieval of court records.

2.2 California Rules of Court

General Provision for Court Records
Rule 2.400. Court records

Trial Court Records Management
Rule 10.850. Trial court records definition
Rule 10.851. Court indexes—automated maintenance
Rule 10.854. Standards and guidelines for trial court records
Rule 10.855. Superior court records retention program

Public Access to Electronic Records
Rule 2.500. Statement of purpose
Rule 2.501. Application and scope
Rule 2.502. Definitions
Rule 2.503. Public access

Rule 2.504. Limitations and conditions
Rule 2.505. Contracts with vendors
Rule 2.506. Fees for electronic access
Rule 2.507. Electronic access to court calendars, indexes, and registers of actions

Sealed Records
Rule 2.550. Sealed records
Rule 2.551. Procedures for filing records under seal

3. Records Management Administration

3.1 Application of Standards

The TCRM sets forth standards and guidelines for court records maintained of the California trial courts. The TCRM will be periodically updated to reflect changes in statutes, rules of court, or technology that affect the creation, maintenance, retention, and destruction of court records. As previously noted, except for technical or minor (nonsubstantive) changes not likely to create controversy, proposed revisions to the TCRM will be circulated to the trial courts for comment before the TCRM is updated or revised. Pursuant to California Rules of Court, rule 10.854(c), courts will be notified of any changes in standards or guidelines, including all those pertaining to the permanent retention of records.

Each trial court must develop records management practices consistent with minimum standards authorized in statutes and rules of court, as delineated in the TCRM. Moreover, trial courts are also encouraged to review guidelines described in the TCRM and develop local programs that reflect these policies and practices. Standards and guidelines are intended to lead to more efficient and uniform practices among trial courts to ensure better protection and preservation of and improved public access to trial court records.

3.2 Responsibility for Effective Records Management

The trial court executive officer, as part of the enumerated duties in California Rules of Court, rule 10.610, and Government Code sections 69840 through 69848, shall oversee the creation, maintenance, retention, and destruction of trial court case records in accordance with all applicable laws, rules of court, and guidance provided in the TCRM. The court executive officer may delegate these duties to subordinate staff members who serve as records managers.

3.3 Duties and Responsibilities of Records Managers

Trial courts have developed many effective records management programs and practices. For the purposes of this manual, the duties of effective records managers have been identified and may include the following:

- plan for the management and control of records;
- recommend procurement of records management equipment and supplies;
- investigate and recommend new technologies;
- implement standard procedures;
- conversion and transfer of paper records to other media, and establish and oversee the primary and backup storage systems for these records;
- develop disaster recovery programs in the event that primary data systems become damaged or inoperable;

- maintain the inventory of records;
- manage records destruction programs, which includes ensuring that appropriate notices of destruction are prepared and disseminated by mail or publication, monitoring the destruction of records, validating records destruction, and obtaining certificates of destruction from qualified service providers;
- research new and emerging technologies that are designed to assist organizations with records management;
- monitor inventory and maintain security at off-site storage; and
- train subordinates and representatives of related entities in records management.

3.4 Records Management Training

(Training and curriculum content will be developed in the next version of TCRM.)

4. Creation, Filing, and Retrieval of Court Records

Records management is a specialized field of court administration for determining how records will be organized, categorized, and stored, and in what format (paper or electronic). Establishing an efficient system to create, file, and retrieve court records involve careful planning to ensure productive workflow. This includes

- developing clear protocols on how records are created;
- devising case type and numbering classification systems that convey meaningful information to those who access the records;
- deciding how records will be organized in paper and electronic filing systems;
- determining the best methods for tracking the movement of records within the court and among court facilities; and
- researching and selecting the proper equipment (shelving, tracking applications, scanners) and supplies (file folders, labels, bar codes).

4.1 Court Record Creation Process

One of the most basic and critical functions performed by trial courts is the creation and maintenance of the case record. The case record consists of documents filed by attorneys, self-represented litigants, local justice agencies, and other case parties who submit documents to the court. In some instances, courts also create and file documents. This section of the TCRM is intended to provide court staff with suggested guidance regarding the creation and maintenance of the case record. It is divided into three subparts applicable to documents submitted by attorneys, self-represented litigants, and others involved in cases, but not those prepared by the court itself.

4.1.1 Filing Papers in Court: Methods of Filing

Effective Filing Date – Currently, courts receive legal documents for filing and processing through various means including:

- Over the counter
- By mail
- By drop box
- E-filed directly or through e-filing service provider (EFSP)
- As an attachment to e-mail (often referred to as e-delivery)
- By fax

Government Code section 69846.5 states, “The clerk of the superior court shall endorse on each paper filed with the court the day, month, and year it is filed.” The issue of when a paper is deemed “filed” depends on the applicable law for the mode of delivery and the type of filing. To assist courts in determining the effective filing date for court documents, the

following is a list of applicable statutes and California Rules of Court for documents received through various means.

Note that the filing date depends on when the document was received by the court, not when the court completed processing of the document. It takes a finite amount of time for the clerk's office to review a document, determine whether it meets filing criteria as to form and attachments, check the fee payment, if any, enter data into a register of action or case management system, and scan the document, if scanning is done. These steps may take several minutes, spread over several hours. As a result, the document processing may not be complete on the same day the document is received. Nonetheless, the filing date should be the date received.

- **Filing in person** – Rule 1.20 of the California Rules of Court. (See Cal. Rules of Court, rule 1.20(a): "Unless otherwise provided, a document is deemed filed on the date it is received by the court clerk.")

- **Filing by mail** – Rule 1.20 of the California Rules of Court. (See Cal. Rules of Court, rule 1.20(a): "Unless otherwise provided, a document is deemed filed on the date it is received by the court clerk.")

- **Filing at drop box** – Government Code section 68108(b) and rule 2.210 of the California Rules of Court. (See Cal. Rules of Court, rule 2.210(b): "Any document deposited in a court's drop box up to and including 4:00 p.m. on a court day is deemed to have been deposited for filing on that day. A court may provide for same-day filing of a document deposited in its drop box after 4:00 p.m. on a court day. If so, the court must give notice of the deadline for same-day filing of a document deposited in a drop box." See also Cal. Rules of Court, rule 2.210(c): "Any document deposited in a court's drop box is deemed to have been deposited for filing on the next court day if: (1) It is deposited on a court day after 4:00 p.m. or after the deadline for same-day filing if a court provides for a later time; or (2) It is deposited on a judicial holiday.")

- **Filing electronically** – Code of Civil Procedure section 1010.6 and rule 2.259 of the California Rules of Court. (See Code Civ. Proc., § 1010.6(b)(3): "Any document that is electronically filed with the court after the close of business on any day shall be deemed to have been filed on the next court day. 'Close of business,' as used in this paragraph, shall mean 5 p.m. or the time at which the court would not accept filing at the court's filing counter, whichever is earlier." See Cal. Rules of Court, rule 2.259(c): "A document that is received electronically by the court after the close of business is deemed to have been received on the next court day." Note: Assembly Bill 2073 has authorized a different legal standard for documents filed electronically under the mandatory e-filing pilot project, effective January 1, 2013, in the Superior Court of Orange County: the law allows documents filed in that pilot project before midnight on a day to be deemed filed on that day. (See Code Civ. Proc., § 1010.6(d)(1)(D) (the court "may permit documents to be filed electronically until 12 a.m. of the day after the court date that the filing is due, and the filing shall be

considered timely.") However, as of January 1, 2013, when the TCRM, Version 2.0 became effective, the Superior Court of Orange County had not yet adopted this different standard for the effective time of papers filed electronically in that court.

The California Rules of Court also recognize that a technical problem with a court's electronic filing system may warrant deeming certain late-filed documents as filed when the attempt was made to file the documents rather than when the documents were actually received by the court. (See Cal. Rules of Court, rule 2.259(d): "If a technical problem with a court's electronic filing system prevents the court from accepting an electronic filing during its regular filing hours on a particular court day, and the electronic filer demonstrates that he or she attempted to electronically file the document on that day, the court must deem the document as filed on that day. This subdivision does not apply to the filing of a complaint or any other initial pleading in an action or proceeding.")

These laws apply to both e-filed documents and e-delivered documents as the statute contemplates the method of transmission ("electronically") not the form of the document or message.

- **Filing by fax** – Filing through a fax filing agency under rule 2.303 and rule 1.20 of the California Rules of Court; For direct fax filing with the court under rule 2.304 and rule 1.20 of the California Rules of Court. (See Cal. Rules of Court, rule 2.304 containing provisions specifying, when a party directly fax files with the court, how failures of transmission and rejection of credit card charges are to be handled.)

- **Filing on a court holiday** – Code of Civil Procedure section 134(d): "The fact that a court is open on a judicial holiday shall not make that day a nonholiday for purposes of computing the time required for the conduct of any proceeding nor for the performance of any act. Any paper lodged with the court at a time when the court is open pursuant to subdivision (c), shall be filed by the court on the next day that is not a judicial holiday, if the document meets appropriate criteria for filing."

Courts are encouraged to consult these statutes and rules when assessing their filing processes and procedures and seek assistance from local counsel or the ~~AOC~~ Judicial Council's Legal Services ~~Office~~ if they have specific questions or issues in this regard.

Filing redacted documents – Rule 1.20 of the California Rules of Court. The California Rules of Court require that certain sensitive information—specifically, social security numbers and financial account numbers—must be redacted or excluded from documents filed with the court, with certain exceptions (see Cal. Rules of Court, rule 1.20(b)(3)): The responsibility for excluding or redacting information from documents filed with the court rests solely with the parties and their attorneys, not the clerk (see Cal. Rules of Court, rule 1.20((b)(3).) The rule on redaction provides that the court clerk will not review each pleading or other paper for compliance.

Filing records that are confidential as a matter of law – For direction in dealing with confidential records, see section 10.3.1, "Confidential Records," and Appendix 1. Depending on the law, entire cases, categories of cases, or individual documents in a case may be confidential. Also, some case files and/or documents may be permanently classified as confidential while others may be confidential only for a specified period of time.

Filing records under seal – For direction in dealing with court files and documents ordered sealed, see section 10.3.2, "Sealed Records." Also, you may consult the following California Rules of Court:

- Filing records under seal – Rule 2.551(a) of the California Rules of Court: "A record must not be filed under seal without a court order."
  Rule 2.551(f) of the California Rules of Court: "Sealed records must be securely filed and kept separate from the public file in the case."
  Rule 2.551(d) of the California Rules of Court, also contains procedures for conditionally lodging documents that may be filed under seal.

- Filing records under seal in a False Claims Act case – Rule 2.571 of the California Rules of Court.

Types of Documents Maintained in Case Files and Elsewhere (Filed Documents and Other Documents Submitted, Lodged, or Deposited with the Court)
"The clerk of the superior court shall safely keep or dispose of according to law all papers and records filed or deposited in any action or proceedings before the court." (Gov. Code, § 69846.)

Official court documents used in the adjudication of the actions or proceedings such as complaints, petitions, answers, responses, and motions with or without attached exhibits, are filed with the court and included in the register of actions, if kept. In addition, parties lodge, deposit, or submit various other documents that are not officially filed and entered into the register of actions.

There are several types of documents that are accorded different treatments based on statutes and rules. To assist courts in determining the appropriate manner of handling these types of documents, the following information is provided:

- **Administrative records** – "Court records" include administrative records "filed in an action or proceeding…." Government Code section 68151(a)(2). In addition, some statutes and rules specifically require particular administrative records to be "lodged" with the court. (See for example, on CEQA actions, Pub. Resources Code, § 21167.6(b)(1) (providing for the lodging of CEQA records by the public agency) and Cal. Rules of Court, rule 3.1366 ("The party preparing the administrative record must lodge it with the court and serve it on each party….").)

- **Arrest Warrants with No Existing Related Case –** Law enforcement and other agencies can request that the court issue an arrest warrant. Often there is not yet a

filing or case involving the proposed arrestee, and there may never be a court filing. Consequently, the court will have arrest warrants issued by a judge that are not associated with any case at the time of issuance.

Because arrest warrants may not be associated with a particular case, it is important for the court to have a specific procedure for identifying, storing, and retrieving every warrant. In this system, arrest warrants should typically be indexed by the name of the person to be arrested.

There are several options for where to maintain arrest warrants, given the possibility that a case will be filed related to a warrant. When a case is subsequently filed, it can be very problematic for court staff to identify the existence of an associated arrest warrant, let alone find the warrant and place it in or link it to the case file. One option is to have court staff attempt to match "orphan" arrest warrants with new cases as they are filed, though this may be a time-consuming activity for relatively infrequent occurrences. A second option is to leave warrants in the location where they were originally placed and for court staff to locate a warrant when an issue about the warrant is raised in a particular case. While this involves less work for the clerk's office, being done only when needed, it still places the burden on the clerk to find the arrest warrant. Another option would be for the court to indicate to parties that if they raise an issue about the warrant, they should contact the agency that originally requested the warrant to produce the warrant. This will lessen the burden on court staff to spend resources locating the warrant in a particular case. If the agency cannot find the warrant and supporting documents, or there is a question about the validity of the documents offered, the court can then direct the clerk to produce the documents maintained by the court.

The arrest warrants should be retained for the period provided by statute, as they document the decisions of a judicial officer, which may be litigated in a subsequently filed case. (See Gov. Code, § 68152(c)(15).)

Certain arrest records may be confidential. See section 10.3.1, "Confidential Records, and Appendix 1.

- **Court transcripts** – Some court reporter's transcripts, such as preliminary hearing transcripts and transcripts prepared as part of an appellate record, may be included in the case file. Although part of the case file, these transcripts are subject to different requirements from other records in the case file with respect to copying and electronic access. Courts generally may not provide or sell a copy of a transcript to a party or other person without an additional fee being paid to the court reporter (Gov. Code, § 69954) and any reporter's transcript for which the reporter is entitled to receive a fee for any copy is explicitly excluded from the definition of "court record" for purposes of the rules on Public Access to Electronic Trial Court Records (Cal. Rules of Court, rule 2.502(1)). If a request is received for a copy of a reporter's transcript, the interested party should be directed to contact the court reporter who reported the hearing to obtain a copy for a fee. (See Gov. Code § 69954.)

- **Exhibits** – see section 5.1.4

- **Juror Records** – see section 5.1.5

- **Lodged Records** – see, section 5.1.3

- **Mandatory settlement conference statements** – These statements are submitted to the court rather than filed and should be transmitted to the judicial officer who will conduct the conference. California Rules of Court, rule 3.1380(c) states, "No later than five court days before the initial date set for the settlement conference, each party must submit to the court and serve on each party a mandatory settlement conference statement…."

- **Prefiled Records** – see section 5.1.2

- **Proposed orders** – Proposed orders in civil cases are governed by rule 3.1312 of the California Rules of Court. These are generally submitted to the court rather than filed and should be transmitted to the appropriate judicial officer for further action. (See Cal. Rules of Court, rule 3.1312(b).) Special procedures exist for handling proposed orders that are submitted electronically—two versions of the proposed order must be submitted to the court: (1) a PDF version attached to a completed *Proposed Order (Cover Sheet)* (form EFS-020), which is filed, and (2) a version in an editable word-processing format, which is made available for the judge's use. (See Cal. Rules of Court, rule 3.1312(c).)

- **Search warrants** – See discussion and options under "Arrest Warrants" on page 14. Because search warrants may not be associated with a particular case, it is important for the court to have a specific procedure for identifying, storing, and retrieving every search warrant. For example, search warrants could be indexed by the location of the place to be searched.

  Certain search warrants or information contained in a search warrant may be confidential. See section 10.3.1, "Confidential Records," and Appendix 1.

- **Trial subpoenas** – See section 5.3, "Subpoenaed Records and Documents."

- **Wills** – Original wills must be delivered to the court under Probate Code section 8200 – Production of Will. Probate Code section 8200(a) states: "Unless a petition for probate of will is earlier filed, the custodian of a will shall, within 30 days after having knowledge of the death of the testator…[d]eliver the will to the clerk of the superior court of the county in which the estate of the decedent may be administered."

  An original will is lodged or deposited with the court rather than filed; however, a copy of the will must be attached to the petition for probate filed with the court. (See Prob. Code, § 8002(b)(1).)

Letters and other correspondence – Generally, correspondence sent to the court should be placed in the same physical file with the other documents in a case (pursuant to Gov. Code, § 69846) but is not entered into the register of actions. The correspondence should be organized separately from the filed documents. The correspondence may be marked with a "received" stamp and placed in the file in chronological order. Courts maintaining records in electronic form should consider establishing a process or procedure for addressing correspondence received in the case, separate from the documents that are filed.

Some correspondence may require special treatment. For example:

Correspondence requesting action – Correspondence that seeks a particular action should be processed by the court or judicial officer, as appropriate. Thus, letters containing proposed orders should be transmitted to the appropriate judicial officer. A request for copies of court documents should be processed by the court if the requesting party has paid the costs of copying and mailing. Complaints against judicial officers should be processed in accordance with the court's procedures. (See Cal. Rules of Court, rule 10.703 (subordinate judicial officers) and rule 10.746 (temporary judges).)

Ex parte communications – Correspondence that seeks to communicate with the judicial officer handling a matter, without a copy being served on other parties that have appeared in the action, should not be placed in the file where it might be seen by a judicial officer involved in the case. Instead, courts should develop procedures whereby such communications are returned to the submitting party with an explanation as to why the document was not placed in the case file.

4.1.2 Filing Papers in Court: Form and Format Requirements

Form and format of papers filed in the trial courts – Rules 2.100–2.116 of the California Rules of Court, prescribe the form and format of papers presented for filing to the trial courts. These rules preempt any local rules on the form and format of papers. (Cal. Rules of Court, rule 2.100.) The form and format requirements in rules 2.100–2.116 do not apply to Judicial Council forms, local forms, or forms for juvenile dependency proceedings. (Cal. Rules of Court, rule 2.119.)

Court's acceptance or rejection of papers for filing – The clerk of the court must not accept papers for filing that do not comply with the form and format requirements in rules 2.100–2.116 of the California Rules of Court, except the clerk must not reject a paper for filing solely on the ground that (1) it is hand-written or hand-printed, or (2) the handwriting or hand printing on the paper is in a color other than black or blue-black. (Cal Rules of Court, rule 2.118(a).) The clerk also must not reject a paper for filing solely on the ground that it does not contain an attorney's or a party's fax number or e-mail address on the first page. (Cal Rules of Court, rule 2.118(b).) For good cause, the court may permit the filing of papers that do not conform to the form and format requirements. (Cal. Rules of Court, rule

2.118(c).) While the responsibilities of the clerk under (a) and (b) are ministerial, the good cause determination to permit filing under (c) is a judicial function.

Duty to file documents – "If a document is presented to the clerk's office for filing in a form that complies with the rules of court, the clerk's office has a ministerial duty to file it. (See *Carlson v. Department of Fish & Game* (1998) 68 Cal.App.4th 1268, 1276.) Even if the document contains defects, the clerk's office should file it and notify the party that the defect should be corrected. (See *Rojas*…67 Cal.App.4th at p. 777.)" *Voit v. Superior Court*, 201 Cal.App.4th 1285, 1287.)

Effect of failure to submit civil case cover sheet – The first paper filed in a civil action or proceeding must be accompanied by a completed *Civil Case Cover Sheet* (form CM-010). (Cal. Rules of Court, rule 3.220(a).) But if a party that is required to provide a cover sheet under rule 3.220 or a similar local rule fails to do so or provides a defective or incomplete cover sheet at the time the party's first paper is submitted for filing, the clerk must still file the paper; failure to file a cover sheet may subject a party or its counsel to monetary sanctions. (Cal. Rules of Court, rule 3.220(c).)

4.1.3 Filing Papers in Court: Role of Civil Fees and Fee Waivers

Effects of Failure to Pay All Required Filing Fees – The effect on filing of a failure to pay filing fees depends, among other things, on:

- Whether the party is required to pay a filing fee
- Whether an application for a fee waiver was submitted
- Whether the party paid no fee at all
- Whether the amount tendered was less than the amount of the required fee
- Whether the amount was tendered by a check that was returned for insufficient funds
- Whether a credit card payment was rejected

The following additional information is provided regarding filing fees and fee waivers:

- **Schedule of fees** – A statewide civil fee schedule is available online at: *http://www.courts.ca.gov/documents/StatewideCivilFeeSchedule-20140101.pdf*. Many courts also prepare their own fee schedules. The schedules list the documents which, upon filing, require payment of a fee and the amount of the fee. Note: (1) Certain documents do not require payment of a fee to be filed (See e.g., Gov. Code, § 70617(b).); (2) Government entities are generally exempt from paying civil filing fees. (See Gov. Code, § 6103); for some other exemptions from fees for court services, see Gov. Code, § 70633.)

- **No fee paid** – If a party is required to pay a fee for filing a particular document and no fee is tendered, the court may reject the filing unless the party has submitted a fee waiver application with its papers or a fee waiver has previously been granted in the action.

- **Fee waivers** – Government Code sections 68630–68641; California Rules of Court, rules 3.50–3.58. The clerk shall accept all applications for an initial fee waiver for filing. If an applicant submits an application without providing all required information to complete the form, the clerk may request that the applicant supply the omitted information, but shall not refuse to file the application, or refuse to file any pleadings accompanying the application, on the ground that the fee has not been paid. (Gov. Code, § 68634(b).)

- **Amount tendered is less than the amount of the required fee** – Code of Civil Procedure section 411.21. If a complaint or other first paper, except in an unlawful detainer action, is accompanied by a check in an amount less than the required fee, the clerk shall accept the paper for filing, but shall not issue a summons until the court receives full payment of the required fee. The court, by mail, shall notify the party tendering the check that (1) the check was made out for an amount less than the required filing fee, (2) the administrative charge specified in the statute has been imposed to reimburse the court for the costs of processing the partial payment and providing the notice, and (3) the party has 20 days from the date of mailing of the notice within which to pay the remainder of the required fee and the administrative charge, except where a hearing is scheduled before the 20-day period expires.

  The clerk shall void the filing if the party who tendered a check in an amount less than the required filing fee or on whose behalf a check in an amount less than the required filing fee was tendered has not paid the full amount of the fee and the administrative charge within 20 days of the date on which the notice was mailed.

  Any filing voided by the section may be disposed of immediately after the 20 days have elapsed without preserving a copy in the court records, notwithstanding Government Code section 68152. (See Code Civ. Proc., § 411.21(a)–(e) for more details; for information concerning the administrative fee, see Code Civ. Proc., § 411.21(g).)

- **Check for fee amount is returned for insufficient funds** – Code of Civil Procedure section 411.20. If the clerk accepts for filing a complaint or other first paper, or any subsequent filing, and payment is made by check that is later returned without payment, the clerk shall, by mail, notify the party who tendered the check that (1) the check has been returned without payment, (2) the administrative charge specified in the statute has been imposed to reimburse the court for the costs of processing the returned check and providing the notice, and (3) the party has 20 days from the date of mailing of the notice within which to pay the filing fee and the administrative charge, except where a hearing is scheduled before the 20-day period expires. The notice also shall state that the administrative charge and the filing fee shall be paid in cash, by certified check, or by other means specified by the court, but not by traveler's check or personal check.

  The clerk shall void the filing if the party who tendered a returned check or on whose behalf a returned check was tendered has not paid the full amount of the fee and the

administrative charge by a means specified in the statute within 20 days of the date on which the notice was mailed.

Any filing voided by this section can be disposed of immediately after the 20 days have elapsed without preserving a copy in the court records, notwithstanding Government Code section 68152. (See Code Civ. Proc., § 411.20 (a)–(f) for more details; for information concerning the administrative fee, see Code Civ. Proc., § 411.20(g).)

- **Credit card payment is rejected** – Credit card payments rejected by the processing center should be treated as any other failure to pay a filing fee. In most cases, the person submitting the payment (e.g., at the counter or over the Internet) is immediately notified of the rejection and can provide payment in some other manner. If a request for credit card payment is received through the mail but rejected by the processing center, the court should notify the submitting party of the rejection using the same procedures utilized when a check is rejected by the bank as described in the previous section of this manual. The only exception is that there should be no administrative charge added to the amount owing.

4.2 Numbering Schematic for Court Records

A case numbering system should be rational and meaningful and should convey information to court staff and other users that will help them understand how court records are organized. The numbering system must ensure that each case has a unique number to minimize confusion and facilitate locating and filing the case and its associated documents. The case number may include key information that includes year of filing, case type, and a sequential identifying number. For example, a case number may consist of

1. court jurisdiction identifier;
2. the last two digits of the filing year;
3. an alpha or numeric code to designate case type (e.g., CR for criminal, CV for civil);
4. a continuous sequentially assigned number related to that case type; and
5. additional identifiers as suffixes, such as court branches or designations for multiple defendants, based on local needs.

For example, using this common numbering scheme, the 345th criminal case, with two defendants, filed in Marin County Superior Court in 2010 might generate the following unique case numbers: 21-10-CR0000345A for the first defendant and 21-10-CR0000345B for the second defendant.

4.3 Filing Systems for Court Records Maintained in Paper Format

Effective filing systems for paper records determine how records will be organized, categorized, accessed, and stored. The most efficient filing systems ensure that records can be retrieved at the right time, at the right place, at the lowest possible cost. This includes determining what kind of shelving will be used, who will have access to the record storage areas, how records will be accounted for when not shelved, and how records will be located when they cannot be readily retrieved.

Records managers must first decide how to organize paper records on file shelves or in cabinets. There are several filing systems that may be considered, but all systems have advantages and disadvantages. Ideally, the type of filing system(s) selected will be compatible with the records organized in the system. Below are descriptions of three commonly used filing systems.

4.3.1 Numerical Filing Systems by Case Numbers

Court records may be arranged in numerical sequence, although filing systems that are strictly numerical are uncommon in organizing case records, because of the volume, complexity, and variety of case types. (These systems are more useful for administrative records [procurements, accounts payable, etc.], as these kinds of records are less complex and less variable.)

A numerical arrangement orders records from the lowest number to the highest. This method is also often an indicator of which files are the oldest (the lower-numbered files) and which are the most current (the higher-numbered files). While these filing systems are simple and easy to learn, and make detecting misfiles more readily apparent, a disadvantage of this system is that new records are being shelved only at one end of the system. As old records are purged, staff must shift and reshelve remaining records to make room for new ones. A benefit of these systems is that a numerical scheme is easier to comprehend than an alphanumeric filing scheme and may result in fewer misfiles.

4.3.2 Alphanumeric Filing Systems by Case Numbers

An alphanumeric arrangement combines alpha characters and digits to designate case records and determine how they will be shelved. Alphanumeric filing systems are commonly used for court case records. There are two ways in which these systems are organized. Typically, alpha characters are used to signify case types and often precede sequential case numbers. In some filing systems, all cases with the same case type are grouped together and then filed sequentially by case number. For example, all civil cases with alpha designations of “CV” are in one grouping, while family law cases with designations of “FL” are in a separate section of the filing system. An alternative approach is that all alpha designations are commingled and share the sequential filing number sequence. In these systems, the filing year is an important feature of the case number, to avoid replicating case numbers over time. For example, all civil, probate, and family law cases, with prefixes of “CV,” “PR,” and “FL,” respectively, share a numbering sequence and are

filed together in the same system. Alphanumeric filing systems are often configured to reflect the way the trial court organizes functions in the clerk's offices or courthouse. Because alphanumeric systems are more complex than simple numeric systems, the opportunity for misfiles is increased.

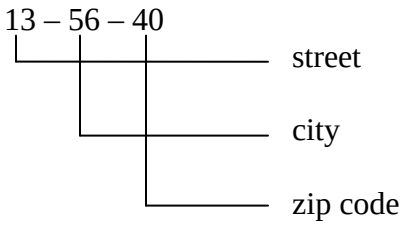
4.3.3 Terminal Digit Filing Systems by Case Numbers

Terminal digit filing systems are also used in many organizations, including trial courts. In a terminal digit system, the focus for shelving records is only on the numerical portion of a case number. Cases are not filed sequentially; instead, every file is shelved based on an "addressing" scheme that is associated with the case number.

In terminal digit systems, the numbers are read from right to left and divided into three sections. In the terminal digit file there are one hundred (100) primary sections ranging from 00 to 99. In this arrangement, the last two digits are the primary unit used for filing; records are ordered by the last two digits, then the middle two digits, and finally by the first two digits.

Another way to conceptualize this system is to treat case numbers as analogous to the postal designations of street, city, and zip code. For example, case number 135640 would be divided into three parts: "13" representing the "street," "56" representing the "city," and "40" representing the "zip code." The entire filing system is divided into 100 areas, or zip codes, starting with section "00" and ending with section "99." Then each zip code is divided into 100 subsections, or cities, from "00" to "99." Finally, each city subsection is divided again into subsections, or streets, from "00" to "99."

For case number 135640, the last two digits of the case number, "40," is analogous to the zip code designation and provides the general area of the filing system in which the case will be shelved. The middle two digits, "56," narrows down the "city" location in section "40" where the record will be shelved. Finally, the first two digits, "13," represent the "street" in the "city" that is the record's final destination.



While this system requires more training initially, once staff is trained, terminal digit virtually eliminates the need to shift and reshelve records, as new records are interspersed among existing records and purged records are removed from throughout the system.

4.4 Electronic Format Filing Protocols

4.4.1 E-Filing Overview

In a period of increasingly tight budgets and ever-expanding caseloads, courts across the country have looked at electronic filing as a way to reduce the considerable demands of handling physical case files and the long-term costs of storing official documents. In theory, electronic filing of pleadings and other court papers will finally make it possible to move toward the ideal of a "less paper" courthouse, thus realizing a wide range of potential spin-off benefits for litigants, judges, lawyers, court administrators, and the general public.

The idea that a court can operate electronically is not new. Quite a few courts have successfully implemented electronic records processes that use imaging technology to "scan" paper documents and convert them to electronic files that are stored in sophisticated document management systems. For example, the bankruptcy court is almost completely paperless after years of transition for the court, attorneys, and other users.

E-filing is the next generation of electronic records processing. Instead of delivering or mailing a paper document to the court, litigants and lawyers send an electronic version of the information or document to the court, via the Internet.

Advantages of e-filing:

- Improved legal processes, as judges and lawyers learn to take advantage of the universal availability and ease of sharing electronic documents.
- Enhanced public safety arising from electronic service of and instantaneous access to court orders (including domestic violence orders of protection) and warrants.
- Shifting of data entry from the clerk to the filer, thus reducing court staff data entry time and potential for data entry errors.
- Savings for the court of costs incurred to convert most documents from paper to electronic form.
- Expedited processing time by eliminating the time required for mailing or personal delivery of pleadings and other documents.
- Increased efficiency and reduced cost from the ultimate reduction or elimination of handling and storing paper case files in courts, lawyers' offices, and official archives.
- "Greener" filing business processes enabled by e-filing.

4.5 Court Record Location Tracking

4.5.1 Paper Record Tracking

There are few court activities that are more frustrating and wasteful of staff resources than searching for lost court records. By implementing effective tracking protocols

and, depending on the court's needs, by investing in tracking technologies (bar codes, RFID, etc.), significant staff time can be saved and deployed in more productive activities.

Automated tracking systems that use bar code or radio frequency technology to track the movement of court records are helpful in managing the check-in and check-out process. Automated tracking systems also can produce reports to assist records staff in locating missing records. Periodic physical inventory of all court records not on file shelving or in file rooms or warehouses can often uncover missing records and restore them to oversight by records custodians.

As described below, there are several common methods for monitoring the whereabouts of court records.

Out Cards

Records custodians are encouraged to use an "out-card" system to track all records removed from file shelves or storage facilities. When a record is retrieved, an out-card can be inserted in the location from which the record was removed. Out-cards may include the name and contact information of the staff person who removed the record, the date the record was removed, and the destination of the record (courtroom, public viewing area, other court facility, etc.). Out-card systems are "low tech," are inexpensive to implement, and can be effective, especially in small courts with only one facility.

Bar Code Technology

Automated tracking systems that use bar codes are another option in managing the check-in and check-out process for court records and monitoring the movement of records. In a bar code system, every file folder is labeled with a bar code (every folder in a multivolume case record receives its own bar code). Key locations in the courthouse (judicial departments, public viewing areas, the accounting unit, off-site facilities, etc.) are also assigned a bar code and placed on a list at each bar code scanning location. Each bar code is associated in a tracking database with its corresponding folder or location. Then, as file folders are checked out of the filing system, the bar codes are scanned by records staff, as well as the destination of the file folder. For example, if a bar coded "civil file" was being routed to a specific judicial department, the folder and the department would be scanned so that the file would be tracked to the judicial department.

Bar code systems are relatively inexpensive, as they are not complex. A tracking application with a relational database and scanning stations and/or portable scanning wands are all that is needed to implement such a system. Bar code technology has been in use for many years and is very reliable. However, a major challenge for a court implementing the tracking system is in determining the number of locations that will be tracking destinations. The tendency to have every desk be a destination may sound like a good idea, but in practice may be too onerous for staff members who are processing hundreds of files a day. Developing a list of key locations that helps narrow the search in the event there is a lost file is typically the most advantageous. Another key decision is which staff person will be responsible for tracking the file to the next location—the staff person who is passing on a file or the staff person who is

receiving it. Since the identity of the person scanning the file will be retained by the tracking system, it is critical to gain cooperation from all staff to use the technology with every file.

Automated tracking systems also can produce reports to show what was requested, when, and by whom. Many scanning systems have battery-powered portable scanners that records management staff can carry around the courthouse to periodically update the location of every file that is not in the filing area.

RFID Technology

Radio-frequency identification (**RFID**) is the use of a wireless non-contact system that uses radio-frequency electromagnetic fields to transfer data from a tag attached to an object, for the purposes of automatic identification and tracking. RFID systems are a "high tech" and more expensive method for locating and tracking files. Like bar code technology, RFID tags are created and attached to file folders. RFID tags are "active" bar codes that can exchange information with a networked system to track every file. RFID tracking solutions save time by providing continuous, automatic tracking of files and other items as they move around the courthouse and pass through an area where an RFID reader is present. Like a traditional bar code, an RFID tag must be read. However, an RFID tag does not need to be physically scanned. It can be detected and read as it passes by a reader that can be mounted on a wall and up to 25 feet away. Staff members are relieved of the responsibility to scan files, as they are automatically monitored at all times by the technology, and their locations are typically updated in real time. Records staff can locate files at any time by checking the tracking database online.

This technology has been cost prohibitive in the past, but in recent years the cost has been coming down. In situations where it is affordable, this technology could be beneficial for small to medium court systems.

4.5.2 Electronic File Tracking and Security

In the CCMS V3 system, the "Track Case Files" function describes the activities involved in changing the location of physical case files. This process incorporates maintaining a "chain of custody" during the location change of physical case file(s) and defining who has ownership of a physical case file at a particular place, time, and location. Case files may be tracked to separate locations (e.g., facility, department) within the court's jurisdiction. Case files may also be located out of a court's jurisdiction, in the event there is a change of venue.

The "Track Case Files" function also defines the activities involved in creating and tracking the case file, including the initial and subsequent volumes, as well as defining an indirect association between volumes and documents within the volumes. The CCMS V3 user may choose to update the location of case files within the context of a case (selecting associated volumes) or outside the context of a case (in the scenario where a request may span multiple cases based on a court calendar or any other criteria).

5. Record Classification

California statutes define the characteristics of court case records, typically at the case type level. These requirements are contained in numerous code sections in law. To assist records managers in determining the correct classification of court case records, these characteristics and special records management directives are included in TCRM section 11.4, "Schedule of Records Retention and Destruction and Special Case Type Characteristics."

It is important to recognize distinctions between case *categories* and case *types*. For records management purposes, sometimes case records are organized by case *category*, which groups case records together by common attributes such as operational or statistical reporting needs (i.e., case category = criminal). Case records can also be organized by case *type*, which groups case records together by common attributes such as retention periods or other statutory requirements (i.e., case type = felony).

The characteristics for each case *type* are described in section 11.4, "Schedule of Records Retention and Destruction and Special Case Type Characteristics." They include whether

- the case type is classified as available to the public or confidential;
- there are special destruction or deletion/redaction requirements of portions of the case record; and
- there are requirements to maintain cases as confidential for a limited period of time, rather than the life of the case record.

5.1 Standard Record Classifications

5.1.1 Case Record Classification

The California judicial branch maintains an electronic statistical reporting system called the Judicial Branch Statistical Information System (JBSIS). JBSIS defines and collects summary information for each major case-processing area of the court and makes court data available via the JBSIS data warehouse. JBSIS was created to inform the Judicial Council on its policy and budgetary decisions, provide management reports for court administrators, and allow the Judicial Council to fulfill its legislative mandate to report on the business of the courts. The JBSIS system comprises 10 report types, which are broad case *categories* (e.g., Family Law report 6a) made up of a collection of individual case types (e.g., Paternity).

The standard case record classifications contained in the JBSIS system include the following:

Appeals
A classification category for cases appealed to the appellate or California Supreme Court as well as to the appellate division of the superior court.

Civil Cases
A broad classification category for trial court caseload involving lawsuits brought to redress private wrongs, such as breach of contract or negligence, or to enforce civil remedies, such as compensation, damages, and injunctions. The civil limited category captures cases for which the petitioner/plaintiff is seeking relief of less than $25,000. The civil unlimited category captures cases for which the petitioner/plaintiff is seeking relief of $25,000 or greater, including complex litigation and small claims appeals.

Family Law Cases
A major classification category of cases involving family actions, such as marital actions (e.g., dissolution), custody matters, family support, parental rights, and adoption.

Felony Cases
A criminal case type that involves an offense punishable by death or incarceration in a state prison.

Juvenile Delinquency Cases
A broad classification of cases filed against a minor for a violation of the law.

Juvenile Dependency Cases
A broad classification of cases filed on behalf of a minor by a social services agency, the parents, the minor, or others interested in the welfare of the minor. The purpose of this type of proceeding is to provide safety and protection for children who are abused, neglected, exploited, or at risk of harm.

Mental Health Cases
A broad classification of cases in which a trial court is asked to legally determine probable cause or lack of capacity of an individual because of

- mental illness
- developmental disability
- mental retardation
- addiction to narcotics
- or, in the case of an individual who has committed a crime, his or her competency to stand trial and whether the individual should be placed or should remain under care, custody, and treatment.

Misdemeanor and Infraction Cases
Misdemeanors are a type of crimes that are punishable, at the court's discretion, by imprisonment in county jail, by fine, or by both (Penal Code section 17). Infractions are a category of crimes other than felonies and misdemeanors, punishable by a fine or other penalty but not by incarceration.

Probate Cases
A broad classification category for trial court caseload that includes cases in which a court is asked to make a legal determination as to the disposition or transfer of decedents' assets, the

appointment of conservators and guardians, the internal affairs or existence of a trust, and other miscellaneous probate matters. Probate cases consist of decedents' estates, trusts, adult conservatorships, guardianships of minors, and miscellaneous probate proceedings.

Small Claims
A broad classification category for small claims cases that encompass a wide variety of civil case types in which the remedy sought is $5,000 or less, or, in actions brought by a natural person, $10,000 or less. (See Code Civ. Proc., §§ 116.220–116.221.) However, until January 1, 2015, the small claims court has jurisdiction in actions brought by a natural person for bodily injuries resulting from an automobile accident only in cases in which the amount of the demand is $7,500 or less. (See Code Civ. Proc., § 116.224.)

5.1.2 Prefiled Records

This category includes search warrants, wiretaps, probable cause declarations, grand jury indictments, and investigative reports pertaining to the release of a defendant on his or her own recognizance pursuant to Penal Code section 1318.1. Retention, destruction, and special characteristics of these records are described in section 11.4.3, "Schedule of Records Retention and Destruction for Prefiled and Juror Records."

5.1.3 Lodged Records

A lodged record is a record that is temporarily placed or deposited with the court, but not filed. (Cal. Rules of Court, rule 2.550(b)(3).) Some records may be lodged with the court for long periods of time, such as wills and codicils. Other records may be lodged with the court only while awaiting a judicial ruling and, following the ruling, may or may not be returned to the depositor.

5.1.4 Exhibits

A document or object formally presented to the court as evidence. Exhibits management is described in section 7, "Exhibits Management."

5.1.5 Juror Records

For juror records, see section 11.4.3, "Schedule of Records Retention and Destruction for Prefiled and Juror Records."

5.2 Confidential and Sealed Records

Statutes define specific case types that are to be maintained as confidential records. Some types of records are confidential from the date the records are created and are never made available to the public. Other types of records may remain confidential for a period of time, and then become public.

Under rule 2.550 of the California Rules of Court, a sealed record is a record that by court order is not open to inspection by the public. Under rule 2.551(f) sealed records must be securely filed and kept separate from the public record. Only a judicial officer has the authority to seal and unseal a record.

For a more detailed discussion of confidential and sealed records, see section 10.3, "Confidential and Sealed Records."

5.3 Subpoenaed Records and Documents

Courts occasionally receive subpoenas for testimony or production of court records that are not made part of the court record. These documents are typically not file stamped and may or may not be lodged in the court record.

Under Evidence Code section 1560(d), subpoenaed records delivered to the clerk of the court include

- lodging and handling (sealed envelope) subpoenaed records and items (Evid. Code, § 1560(d))
- return or destruction of subpoenaed records and items (Evid. Code, § 1560(d))

Under Evidence Code sections 1560(c) and 1561, *subpoena duces tecum* served on the clerk of court to provide court records for

- preparation and delivery of records (Evid. Code, §§ 1560(c) and 1561)
- charges for preparation of documents

6. Storage, Maintenance, and ~~Security~~ Electronic Signing of Records

6.1 Industry Standards for Storage of Paper and Electronic Records

6.1.1 Recommended Standards for Paper Records Storage Facilities

While there are no statutes or rules of court that provide guidance to trial courts in the area of storage facilities, the standards below offer best practices in records storage to improve the likelihood that paper records will not deteriorate over time. Courts are encouraged to review and comply with the standards below whenever possible. Standards for the storage of paper records are available from the American National Standards Institute (ANSI), Inc. These standards exclude records stored in central file areas and file rooms containing active records used and maintained in their office of origin, and records staging areas used for temporary storage of records before their transfer to an off-site records center.

ANSI recommends the following paper records storage and facilities standards:

1. Any records storage facility for public records should be constructed of noncombustible and fire-resistant materials. The facility should be of a nature that minimizes the potential for and the resultant effects of fire.
2. The facility should be a stand-alone structure. If the structure is shared with other tenants, fire walls of approved construction should separate the records storage facility from other areas in the building.
3. If the records storage facility is located in a structure with other nonrelated tenants, activities conducted in other parts of the building should not be of the nature that would create a hazard to the records stored there.
4. Access to the facility should be restricted to authorized personnel. Adequate security procedures and systems should be provided to prevent loss, theft, or destruction of public records and to ensure the safety and integrity of the public records stored there.
5. A records storage facility should maintain a fire prevention program based on good housekeeping practices. Smoking, use of open flame devices, or the presence of flammable materials should be prohibited in storage areas.
6. The facility should have appropriate fire detection and suppression systems with procedures in place to ensure their effectiveness.
7. A slightly positive air pressure balance should be maintained within the records storage area so as to ensure (1) consistency of temperature and relative humidity and (2) minimize infiltration of contaminants.
8. Air handling ducts should be equipped with fire detectors and applicable shutoff apparatus.
9. The facility should have a power supply sufficient to maintain environmental controls, security, lighting, and fire detection and suppression equipment.

10. No cellulose nitrate films should be stored in the facility.
11. All door openings of the records storage facility should be fitted with suitable and approved fire-resistant doors.
12. All electrical wiring within the facility, exclusive of low-power alarm circuits, should be encased in an approved conduit.
13. Portable fire extinguishers of a type appropriate for Class A fires should be readily accessible inside and immediately outside the record storage area.
14. All records storage containers within a facility should be kept at least six inches from piping or conduits.
15. Work, reference, and storage areas should be constructed so as to avoid prolonged exposure of archival records to direct or indirect sunlight, which contains ultraviolet rays that can damage archival material. Ultraviolet light filters should be placed on all fluorescent lights in areas where archival records are stored, displayed, processed, or researched.
16. Storage containers, folders, and other enclosures for archival material should be constructed of acid-free buffered, lignin-free paper or other material free of harmful off-gassing material.

6.1.2 Recommended Standards for Managing Microfilm

The purpose of reproducing court records is to generate a reliable and usable reproduction that is deemed and considered an original. It is necessary to determine if a reproduction is successful while the source documents are still available for re-imaging. Some level of inspection is necessary to determine if the various requirements have been met.

A. Processing Microfilm

The proper processing of film is crucial to permanent quality. The following tests should be performed by a microfilm processing lab or qualified court personnel to ensure quality film is produced:

1. Perform a Methylene Blue Test on the film to determine and measure residual thiosulfate and other chemicals in the film. Test should be conducted within two weeks after processing.
2. Perform a density test. Density is a numerical measure describing the lightness or darkness of a microfilm image. The density of microfilm is measured in two ways, d.min and d.max. D.max is measured on the background of the exposed area. D.min is measured on the unexposed area of the film.
3. Perform a resolution test. Resolution, or resolving power, is the measure of a microfilm system's ability to resolve and record fine detail. The resolution directly affects the legibility of documents being filmed.
4. Perform a print test to verify printed copies are legible.

Please note that if any of the above mentioned criteria is not met, the microfilm reel should be rejected and the source documents should be refilmed. Logs should also be kept to record the above mentioned criteria for each reel tested. Refer to ANSI/AIIM MS-23 for acceptable ranges on the above mentioned criteria.

B. Industry Standards for Microfilm Records Storage Facilities

Providing a suitable storage environment for microfilm is essential. If properly stored, microfilm can last from 100 (acetate based) to 500 (silver film) years.

Industry standards for storing include:

1. Microfilm should be stored in a secured, sealed, airtight room with a constant cool environment with temperatures not exceeding 70 degrees.
2. Relative humidity should be maintained between 20 and 30 percent and should not fluctuate ± 5 percent in a 24-hour period.
3. The storage room should include a properly designed and functioning HVAC system that controls the temperature and humidity and minimizes the infiltration of pollutants.
4. Microfilm enclosures (i.e., boxes, plastic film boxes, etc.) should be made of non-corroding materials that meet certain chemical and photographic criteria.
5. Establish an ongoing inspection procedure to determine if the microfilm is degrading in any way.

6.1.3 Electronic Records

Electronic records are text or data files that are created and stored in digitized form through the use of computers and software applications. They are stored on various magnetic and optical storage media such as magnetic disk, compact disc (CD), and digital versatile disc (DVD). The format of an electronic document does not change the fact that it is a court record, but its electronic form and its dependence on computers for creation and reference do change the way these records must be stored and managed.

Although court records have historically been maintained in paper form, the statutes on court records have been modernized to reflect the digital age. In 2010, Government Code sections 68150 and 68151 were updated to enable courts to use technology as a way to modernize the methods of creating, maintaining, and preserving court records.

To assist courts in managing electronic records, best practices, guidelines, and industry standards follow. The information includes:

- File formats
- Digital imaging and scanning
- Quality assurance
- Technology scanning refresh
- Data backup and storage

- Records retention and destruction

6.1.3.1 Process Overview

Physical court records are typically converted to electronic format by processing a document through a document scanner, reviewing the image at a scanning workstation, and storing it in a document repository. The scanner is used to convert the physical document into an electronic format. During the scanning process, basic index information such as case number, date filed, and document title may be captured or entered. The scanning workstation is then used to review the resulting electronic document and perform quality assurance.

Court records can also be received directly in electronic format. Typically, electronic documents are transmitted to the court through an electronic filing (e-filing) process. E-filing systems ensure that submitted documents are associated with their corresponding case information and track information such as submission time and name of the submitter.

Once a court has the record in electronic format, additional index information such as document type or other case-related information may be added at this time. The electronic documents are then stored in a document repository, which consists of document management software that controls access to the documents and the storage hardware, which usually consists of optical discs, individual magnetic disks, or a series of magnetic disks contained in a storage area network. The electronic documents are usually then also stored on backup tape or duplicated onto another set of magnetic disks or separate storage area network.

6.1.3.2 File Format Best Practices

A. File Formats

A file format is a particular way that information is encoded for storage in a computer file. When trying to determine the most appropriate file format to use for long-term access and preservation, a trial court may want to consider the following aspects:

- The format is based on open standards or is nonproprietary;
- The format is widely used and accepted;
- The format must be stable, well-supported, and well-documented.

In choosing file formats, the trial courts should consider current and future compatibility within the trial courts and between the trial courts and their justice partners, as well as accessibility to the public.

Common File Format Types

Document files. Document files are most often created with word-processing programs. Common file formats for document files include:

- **TXT** – plain text files. File size is small and document is searchable but limited to plain text only. There is minimal ability to format document text, and images are not supported.
- **DOC** – developed by Microsoft, widely used in Windows environment. The file size is often large, especially with graphics, and can possibly be used to transmit viruses. DOC files can be edited with Microsoft Word for Windows or MacOS and OpenOffice for Windows, Linux, MacOS, and Solaris. Microsoft Word 2007 and later save files as DOCX.
- **PDF** (Portable Document Format) – developed by Adobe Systems. This format is widely used since it can combine many multimedia elements such as sound, graphics, images, and text in a format that can be read on many platforms, including mobile devices. It is also small in size and the reader application is free and available on most operating systems. PDF files can only be created and edited with PDF-creation software.
- **PDF/A** (Portable Document Format) – an ISO standard version of PDF, PDF/A is a standard file format for long-term archiving of electronic documents. Files are 100 percent self-contained, all information required to display the document is encapsulated in the file. (International Standards Organization (ISO) standard: ISO 19005-1:2005).

Graphics files. Graphics files store an image (e.g., photograph, drawing). Common file formats for graphic files include:

- **JPEG** (Joint Photographic Experts Group) – commonly used for graphics on web pages and photos taken with a digital camera. JPEG has a small size and can be viewed with most web browsers.
- **TIFF** (Tag Image File Format) – often used for storing high quality images. Viewing TIFF images typically requires a picture or fax viewer (which is often included with the computer operating system).

B. Usage

When choosing a specific file format for electronic documents, courts should consider the following characteristics to ensure they meet operational and legal requirements:

1. File size – file size will vary depending upon the format selected. File size is also related to the portability and searchability of a document. A file encoded to be portable and easily viewed on any device will be larger than one encoded in a more proprietary format. Encoding a file to enable text search within the document could increase the document size by 5 to 10 percent.
2. Accessibility – courts should accommodate public and judicial partner access to documents by selecting a file format that provides the broadest level of accessibility. A court should not require the use of a particular software or tool but rather provide documents in a format that can be viewed by a large number of software platforms and devices.

3. Longevity – court documents have specific retention periods. When selecting a file format, a court needs to determine how long the document will be retained. In general, the longer a file needs to be kept, the more portable it should be.
4. Searchability – some file formats preserve documents as an image and therefore result in a file with contents that cannot be searched.
5. Document formatting – formatting and content of the original document must be preserved. Non-text images like signatures, charts, or diagrams must be supported by the selected file format.

The chart below summarizes these characteristics:

Format	File Size	Accessibility	Longevity	Searchable	Document Formatting
TXT	Small	Excellent	Excellent	Yes	Poor
DOC	Medium	Fair	Fair	Yes	Excellent
PDF	Small	Good	Very Good	Yes	Excellent
PDF/A	Medium	Good	Excellent	Yes	Excellent
JPEG	Very Large	Very Good	Very Good	No	Good
TIFF	Large	Very Good	Very Good	No	Excellent

C. Selecting a Solution

Recommended:

1. PDF/A is the recommended file format for long-term/permanent preservation of electronic records. With excellent longevity, searchability, and good accessibility, PDF/A is an excellent choice for courts. Although PDF/A files are slightly larger than PDF files and therefore require more storage space, this issue will become less important over time as the unit cost of storage continues to drop. PDF/A files are approximately 5 percent to 20 percent larger than a PDF file but approximately the same size as a Microsoft Word document.
2. PDF is the recommended file format for short-term preservation of electronic records. Although PDF may not be as accessible as PDF/A in the long term, PDF files are smaller in size and retain all the other benefits of PDF/A.

Alternatives:

1. Courts may wish to consider TIFF as an alternative format for long term preservation of electronic documents since it is highly accessible and has very good longevity. However, the inability to perform searches within a TIFF file and its larger file size may make this format unsuitable for some environments.

Not Recommended:

1. DOC and DOCX are proprietary formats and are not recommended. They are developed and managed by a specific vendor for use with specific software programs and not intended for long-term document preservation.
2. TXT files are unable to capture images and rich document formatting and are not a recommended file format for electronic records.
3. JPEG documents are very large, unsearchable, and are subject to loss of quality when the original document is converted to electronic format.

6.1.3.3 Color Palettes

A color palette describes the type and number of colors used when converting a scanned document or image to electronic format.

A. Palette Types

There are three primary color palettes that can be used when scanning documents:

1. Black and White – everything contained in the original document is converted to one of these two colors.
2. Grayscale – document and image contents are converted to black, white, or shades of gray. Typically up to 65,536 levels of gray are available.
3. Color – all colors of the original document or image are retained in the electronic version.

B. Usage

When choosing a specific color palette for electronic documents, courts should consider the following characteristics to ensure they meet operational and legal requirements:

1. File size – file size will vary depending upon the palette selected. Documents scanned as grayscale and color are about 10 times larger than those scanned as black and white.
2. Clarity – while all color palettes will represent black and white text-only documents well, documents that contain handwriting, images, or carbon copies will vary in clarity depending upon the palette used.
3. Accuracy – when an exact copy of an image is required, the palette that best represents the original should be used.

The chart below summarizes these characteristics:

Palette	File Size	Clarity	Accuracy	Best for
Black and White	Small	Fair	Fair	• Black and white text documents • Black and white text documents with simple tables
Grayscale	Large	Good	Good	• Documents that contain a wet signature or fingerprint • Carbon copy documents • Documents printed on colored paper
Color	Large	Good	Excellent	• Images and content that contain color

C. Selecting a Solution

Recommended:
A black and white color palette should be used when scanning most court documents. Most court documents only contain black and white text and the black and white color palette will minimize file size and storage space.

Alternative:
When it is important to capture a wet signature, fingerprint, or other non-text content and a court can afford the extra storage space, grayscale can be used to accurately capture that content. Documents scanned as grayscale are about 10 times larger than those scanned as black and white.

Not Recommended:
Color images are large and usually unnecessary when imaging the majority of court documents. Documents scanned as color are about 10 times larger than those scanned as black and white. Although the resulting size of a document scanned as color is about the same as grayscale, printing an electronic color document requires a color printer for best results.

6.1.3.4 Digital Imaging and Scanning Best Practices

Document imaging converts paper documents into digital files that are stored electronically. Accessibility, full text search, and, physical space savings are several reasons why we decide to transform these paper documents and make them available electronically.

A. Best Practices

The following best practices will ensure that documents that are scanned and digitally imaged will meet practical requirements for image quality, retention, and security:

- Before disposing of the original physical records after they are scanned, courts should ensure that there are at least two copies of the record stored in electronic format on a trusted system (e.g., production and storage backup or local and disaster recovery copies).
- To ensure image quality, courts should use a minimum scanning resolution of 300 dots per inch (dpi) for all *future* projects involving a court that is going to electronically image documents for archival purposes. Adopting this recommendation ensures that documents will comply with the California Rules of Court, Association for Information and Image Management (AIIM) guidelines, and National Archives standards.
- Care and consideration should be given with regard to "hidden" data and metadata when exporting electronic files for use outside of the court. This data may contain identifiers or information that would not be appropriate for disclosure (e.g., working notes from the judicial officer hearing the case, personal identifiers such as birth date, etc.).
- If electronic documents are stored with Optical Character Recognition (OCR) metadata contained in the file (e.g., to facilitate text searches), the metadata should be contained "behind" the image of the document. The original image of the document should be preserved and not be replaced with information resulting from OCR.
- There may be variations in the level of quality of existing digital images that were created using older technologies (e.g., microfilmed documents at 200 dpi). Courts may wish to certify these documents by stamping them "Correct Copy of the Original" or "Best Available Image" when requested to produce a copy from electronic storage.

B. Quality Assurance

Quality Control Standards for Electronic Document Images

In order to realize all the anticipated benefits of imaging, it is imperative to ensure the quality of the imaged case files. Quality assurance is a two-tiered process:

1. Initial data validations should be performed at multiple points during the document capture process (i.e., at indexing time).
2. Secondary inspections should be performed after document capture.

There are three quality attributes that must be substantiated:

- Image quality
- Index accuracy
- Document completeness

Document Capture Review

Image Quality
Image quality defines how readable the document is. It must be legible to the human eye. Defects include speckling, skewing, streaking, poor contrast, folded pages, tears, etc. These defects can be present as long as the document is still legible. A fold or crease that blocks no text is acceptable, while any text that is illegible would be unacceptable. There is software available to correct image quality problems during document capture.

For best results, every page should be reviewed. Barring that level of review, at least the first, middle, and last pages should be reviewed. This lesser level of review works on the principle that many image quality problems are related to the scanning process and cause the same defect on every page. Note that this may not catch page-level defects caused by folded corners, colored paper, or unclear original copies of triplicate images (i.e., NCR paper). To avoid unnecessary re-scanning, extremely poor quality originals that cannot be corrected or enhanced could be stamped "Best Available Image."

Index Accuracy
While some index fields are critical for locating documents, other fields provide additional information but are not necessarily critical. There are multiple methods for ensuring the accuracy of critical index values.

1. Character-Level Validations – Individual characters can be validated through the use of character filters, which prevent the entry of invalid characters. For example, a phone number field would not allow entry of alphabetic characters. This type of validation should be real time without slowing the user down. Invalid keystrokes should be blocked as they are typed rather than waiting to validate the data when saving the document or after moving to the next field to be entered.
2. Field-Level Validation – Field-level edits can help catch errors as soon as the field is completed. Examples include minimum and maximum values, minimum and maximum number of characters, date range checks, etc. Values may be selected from drop-down lists when applicable or compared against lists of valid values prior to saving the data. Check digits or other types of calculation validations are useful when applicable.
3. Record-Level Validation – Some data cannot be validated until all fields have been entered and the user is ready to save the data. For example, if names are optional but a first name is entered, the last name must also be entered. Any messages displayed should be as clear as possible to make it easy for the indexer to make corrections. Results of record-level validation must be displayed as quickly as possible to avoid negatively impacting throughput.
4. Double Key Entry – For critical index data, the most effective way to ensure accuracy of key-entered data is to key it twice and programmatically compare the results. If the values don't match, they must be re-entered. Blind double key entry requires the key entry to be performed by two different people. This increases the likelihood of

accuracy based on the fact that it is less likely that two different people will make the same typographical errors.

5. External Validation – If authoritative data is stored in an external system such as a case management system, that system can be queried to validate or populate index data. Integration effort and speed of access to data residing in the external system must be considered to ensure that overall processing time is acceptable.

Some courts may generate index information by creating barcode cover sheets from the case management system. In this situation, any of the five previous approaches can be used as appropriate. However, validation that the document is associated with the correct case will vary depending upon the specific imaging, quality assurance, and case management technologies used.

Document Completeness

The most effective way to ensure document completeness is to count pages prior to scanning and have the software compare the human count to the machine count. There are two ways to count the pages:

- Pre-blank page removal; and
- Post-blank page removal.

The pre-blank page removal count is the count of physical pages in the batch, including document separator sheets. It is independent of whether the pages are duplex or simplex. The post-blank page removal count is the count of actual images after programmatically removing blank pages and separator sheets. This count is much more cumbersome to obtain since the user must examine the front and back of every page and track.

Whichever counting method, there are three possible outcomes to the comparison:

1. The counts match;
2. The machine count is higher; or
3. The machine count is lower.

If the counts match, the batch can be accepted with a high degree of certainty that the documents are complete.

If the machine count is higher, it is likely that the human undercounted since it is unlikely that a page was captured twice. To increase certainty, the batch could be re-scanned to see if the machine count remains the same.

If the machine count is lower, it is possible that the scanner double-fed two or more pages or the human count was too high. In this case the batch should be re-counted and re-scanned.

Note that the pre-blank page removal counts could match while the software could remove a page that is not technically blank, causing the document to be incomplete. In order to

maximize the level of certainty that all documents are complete, both counts should be performed and compared.

Post–Document Capture Review

Even if all the above steps are taken to ensure document quality, random documents should be examined after the document capture process. The same reviews should be performed (image quality, index accuracy, and document completeness). Defects should be corrected to the extent possible. If the original source documents have been destroyed, then poor images cannot be rescanned. They can, however, be modified electronically to remove blank pages, or combined or split to accommodate for missing document separator sheets. Incorrect index data should be corrected.

The sampling plan is based on the desired Acceptance Quality Level (AQL). There are a number of publications available detailing this, including American National Standards Institute/American Society for Quality Control (ANSI/ASQC) Standard Z1.4

6.1.3.5 Technology Refresh

Procedures for technology monitoring and refresh should ensure that existing electronic records are retrievable and viewable in the future.

This section is divided into three parts. The first part focuses on the suggested refresh cycle and update procedures for scanning and storage hardware. The second part focuses on update procedures for scanning software. The third part identifies industry standards organizations that should be monitored.

A. Hardware

Most document imaging solutions have three main hardware components: the scanner, the scanning workstation, and the document repository. Each of these plays a vital role in the overall process and performance of the scanning solution. Most courts have a hardware refresh cycle that they follow. These may be sufficient. The industry standard for replacement of scanning and imaging hardware is between five and seven years (AIIM.org, 2011). If a court's hardware replacement cycle policy meets these guidelines, then the document imaging solution can simply be included in the court's existing processes. If the court's policy does not meet these guidelines, then the court may need to establish a different process for specifically refreshing the hardware components of the document imaging solution.

Since the document imaging solution typically resides on one or more PCs or servers, the court should follow the manufacturer's guidelines for driver updates and patches. It is not recommended that new drivers or patches be applied as soon as they are released, unless there is a specific problem or issue that the driver or patch is expected to solve. All patches and drivers should be tested in a test environment before being applied to the production environment if possible.

B. Software

The document imaging solution may be all inclusive or it may rely on other software, such as Microsoft SQL or Oracle. Regardless of the requirements of each court's individual document imaging solution, there are some best practices and general guidelines that should be followed.

The underlying operating system should always be patched and protected from viruses/malware. This can be accomplished by applying system updates and patches once they are tested and determined to be stable. Each court may have a policy or procedure on how and when system patches are applied, and these may meet or exceed industry guidelines. Courts should follow a process that best protects the operating system and meets the court's specific business requirements.

The specific document imaging software (e.g., scanning software, document management software) will also have periodic patches and updates. It is recommended that these be installed based on the software manufacturer's recommendations only after being applied to a test or staging environment first to ensure that existing functionality performs as expected and the impact of the patch and update is fully understood.

C. Industry Standards Organizations

There are two primary organizations that help shape the document management industry: the Association for Information and Image Management (AIIM) and Association of Records Managers and Administrators (ARMA). Both of these associations offer insight and guidance for document management.

The recommendations and publications from these two organizations should be monitored and courts should consider new technologies or guidelines at least once a year.

6.1.3.6 Data Backup and Storage

The electronic copy of a court record may be the only copy that exists. Therefore, preservation of that electronic information is critical. Storage of the primary copy of an electronic record should be reliable. Duplicate copies should be stored in different locations in case of a disaster. In addition to backup and storage, courts should ensure that all electronically stored data can be retrieved today and in the future.

A. Storage Media

Electronic documents are usually stored on magnetic disk, optical disc, or magnetic tape. Each type of media varies in the speed of access, capacity, and durability. Courts should not rely on a single type of storage media but instead use a combination of media focused on a specific purpose. The following chart provides some general characteristics and suggested usage:

Media Type	Speed	Capacity	Durability	Usage
Magnetic Disk	Very Fast	Medium	Low	Primary storage and access to frequently used data
Optical Disc	Fast	Low	High	Secondary storage and access to occasionally used data
Magnetic Tape	Slow	High	Medium	Long-term backup. Only used for data recovery purposes.

B. Backup and Redundancy

Data backup provides a long-term storage solution for data recovery in the case of a major disaster or catastrophe. Backup copies of all electronic court records can be made on various storage media based on an individual court's business requirements and resources. Copies should be distributed and stored in different locations to protect them against potential disasters such as fire or flood. A data backup is usually performed daily. Recovery from a data backup will likely result in some data loss between the time the backup was made and the time of disaster.

Data redundancy provides a short-term storage solution for data recovery in the case of an immediate system failure or power outage. Data redundancy requires that all electronic information is immediately stored twice—typically on magnetic media located in different physical locations. Since all data is immediately copied to a separate system, there is typically no data loss when the primary system fails. However, this solution is costly since it requires a full duplicate of the production system and the data must be synchronized between the two systems to ensure that changes made to the primary system are also made to the duplicate system.

C. Long-term Accessibility

To ensure long-term accessibility of electronic court data, courts should review their data storage technology periodically, at least every three to five years, to ensure that stored data can be retrieved. For example, ensure that technology exists to read backup tapes that have been placed into long-term storage and that optical discs that have been archived can be read by current optical readers.

If possible, courts should occasionally also take a random sample of backups that have been made and actually try to access the data using current technology to ensure that the backup is still accessible and contains valid information.

Courts should anticipate that storage and retrieval technology will continue to evolve and that new formats and standards will be created. Consequently, all electronic data records may at some point need to be migrated from existing technology platforms to new technology platforms.

When selecting a data backup and storage solution, overall cost and technology longevity need to be both considered and balanced. As technology ages, it becomes more difficult to retrieve data from storage devices as storage formats and connectivity standards evolve. For example, site data replication to a remote storage area network is likely to be more easily and reliably accessed in the long-term but initial implementation costs as well as ongoing network costs must be considered. Magnetic tape on the other hand typically has a lower initial cost but tape storage formats and mechanisms tend to change faster.

D. Selecting a Solution

Recommended:

1. Electronic records should be copied to magnetic tape or other medium daily for data backup and stored in an offsite storage location.
2. Physical records should not be destroyed until a backup of the electronic copy of the records have been made and confirmed to be retrievable.

Alternatives:

1. Optical storage can be used as secondary storage for infrequently accessed information.
2. Both onsite and offsite data redundancy and replication can be implemented if resources are available to add an extra level of data protection in case of a short-term service disruption.

Not Recommended:

1. Proprietary solutions that are only supported by a single vendor may jeopardize the ability to retrieve the electronic records in the future.

6.1.3.7 Retention and Destruction

Electronic records should be retained per Government Code section 68152 and destroyed per Government Code section 68153. For more information on records retention and destruction, see section 11, “Retention, Preservation, and Destruction of Court Records.”

Individual court records retention procedures should include the retention and destruction of electronic case management records, electronic documents, and physical case files.

The electronic repository of court records should be managed with the same focus as the physical records retention requirements have been managed. For example, if records are eligible for destruction, but an index is required, the case index would be preserved and the electronic case file would be deleted, just as the physical paper would be destroyed.

Each individual court should determine how long they wish to retain the original physical document after it has been converted to electronic format. Minimally, a court should not destroy the original physical document until the electronic copy of the document has been verified as a true image, copied to a backup, and that the backup has been validated.

Courts can save physical space, electronic storage, and management effort by destroying documents and electronic records as soon as feasibly possible.

6.1.3.8 References

National Archives transfer requirements regarding PDF documents containing OCR
http://www.archives.gov/records-mgmt/initiatives/pdf-records.html

Proposed legislation by Secretary of State of California, Trustworthy Electronic Document or Record Preservation
http://www.sos.ca.gov/admin/regulations/proposed/tech/electronic-docs/

AIIM 2009 Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)
http://www.sos.ca.gov/archives/local-gov-program/pdf/aiim-2009.pdf

Rule 1.44 of the California Rules of Court. Electronically produced forms
http://www.courtinfo.ca.gov/cms/rules/index.cfm?title=one&linkid=rule1_44

Rule 2.104 of the California Rules of Court. Printing; type size
http://www.courtinfo.ca.gov/cms/rules/index.cfm?title=two&linkid=rule2_104

Rule 2.105 of the California Rules of Court. Type style
http://www.courtinfo.ca.gov/cms/rules/index.cfm?title=two&linkid=rule2_105

Federal Judiciary transitioning to PDF/A
http://www.pacer.gov/announcements/general/pdfa.html

National Security Agency Information Assurance Guidance, Hidden Data and Metadata in Adobe PDF Files
http://www.nsa.gov/ia/_files/app/pdf_risks.pdf

Optical Disc Longevity
http://www.loc.gov/preservation/resources/rt/NIST_LC_OpticalDiscLongevity.pdf

~~6.2 Security and Protection~~

~~(The content for this section will be addressed in the next version of TCRM.)~~

6.2 Electronic Signatures: Standards and Guidelines

6.2.1 Electronic Signatures on Court-Created Records

A. Purpose

This section provides standards and guidelines for the creation of electronic signatures by judicial officers and the superior courts. These standards and guidelines implement Government Code section 68150(g), which provides that any notice, order, judgment, decree, decision, ruling opinion, memorandum, warrant, certificate of service, or similar document issued by a court or a judicial officer may be signed, subscribed, or verified using computer or other technology in accordance with procedures, standards, and guidelines established by the Judicial Council.

The following principles guided the drafters in preparing these standards and guidelines:

- Electronic signature standards should provide appropriate requirements and should generally not be more restrictive than standards for traditional 'wet' signatures.
- Electronic signature standards should consider how the signature is being applied when setting the level of authentication required.
- Electronic signature standards should allow for flexibility in the method of applying and the appearance of the signature.
- Electronic signature standards, wherever possible, should avoid requiring specific proprietary tools. Instead the standards should present attributes of acceptable authentication tools and encourage leveraging security within other business-critical systems.

B. Definitions

As used in these standards and guidelines, the following definitions apply:

- ***Electronic*** means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.
- ***Electronic court record*** means a court record created, generated, sent, communicated, received, or stored by electronic means.
- ***Electronic signature*** means an electronic sound, symbol, or process attached to or logically associated with an electronic court record and executed or adopted by a person with the intent to sign the electronic court record. (Code Civ. Proc., § 17.)
- ***Person*** includes judicial officers, court clerks, deputy court clerks, and others authorized to sign documents issued by a judicial officer or a court.
- ***Record*** means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
- ***Security procedure*** means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

C. Format of Signatures

Unless otherwise prescribed in a statute or rule, an electronic signature may be in the form of:

- A digitalized image of the person's signature;
- An "/s/" followed by the person's name; or
- Any other electronically created method of indicating with clarity the name of the person whose signature is being affixed to the document.

All such signatures, to be legally effective, must satisfy the requirements stated in this section.

D. Electronic Signatures Must Be Executed or Adopted With an Intent to Sign, Attributable to an Authorized Person, and Capable of Verification

The following guidelines apply to electronic signatures executed or adopted by a judicial officer or the court:

- When a person is presented with the opportunity to sign a document electronically, it must be clear to the person that he or she is being asked to sign the document electronically. This demonstrates that the person in fact intended to sign the document. (See Code Civ. Proc., § 17 [electronic signatures must be "executed or adopted with the intent to sign"].)
- When a document is to be signed electronically, it must be presented only to an authorized person or to someone authorized to execute the signature on the person's behalf.
- An electronic signature is attributed to a person if it was the act of that person (or the act of someone authorized to execute or adopt the signature on that person's behalf), which may be shown in any manner, including by showing the efficacy of any security procedure applied when the signature was executed or adopted.
- The identity of the person who executed or adopted the electronic signature must be capable of verification. If a document is signed electronically, the court should retain any data relevant to verifying the signature, such as the identity of the person who executed or adopted the signature and the date and time that the signature was executed or adopted.

 Courts should consider designing business practices and technology systems—such as workflows, pop-up screens, and access and security procedures—to facilitate compliance with these guidelines.

 Courts may want to consider utilizing different electronic signatures depending on whether the electronic signature is executed and adopted by a person or by someone authorized to execute and adopt the signature on that person's behalf. For example, if a clerk is authorized to sign on behalf of a judge, the clerk's initials could be placed after the judge's signature. Utilizing different signatures depending on the identity of the signer would make it easier to distinguish who actually executed or adopted the signature from the face of the document. Regardless, the court would still retain any data relevant to identifying the person who executed or adopted the signature for verification purposes.

 In deciding what types of verification data should be retained, courts may want to consider saving (1) the owner/user ID and timestamp (date and time) generated when a document is prepared, changed, or acted upon; and (2) the owner/user ID and timestamp (date and time) when the signer logs into an application, if the electronic signature is executed using an application.

E. Signatures Under Penalty of Perjury

If a law requires that a statement be signed under penalty of perjury, the requirement is satisfied with respect to an electronic signature if an electronic record includes:

- The electronic signature;
- All of the information as to which the declaration pertains; and
- A declaration under penalty of perjury by the person who submits the electronic signature that the information is true and correct.

F. Legal Effect

Unless otherwise specifically provided by law, all notices, orders, judgments, decrees, decisions, rulings, opinions, memoranda, warrants, certificates of service, or similar documents that are signed, subscribed, or verified by using a computer or other technological means shall have the same validity, and the same legal force and effect, as paper documents signed, subscribed, or verified by a court official or judicial officer. (Gov. Code, § 68150(g); see also Code Civ. Proc., § 34 ["An electronic signature . . . by a court or judicial officer shall be as effective as an original signature"].)

A signature may not be denied legal effect or enforceability solely because it is in electronic form. The legal effect of an electronic signature is determined from the context and circumstances surrounding its creation, execution, or adoption, and otherwise as provided by law.

G. Acceptable Security Procedures for Verification of Identity When Applying Electronic Signature

The acceptable procedures for verifying the identity of persons executing electronic signatures are varied and are subject to change as the technology in this area is developing quickly. Certain guidelines can be applied at this time to determine whether electronic signatures are verifiable.

First, all systems used in the capture, application, and storage of electronic media, including any electronic signatures or electronic documents, ~~are subject to~~should align, to the extent possible, with the data and information security guidelines ~~as~~ recommended in *How to Use the Information Systems Controls Framework: A Guide to California Superior Courts ~~(Draft May 27, 2015)~~*. This requirement ensures that access to any electronic signature, electronically signed document, or the tools and mechanisms for applying an electronic signature is limited to authorized individuals and that original files and documents have not been altered or modified since they were created.

Second, currently acceptable procedures for verification of electronic signatures include the following:

1. Real-time digitized electronic signatures

A digitized signature is a graphical image of a handwritten signature. The signature is captured by means of a digital pen, pad, or other device that converts the physical act of signing into a digital representation of the signature and applies that digital representation to the document, transaction, or database entry.

User authentication before the application of the digitized signature should be similar to authentication methods used when a physical handwritten signature is applied to a hard copy or traditional paper document.

2. System-applied electronic signatures

A system-applied electronic signature is an electronic signature that is applied to a document, transaction, or database through use of a computer, software, or application following affirmative action by the individual or a person authorized to act on the person's behalf. The affirmative action could include, for example, the requirement that the signer click on an "OK" box or similar act.

User authentication for applying a system-applied electronic signature may be obtained through one of the following methods:

- ***Password or PIN*** — The user is authenticated through a password or PIN to gain access to the computer application, database, or network. Alternatively or in addition, the user is authenticated through a password or PIN tied directly to the application of the signature.
- ***Symmetric Cryptography*** — The user is authenticated using a cryptographic key that is known to the system and the individual signing the document. This is often done via a single-use password that is randomly generated.
- ***Asymmetric Cryptography (Digital Certificates)*** — The user is authenticated using both private and public keys. This is the most secure method of user authentication and should be considered when applying signatures made under penalty of perjury.
- ***Biometrics*** — The user is authenticated using biometrics, including but not limited to voice, fingerprint, or retina.

The method selected should take into consideration business requirements, cost, and relative risk and consequence of a breach. Courts should document and adopt security procedures for authentication before the implementation of a system-applied electronic signature.

H. Judicial Signatures on Scanned Documents

Government Code section 68150(a) authorizes the preservation and maintenance of trial court records in electronic form. Under this provision, trial courts may convert their paper records to electronic form by scanning. The act of scanning an original signature results in a digitized signature. The digitized signature of a court or judicial officer created by scanning shall have the same validity, and the same legal force and effect, as the original signature.

I. Examples of Court-Created Documents That May Be Electronically Signed by a Judicial Officer or Clerk

The following is a list of various court-created documents that may be signed electronically by a judge or clerk under Government Code section 68150(g). This list is provided for illustrative purposes only. It is not intended to suggest that a signature is required on these documents, unless a signature is otherwise mandated by statute or rule.

- Judgments
- Deferred entry of judgment
- Orders after hearings
- Minute orders
- Exemplifications of records
- Probable cause determinations
- Arrest warrants
- Search warrants
- Bench warrants
- Protective orders
- Abstracts of judgment
- Summonses
- Notices
- Fee waivers granted by statute
- Certificates of mailing
- Clerk's declarations
- Entry of judgment
- Notices of intent to dispose of exhibits
- Certifications of records

- Letters for probate
- Writs of attachment
- Writs of possession
- Writs of execution
- Lis pendens
- Clerk's certificates of service
- Felony abstracts of judgment
- Notices of cost of electronic recording

6.2.2 Electronic Signatures on Documents Submitted to the Courts

A. Purpose

The purpose of this section is to provide guidance on the signatures that appear on documents that are submitted electronically to the courts. For such signatures, there is currently no equivalent to the comprehensive authorization for the use of electronic signatures that exists for the signatures of judicial officers and court clerks under Government Code section 68150(g) and Code of Civil Procedure section 34. There are, however, various statutes and rules on signatures on electronically submitted documents that apply to particular types of proceedings.

B. Signatures on Documents Filed Electronically in Civil Cases

The statutes and rules on e-filing in civil cases include specific provisions on signatures. Code of Civil Procedure section 1010.6(b)(2) provides:

> (A) When a document to be filed requires the signature, not under penalty of perjury, of an attorney or a self-represented party, the document shall be deemed to have been signed by that attorney or self-represented party if filed electronically.
>
> (B) When a document to be filed requires the signature, under penalty of perjury, of any person, the document shall be deemed to have been signed by that person if filed electronically and if a printed form of the document has been signed by that person prior to, or on the same day as, the date of filing. The attorney or person filing the document represents, by the act of filing, that the declarant has complied with this section. The attorney or person filing the document shall maintain the printed form of the document bearing the original signature and make it available for review and copying upon the request of the court or any party to the action or proceeding in which it is filed.

Similarly, the California Rules of Court have a specific rule on the requirement for signatures on documents filed electronically with the court. Rule 2.257 provides:

> **(a) Documents signed under penalty of perjury**

When a document to be filed electronically provides for a signature under penalty of perjury, the following applies:

(1) The document is deemed signed by the declarant if, before filing, the declarant has signed a printed form of the document.

(2) By electronically filing the document, the electronic filer certifies that (1) has been complied with and that the original, signed document is available for inspection and copying at the request of the court or any other party.

(3) At any time after the document is filed, any other party may serve a demand for production of the original signed document. The demand must be served on all other parties but need not be filed with the court.

(4) Within five days of service of the demand under (3), the party on whom the demand is made must make the original signed document available for inspection and copying by all other parties.

(5) At any time after the document is filed, the court may order the filing party to produce the original signed document in court for inspection and copying by the court. The order must specify the date, time, and place for the production and must be served on all parties.

(b) Documents not signed under penalty of perjury

If a document does not require a signature under penalty of perjury, the document is deemed signed by the party if the document is filed electronically.

(c) Documents requiring signatures of opposing parties

When a document to be filed electronically, such as a stipulation, requires the signatures of opposing parties, the following procedure applies:

(1) The party filing the document must obtain the signatures of all parties on a printed form of the document.

(2) The party filing the document must maintain the original, signed document and must make it available for inspection and copying as provided in (a)(2). The court and any other party may demand production of the original signed document in the manner provided in (a)(3)–(5).

(3) By electronically filing the document, the electronic filer indicates that all parties have signed the document and that the filer has the signed original in his or her possession.

(d) Digital signature

A party is not required to use a digital signature on an electronically filed document.

(e) Judicial signatures

If a document requires a signature by a court or a judicial officer, the document may be electronically signed in any manner permitted by law.

C. Signatures on Documents in Criminal and Traffic Cases

In criminal and traffic proceedings, the Legislature has authorized the use of electronic or digital signatures in particular types of matters.

1. Probable Cause Declarations for Warrants for Arrest

Penal Code section 817 addresses the procedures to be used when a peace officer submits a declaration of probable cause to obtain a warrant of arrest before criminal charges are filed.[1] These warrants are sometimes called *Ramey* warrants, referring to *People v. Ramey* (1976) 16 Cal.3d 263. (*Goodwin v. Superior Court* (2001) 90 Cal.App.4th 215, 218.) Penal Code section 817 requires the peace officer to submit a sworn statement made in writing in support of the warrant of probable cause. (Pen. Code, § 817(b).) As an alternative under Penal Code section 817(c)(2), the magistrate may take an oral statement under oath if the oral oath is made using telephone and facsimile transmission equipment, or made using telephone and electronic mail, and the following conditions are met:

(A) The oath is made during a telephone conversation with the magistrate, after which the declarant shall sign his or her declaration in support of the warrant of probable cause for arrest. The declarant's signature shall be in the form of a digital signature or electronic signature if electronic mail or computer server is used for transmission to the magistrate. The proposed warrant and all supporting declarations and attachments shall then be transmitted to the magistrate utilizing facsimile transmission equipment, electronic mail, or computer server.

[1] Penal Code section 817 does not apply to bench warrants or warrants for arrest that are sought via a criminal complaint. (Pen. Code, § 817(b); see also *id.*, §§ 740, 813.)

(B) The magistrate shall confirm with the declarant the receipt of the warrant and the supporting declarations and attachments. The magistrate shall verify that all the pages sent have been received, that all pages are legible, and that the declarant's signature, digital signature, or electronic signature is acknowledged as genuine.

(C) If the magistrate decides to issue the warrant,[2] he or she shall:

(i) Cause the warrant, supporting declarations, and attachments to be subsequently printed if those documents are received by electronic mail or computer server.

(ii) Sign the warrant. The magistrate's signature may be in the form of a digital signature or electronic signature if electronic mail or computer server is used for transmission to the magistrate.

(iii) Note on the warrant the exact date and time of the issuance of the warrant.

(iv) Indicate on the warrant that the oath of the declarant was administered orally over the telephone.

The completed warrant, as signed by the magistrate, shall be deemed to be the original warrant.

(D) The magistrate shall transmit via facsimile transmission equipment, electronic mail, or computer server, the signed warrant to the declarant who shall telephonically acknowledge its receipt. The magistrate shall then telephonically authorize the declarant to write the words "duplicate original" on the copy of the completed warrant transmitted to the declarant and this document shall be deemed to be a duplicate original warrant.

2. Probable Cause Declarations for Search Warrants: Penal Code Section 1526(b)

Before issuing a search warrant, the magistrate must take the officer's affidavit in writing and cause the affidavit to be subscribed by the affiant. (Pen. Code, § 1526(a); see *Powelson v. Superior Court* (1970) 9 Cal.App.3d 357, 360–361.) As an alternative to this written affidavit, Penal Code section 1526(b)(2) authorizes the magistrate to take an oral statement under oath if the oral oath is made using telephone and facsimile transmission equipment, telephone and electronic mail, or telephone and computer server, and if the following conditions are met:

[2] The magistrate may issue the warrant if, and only if, he or she is satisfied from the declaration that there exists probable cause that the offense described in the declaration has been committed and that the defendant described in the declaration has committed the offense. (Pen. Code, § 817(a)(1).)

(A) The oath is made during a telephone conversation with the magistrate, after the affiant has signed his or her affidavit in support of the application for the search warrant and transmitted the proposed search warrant and all supporting affidavits and documents to the magistrate. The affiant's signature may be in the form of a digital signature or electronic signature if electronic mail or computer server is used for transmission to the magistrate.

(B) The magistrate shall confirm with the affiant the receipt of the search warrant and the supporting affidavits and attachments. The magistrate shall verify that all the pages sent have been received, that all pages are legible, and that the affiant's signature, digital signature, or electronic signature is acknowledged as genuine.

(C) If the magistrate decides to issue the search warrant, he or she shall:

(i) Sign the warrant. The magistrate's signature may be in the form of a digital signature or electronic signature if electronic mail or computer server is used for transmission by the magistrate.

(ii) Note on the warrant the exact date and time of the issuance of the warrant.

(iii) Indicate on the warrant that the oath of the affiant was administered orally over the telephone.

(D) The magistrate shall transmit via facsimile transmission equipment, electronic mail, or computer server, the signed search warrant to the affiant. The completed search warrant, as signed by the magistrate and received by the affiant, shall be deemed to be the original warrant. The original warrant and any affidavits or attachments in support thereof shall be returned as provided in Penal Code section 1534.

3. Electronic Signatures on Notices to Appear

Vehicle Code section 40500 addresses Notices to Appear for traffic violations and requires that the arresting officer prepare in triplicate a written notice to appear in court. (Veh. Code, § 40500(a); *id.*, § 40600(a) [similar provisions].) The arresting officer must deliver a copy to the arrested person, a copy to the court, and a copy to the commissioner, chief of police, sheriff or other superior officer of the arresting officer. (*Id.*, §§ 40500(d), 40506.) A Notice to Appear may also be issued for nontraffic infraction and misdemeanor offenses. (Pen. Code, §§ 853.5, 853.6.)

Penal Code section 959.1(d)–(f) authorizes a court to receive and file an electronically transmitted Notice to Appear issued on a form approved by the Judicial Council if the following conditions are met:

(1) The notice to appear is issued and transmitted by a law enforcement agency pursuant to [specified Penal Code or Vehicle Code sections].

(2) The court has all of the following:

(A) The ability to receive the notice to appear in electronic format.

(B) The facility to electronically store an electronic copy and the data elements of the notice to appear for the statutory period of record retention.

(C) The ability to reproduce the electronic copy of the notice to appear and those data elements in printed form upon demand and payment of any costs involved.

(3) The issuing agency has the ability to reproduce the notice to appear in physical form upon demand and payment of any costs involved.

The Notice to Appear that is received under Penal Code section 959.1(d) is deemed to have been filed when it has been accepted by the court and is in the form approved by the Judicial Council. If transmitted in electronic form, the Notice to Appear is deemed to have been signed by the defendant if it includes a digitized facsimile of the defendant's signature on the Notice to Appear. The Notice to Appear filed electronically under Penal Code section 959.1(d) need not be subscribed by the citing officer. An electronically submitted Notice to Appear need not be verified by the citing officer with a declaration under penalty of perjury if the electronic form indicates which parts of the notice are verified by that declaration and the name of the officer making the declaration.

A Judicial Council Notice to Appear form that is issued when a person is arrested for misdemeanor or infraction violations of the Vehicle Code or for nontraffic misdemeanors or infractions serves as a complaint. (Veh. Code § 40500(b); Pen. Code, § 853.9(b).) Under rule 4.103 of the California Rules of Court, the Judicial Council has approved the following types of Notice to Appear forms:

Form TR-115	*Automated Traffic Enforcement System Notice to Appear*
Form TR-130	*Traffic/Nontraffic Notice to Appear*
Form TR-120	*Nontraffic Notice to Appear*
Form TR-106	*Continuation of Notice to Appear*
Form TR-108	*Continuation of Citation*

Form TR-130 is used for both electronic and handwritten citations. (See www.courts.ca.gov/documents/trinst.pdf; Cal. Rules of Court, rule 4.103.)

6.2.3 Signatures on Scanned Documents

Government Code section 68150(a) authorizes the preservation and maintenance of trial court records in electronic form. Under this provision, trial courts may convert their paper records to electronic form by scanning. The act of scanning an original signature results in a digitized signature. This digitized signature shall have the same validity, and the same legal force and effect, as the original signature. This section applies generally to electronic signatures by parties and others on documents submitted to the courts, in addition to electronic signatures by judicial officers and courts (which are also addressed above in the standards and guidelines implementing Government Code section 68150(g).)

7. Exhibits Management

Exhibits management is a fundamental responsibility of records managers. Accepting, maintaining, returning, and disposing of exhibits is generally the responsibility of the clerk of the court, unless the court orders otherwise.

Each trial court is encouraged to develop local procedures for managing exhibits, including

- scheduling periodic physical inventory of exhibits,
- handling of dangerous or biohazard exhibits,
- handling of exhibits with a high monetary value,
- transferring custody of exhibits between courtroom staff and exhibits custodians,
- monitoring the movement of exhibits from courtrooms to vaults or exhibit rooms,
- permitting the public viewing of exhibits,
- accounting for lost exhibits,
- alerting parties when exhibits are available to be returned or destroyed,
- managing exhibits while cases are under appeal,
- requesting extension of time for the court to retain exhibits, and
- notifying entities designated by the Judicial Council of the court's intent to destroy felony or unlimited civil records, pursuant to rule 10.856 of the California Rules of Court.

Pursuant to rule 2.400(c)(1) of the California Rules of Court, the clerk must not release any exhibit except on order of the court. The clerk must require a signed receipt for a released exhibit.

7.1 Receiving, Handling, and Transfer of Exhibits in Criminal Cases

Pursuant to Penal Code section 1417, all exhibits that have been introduced or filed in any criminal action or proceeding shall be retained by the clerk of the court, who shall establish a procedure to account for the exhibits properly, subject to Penal Code sections 1417.2 and 1417.3, until final determination of the action or proceedings, and the exhibits shall thereafter be distributed or disposed of as provided in the code.

7.2 Receiving, Handling, and Transfer of Exhibits in Civil Cases

Pursuant to Code of Civil Procedure section 1952, all exhibits introduced, lodged, or filed in any civil or small claims action or proceeding shall be retained by the clerk of the court for 60 days following the judgment date or date of appellate decision.

Pursuant to Code of Civil Procedure section 1952.3, exhibits related to sealed civil files must be retained for an additional two years beyond the date that they would have been destroyed had the records not been sealed.

7.3 Protocols for Dangerous and Biohazard Exhibits

The court may adopt local orders or rules that address the custodial responsibilities for managing exhibits that are dangerous or contain biohazard materials. Courts may make arrangements with prosecuting agencies or local law enforcement agencies to secure such exhibits in their own secure evidence lockers or vaults, as an alternative to having court staff handle these dangerous items.

As noted in Penal Code section 1417.9(a)(b) notwithstanding any other provision of law, the court shall retain all biological material that is secured in connection with a criminal case for the period of time that any person remains incarcerated in connection with that case. The court shall have the discretion to determine how the evidence is retained pursuant to this section, provided that the evidence is retained in a condition suitable for deoxyribonucleic acid (DNA) testing. The court may dispose of biological material before the expiration of the period of time described in Penal Code section 1417.9(b).

7.3.1 Exhibits That Pose a Security, Storage, or Safety Problem (Pen. Code, § 1417.3(a))

The clerk may recommend the return of exhibits that pose security, storage, or safety problems prior to the final determination of the actions or proceedings.

If an exhibit by its nature is severable, the court shall order the clerk to retain a portion of the exhibit not exceeding three pounds by weight or one cubic foot by volume and shall order the return of the balance of the exhibit to the district attorney.

The clerk, upon court order, shall substitute a full and complete photographic record of any exhibit or part of any exhibit returned to the state under this section. The party to whom the exhibit is being returned shall provide the photographic record. (Pen. Code, § 1417.3(a))

7.3.2 Exhibits That Are Toxic (Pen. Code, § 1417.3(b))

Exhibits toxic by their nature that pose a health hazard to humans shall be introduced to the court in the form of a photographic record and a written chemical analysis certified by competent authority.

Where the court finds that good cause exists to depart from this procedure, toxic exhibits may be brought into the courtroom and introduced. However, following introduction of the exhibit, the person or persons previously in possession of the exhibit shall take responsibility for it, and the court shall not be required to store the exhibit. (Pen. Code, § 1417.3(b))

7.3.3 Dangerous or Deadly Weapons, Poisonous Drugs, Explosives, or Any Property Prohibited by Law (Pen. Code, § 1417.6(a)) and Biological Material for DNA Testing (Pen. Code, § 1417.9(a))

Any of this property introduced or filed as an exhibit shall not be returned under the provisions of Penal Code section 1417.6(a), but instead, by order of the trial court, be destroyed or otherwise disposed of under the conditions provided in the order no sooner than 60 days after the final determination of the criminal action or proceeding. For biological material introduced or filed as an exhibit in connection with a criminal case under the provisions of Penal Code section 1417.9(a), the appropriate governmental entity shall retain for the period of time that any person remains incarcerated in connection with that case. The governmental entity shall have the discretion to determine how the evidence is retained pursuant to this section, provided that the evidence is retained in a condition suitable for DNA testing.

7.4 Protocols for Cash Value, Historical Value, Narcotics, Sensitive Photographs, Private Property

7.4.1 Exhibits Composed of Money or Currency of Unknown Ownership (Pen. Code, § 1417.5(c)(4) & §§ 1420–1422)

If the party entitled to money or currency fails to apply for the return of the exhibit prior to the date for disposition under Penal Code section 1417.5, the exhibit shall be disposed of pursuant to Penal Code section 1420.

All money received by a district attorney or clerk of the court in any criminal action or proceeding, the owner or owners of which are unknown, and which remains unclaimed in the possession of the district attorney or clerk of the court after final judgment in the criminal action or proceeding, shall be deposited with the county treasurer. Upon the expiration of two years after the deposit, the county treasurer shall cause a notice pursuant to Penal Code section 1421 to be published once a week for two successive weeks in a newspaper of general circulation published in the county.

The notice shall state the amount of money, the criminal action or proceeding in which the money was received by the district attorney or clerk of the court, the fund in which it is held and that it is proposed that the money will become the property of the county on a designated date not less than 45 days nor more than 60 days after the first publication of the notice.

Unless someone files a verified complaint seeking to recover all, or a designated part, of the money in a court of competent jurisdiction within the county in which the notice is published, and serves a copy of the complaint and the summons issued thereon upon the county treasurer before the date designated in the notice, upon that date the money becomes the property of the county and shall be transferred by the treasurer to the general fund.

7.4.2 Exhibits Composed of Stolen or Embezzled Money or Currency (Pen. Code, § 1417.5(c)(1))

If the party entitled to stolen or embezzled money or currency fails to apply for the return of the exhibit prior to the date for disposition under Penal Code section 1417.5, the exhibit shall be disposed of pursuant to Penal Code section 1417.6.

7.4.3 Exhibits Composed of Property Other Than Money or Currency That Is Unclaimed (Pen. Code, § 1417.5(c)(3))

Exhibits of property, other than money, currency, or stolen or embezzled property, that are determined by the court to have no value at public sale shall be destroyed or otherwise disposed of pursuant to court order. (Pen. Code, § 1417.5(c)(3))

7.4.4 Exhibits Composed of Property of Value That Is Unclaimed (Pen. Code, § 1417.5(c)(2))

Exhibits of property other than property that is stolen or embezzled or property that consists of money or currency shall, except as otherwise provided in this paragraph and in paragraph (3), be transferred to the appropriate county agency for sale to the public in the same manner provided by Article 7 (commencing with Section 25500) of Chapter 5 of Part 2 of Division 2 of Title 3 of the Government Code for the sale of surplus personal property. If the county determines that any property is needed for a public use, the property may be retained by the county and need not be sold. (Pen. Code, § 1417.5(c)(2))

7.4.5 Exhibits Composed of Photographs of Minors Deemed Harmful (Pen. Code, § 1417.8(a))

Prior to the final determination of the action or proceeding, the photograph of any minor that has been found by the court to be harmful matter, as defined in Penal Code section 313, shall be available only to the parties or to a person named in a court order to receive the photograph.

After the final determination of the action or proceeding, the photograph shall be preserved with the permanent record maintained by the clerk of the court. The photograph may be disposed of or destroyed after preservation through any appropriate photographic or electronic medium. If the photograph is disposed of, it shall be rendered unidentifiable before the disposal. No person shall have access to the photograph unless that person has been named in a court order to receive the photograph. Any copy, negative, reprint, or other duplication of the photograph in the possession of the state, a state agency, the defendant, or an agent of the defendant shall be delivered to the clerk of the court for disposal whether or not the defendant was convicted of the offense. (Pen. Code, § 1417.8(a))

7.5 Death Penalty Exhibits

In cases where the death penalty is imposed, exhibits may be destroyed 30 days after the date of execution of sentence. (Pen. Code, § 1417.1(d)(1).)

In cases where the death penalty is imposed and the defendant dies while awaiting execution, exhibits may be destroyed one year after the date of the defendant's death. (Pen. Code, § 1417.1(d)(2).)

8. Public Calendars, Indexes, and Registers of Action Minimum Standards

Court calendars are listings of individual cases prepared for use by the clerk of the court and other courtroom personnel in calling cases in an orderly manner. They provide the public with the ability to research and locate court events for a particular individual, case number, or cases being heard on a given day. Public court calendars may be discarded after they are no longer of use.

Indexes are important records of all public cases filed in the court, except infractions and confidential case types, and serve as a cross-reference of case names to the case numbers. Courts are encouraged to create a linkage, preferably automated, between new records entered in case management systems and entries in public indexes. Ideally, a public index entry is created at the same time a new case is filed with the court. Indexes available to the public shall not contain information restricted by statute or rule of court.

Registers of actions, also known as dockets, provide a chronological list of actions taken by the court, as well as some or all of the documents filed in the court. Since the register of actions represents the history of activities in a case, it is vital that it be updated regularly and with as much information as possible.

Under rule 2.503(b) of the California Rules of Court, electronic access to court calendars, indexes, and registers of actions may be available both remotely and at the courthouse, to the extent it is feasible.

8.1 Minimum Content for Court Calendars, Indexes, and Registers of Action

Rule 2.507(b) of the California Rules of Court specifies the minimum content requirements for electronically accessible court calendars, indexes, and registers of action.

The electronic court calendar must include

- date of court calendar,
- time of calendared event,
- court department number,
- case number, and
- case title (unless made confidential by law).

The electronic index must include

- case title (unless made confidential by law),
- party names (unless made confidential by law),
- party type,

- date on which the case was filed, and
- case number.

The register of actions must be a summary of every proceeding in a case, in compliance with Government Code section 69845, and must include

- date case commenced,
- case number,
- case type,
- case title (unless made confidential by law),
- party names (unless made confidential by law),
- party type,
- date of each activity, and
- description of each activity.

8.2 Historical Data Fields Restrictions

Under rule 2.507(c) of the California Rules of Court, the following information must be excluded from court electronic calendar, index, and register of actions:

- social security number,
- any financial information,
- arrest warrant information,
- search warrant information,
- victim information,
- witness information,
- ethnicity,
- age,
- gender,
- government-issued identification card numbers (i.e., military),
- driver's license number, and
- date of birth.

9. Disaster Recovery Planning and Procedures

9.1 Planning for a Disaster

Effective disaster recovery planning and procedures are critical to court records management. In the event of a disaster, a well-planned and well-managed recovery plan can provide expedient access of court records for the court and the general public. Disaster planning, response, and recovery are key components of a comprehensive records management program. The best planning for a disaster is the systematic and full implementation of each major component of a court records management program.

9.2 Response to Disasters

Courts are encouraged to take decisive action after a disaster. The first priority is to assess the scope and nature of the damage to equipment, facilities, and records. It is recommended that the records manager assess the effect of the disaster on records as soon as it is safe to enter the affected area. It is critical to document the location, type, quantity of records affected, and the nature and severity of damage. Once this is accomplished, the prioritization of the recovery plan can proceed.

The court's continuity of operations plan (COOP) prioritizes the functions that are critical if the court will be closed for any period of time, from one day to one week or longer. The COOP can also provide a beneficial guide to prioritizing records recovery efforts. A much different response, but no less urgent, would be called for if the disaster were to affect a remote records facility that holds infrequently accessed archival records. These records may not be needed to resume court operations, but the court has an obligation to safeguard all records under its control.

Data redundancy is a key feature of any effective disaster recovery plan. As this concept relates to court records, redundancy can be created by storing a complete copy of film, magnetic, optical, and digital data at a secure facility at least 50 miles from the court. Several companies specialize in this kind of records storage and will work with the court to create a regular schedule to deliver backup copies of court data to the off-site facility.

9.3 Disaster Recovery

The objective of disaster recovery is to salvage records efficiently and economically while attempting to preserve their integrity for future use. Recovery seeks to salvage or reconstruct case-related information on active files and preserve closed records for at least the minimum retention period required. The severity of the underlying disaster may make such efforts impractical or impossible, but a full assessment should be made of the condition of court records prior to making decisions about recovery.

- Preliminary concerns: Records managers must thoroughly understand the content of the records inventory, including the affected record series and their retention and disposition dates, and their relative importance for the court's daily operations.
- Salvage operations: When records are damaged (soaked, burned, buried, etc.), effective salvage operations require coordination and speed. Mitigating and reversing damage becomes more difficult the longer the salvage effort is delayed.

Creating a master list of the damaged records launches the salvage effort. If the records inventory is complete and current, this list will be relatively easy to compile. Determining whether the damaged records can be duplicated from other sources (microfilm, optical discs, etc.) is the next step. If copies of microfilmed and electronic records are stored at an alternate location, any damaged working copies of microfilm or electronic records may be reconstructed from the off-site originals.

Salvageable records should be examined to determine what can be saved, what was lost or irreparably damaged, and what can be destroyed. Records managers should catalog salvageable records to keep track of their identity and whereabouts throughout the salvage process.

After the preliminary analysis and inventory, salvage efforts may begin. The ~~AOC~~ Judicial Council may be able to assist courts with locating specialists, equipment, and supplies needed to address the specific type of damage to the records. The proper procedures to follow for different kinds of damage are available in many records management sources.

The primary objective of a disaster recovery effort is to salvage active cases and court orders from closed cases. There may be other permanent, intrinsically valuable documents, however, that also deserve priority attention in salvage operations. Courts are legally required to maintain these permanent records, even if they are not vital records, because of their continuing historical, legal, and aesthetic value. Salvageable permanent records that have enduring value shall not be authorized for destruction. Courts may postpone restoring these records, however, once their condition has been stabilized and delayed application of conservation techniques will not cause further deterioration.

Information related to disaster recovery efforts may be updated periodically, and preferably annually. The records inventory, storage area diagrams, contacts (including names, addresses, and telephone numbers), as well as the court's COOP and other policies and procedures are important source documents in any disaster recovery effort.

10. Public Access to Court Records

10.1 Public Access to Trial Court Records

10.1.1 Paper Court Records

Court records are presumed to be open, unless they are confidential as a matter of law or are sealed by court order. Confidential and sealed records are described in section 10.3, "Confidential and Sealed Records."

For information on filing systems for paper records, see section 4.3, "Filing Systems for Court Records Maintained in Paper Format"; for the tracking of paper records, see section 4.5.1, "Paper Record Tracking."

10.1.2 Electronic Court Records

Rules 2.500–2.507 of the California Rules of Court are intended to provide the public with reasonable access to trial court records that are maintained in electronic form while protecting privacy interests. The rules are not intended to give the public a right of access to any electronic record that they are not otherwise entitled to access in paper form, and do not create any right of access to records sealed by court order or confidential as a matter of law. These rules apply only to trial court records and only to access to court records by the public. They do not prescribe the access to court records by a party to an action or proceeding, by the attorney for a party, or by other persons or entities that may be entitled to such access by statute or rule.

Courthouse and Remote Access to Electronic Records

The law requires that court records maintained in electronic form "shall be made reasonably accessible to all members of the public for viewing and duplication as the paper records would have been accessible." (Gov. Code, § 68150(l).) Electronic access must be available at the courthouse and may also be made available remotely. There are some important restrictions on the records that may be made available remotely that do not apply to records at the courthouse. (See rule 2.503 for a list of the types of records, including criminal and family law records that may be made available only at the courthouse.)

If a court maintains records in electronic form, it must provide a means for the public to view those records at the courthouse. "Unless access is otherwise restricted by law, court records maintained in electronic form shall be viewable at the courthouse, *regardless of whether they are also accessible remotely*." (Gov. Code, § 68150(*l*) (emphasis added).)

Access to Registers of Action, Calendars, and Indexes

Courts that maintain records in electronic form must, to the extent feasible, provide—both at the courthouse and remotely—access to registers of action, calendars, and indexes. (Cal. Rules of Court, rule 2.503(b).) The minimum contents for electronically accessible court

calendars, indexes, and registers of action are prescribed by rule. (See rule 2.507(b).) There is also a rule on what information must be *excluded* from court calendars, indexes, and registers of action; the information to be excluded includes social security numbers, financial information, arrest and search warrant information, victim and witness information, ethnicity, age, gender, government (i.e., military) ID numbers, driver's license numbers, and dates of birth. (See rule 2.507(c).)

10.2 Remote Electronic Access Allowed in High-Profile Criminal Cases

One of the most time-consuming tasks for court staff is serving the demand for court records from the media and public interested in a high-profile criminal case. The use of technology can assist the court in dealing with the large number of requests for court records pertaining to these types of cases.

Notwithstanding the general restriction against providing criminal records remotely in rule 2.503(c), under rule 2.503(e) , the presiding judge or a designated judge may order the records of a high-profile criminal case to be posted on the court's website to enable faster and easier access to these records by the media and public. This rule specifies several factors that judges must consider before taking such action. Prior to posting, staff should, to the extent feasible, redact any confidential information contained in the court documents in accord with California Rules of Court, rule 2.503(e)(2). In addition, five days' notice must be provided to the parties and the public before the court makes a determination to provide electronic access under this rule. Notice to the public may be accomplished by posting notice on the court's website. Once issued, a copy of the order must also be posted on the website.

10.3 Confidential and Sealed Records

10.3.1 Confidential Records

A nonexhaustive list of records that are exempt from the presumption of public disclosure by statute, regulation, court rule, or case law is provided below.[3] This list of confidential records is divided into criminal, civil, family and juvenile, probate, and protective order records and jury information. As indicated below, there are some records that by law are strictly confidential and others that may be confidential in particular circumstances. Sealed records, including those that fall under Evidence Code section 1040 et seq., are discussed in section 10.3.2., "Sealed Records."

[3] See Appendix 1 for chart containing a more complete list of types or cases or documents that may be confidential by statute or rule.

Criminal Case Records

Records that are confidential

1. Indigent defendant requests for funds: A request for funds for payment of investigators, experts, and others to aid in presenting or preparing the defense in certain murder cases is confidential. This exemption applies to defendants in capital and life without parole murder cases under Penal Code section 190.05(a). (Pen. Code, § 987.9.)
2. Arrest records: The arrest record for a defendant found to be factually innocent is confidential. (Pen. Code, §§ 851.8, 851.85.)
3. Psychiatric records or reports: Reports prepared at the request of defense counsel to determine whether to enter or withdraw a plea based on insanity or mental or emotional condition are confidential. (Evid. Code, § 1017.) However, most psychiatric reports prepared at the court's request are presumed open to the public. (See Evid. Code, § 1017; Evid. Code, § 730 [report by a court-appointed expert]; Pen. Code, § 288.1 [report on sex offender prior to suspension of sentence]; Pen. Code, § 1368 [report concerning defendant's competency]; and Pen. Code, §§1026, 1027 [report on persons pleading not guilty by reason of insanity].)
4. Probation reports: Probation reports filed with the court are confidential *except* that they may be inspected
   - by anyone up to 60 days after either of two dates, whichever is earlier: (1) when judgment is pronounced, or (2) when probation is granted;
   - by any person pursuant to a court order;
   - if made public by the court on its own motion; and
   - by any person authorized or required by law. (Pen. Code, § 1203.05.)
5. Defendant's Statement of Assets Form (CR-115): This mandatory Judicial Council form is confidential in the same manner as probation reports. (See Pen. Code, § 1202.4.)
6. Presentencing diagnostic reports under Penal Code section 1203.03: The report and recommendation from the 90-day Department of Corrections presentencing diagnosis should be released only to defendant or defense counsel, the probation officer, and the prosecuting attorney. After the case closes, only those persons listed immediately above, the court, and the Department of Corrections may access the report. Disclosure to anyone else is prohibited unless the defendant consents. (Pen. Code, § 1203.03, subd. (b).)
7. Victim impact statements: Victim impact statements filed with the court must remain under seal until imposition of judgment and sentence, except that the court, the probation officer, and counsel for the parties may review such statements up to two days before the date set for imposition of judgment and sentence. (Pen. Code, § 1191.15, subd. (b).) Victim impact statements shall not be otherwise reproduced in any manner. (Pen. Code, § 1191.15, subd. (c).)
8. Criminal history information rap sheets: Summaries of criminal history information are confidential. (*Westbrook v. Los Angeles* (1994) 27 Cal.App.4th 157, 164; Pen. Code, §§ 11105 and 13300–13326.) Public officials have a duty to preserve the

confidentiality of a defendant's criminal history. (*Craig v. Municipal Court* (1979) 100 Cal.App.3d 69, 76.) Unauthorized disclosure of criminal history violates a defendant's privacy rights under the California Constitution. *(Ibid.)* Courts have upheld the confidentiality assigned to criminal history records. (See, e.g., *Westbrook v. Los Angeles* (1994) 27 Cal.App.4th 157 [unauthorized private company was denied access to municipal court information computer system].)

9. Reports concerning mentally disordered prisoners: Reports under Penal Code section 4011.6 to evaluate whether prisoners are mentally disordered are confidential. (Pen. Code, § 4011.6.)

Records that may be confidential

1. Police reports: There is no specific statute, rule, or decision addressing the confidentiality of a police report once it has become a "court record." Generally speaking, a police report that has been used in a judicial proceeding or is placed in a court file is presumed to be open to the public. Many police reports, however, contain sensitive or personal information about crime victims, witnesses, and other third parties. Penal Code section 1054.2 provides that defense counsel may not disclose the address or telephone number of a victim or witness to the defendant or his or her family. Similarly, law enforcement agencies are prohibited from disclosing the address and phone number of a witness or victim, or an arrestee or potential defendant. (Pen. Code, § 841.5.) We suggest that courts should require that personal information be redacted *before* the report is filed with the court or used in a judicial proceeding.
2. Search warrants: It is within the court's discretion to seal the court documents and records of a search warrant until the warrant is executed and returned, or until the warrant expires. (Pen. Code, § 1534, subd. (a).) Thereafter, if the warrant has been executed, the documents and records shall be open to the public as a judicial record.
3. Identity of sex offense victims: The victim of an alleged sexual offense may request anonymity from the court. Upon a proper showing, the judge may order the identity of the victim in all records and during proceedings to be either "Jane Doe" or "John Doe" if the judge finds that such an order is reasonably necessary to protect the alleged victim's privacy and that such measures will not unduly prejudice the prosecution or defense. (Pen. Code, § 293.5.)
4. Records from federally funded drug rehabilitation centers: The Code of Federal Regulations provides that information that would disclose the identity of a person receiving treatment for drug or alcohol abuse under a federally funded program is confidential. (42 C.F.R. § 2.12.) For example, the drug court program receives federal funding. Thus any information that would disclose the names of persons in that program appears to be confidential. Notably, the confidentiality provisions governing federally funded programs are quite broad and include information from a program funded in part by special or general revenue sharing program that receives federal funding. (See *ibid*. at § 2.12(b)(3).)
5. Records of arrest or conviction for marijuana possession or other related offense: These records must be destroyed two years from the date of conviction or arrest if there was no conviction. (Health & Saf. Code, § 11361.5, subd. (c).) This rule is

subject to exceptions for offenders under 18 years of age, records from judicial proceedings, and records related to an offender's civil action against a public entity. (See Health & Saf. Code, § 11361.5.) Public agencies are prohibited from using information in records subject to destruction, even if they have not yet been destroyed. (Health & Saf. Code, 11361.7, subd. (b).)

Civil Case Records

Records that are confidential

1. Fee waiver applications: Applications to proceed without paying court fees and costs are confidential. (Cal. Rules of Court, rule 3.54.)
2. Unlawful detainer proceedings: Court files and records in unlawful detainer proceedings are not publicly available until 60 days after the case is filed, except for persons specified by statute, unless a defendant prevails in the action within 60 days of the filing of the complaint, in which case the clerk may not allow access to any court records in the action except to persons specified in the statute. An exception excludes records of mobile home park tenancies from this code section; those records are not confidential. In addition, effective January 1, 2011, access to court records in unlawful detainer proceedings is permanently limited to persons specified in the statute in the case of complaints involving residential property based on section 1161a (holding over after sale under execution, mortgage, or trust deed [foreclosures]) as indicated in the caption of the complaint, unless judgment has been entered, after a trial, for the plaintiff and against all defendants. (Code Civ. Proc., § 1161.2.) The complaints in these actions shall state in the caption: "Action based on Code of Civil Procedure section 1161a."(Code Civ. Proc., § 1166(c).)
3. Confidential Statements of Taxpayer's Social Security Number in garnishment cases (forms WG-021 and WG-025): These mandatory Judicial Council forms for use in connection with wage garnishments are confidential.[4]
4. False Claims Act Cases: The documents initially filed in cases under the False Claims Act are confidential under Government Code section 12650 et seq. The complaint and other initial papers should be attached to a Confidential Cover Sheet—False Claims Action (form MC-060). The cover sheet contains a place where the date on which the sealing of the records in the case expires.

Records that may be confidential

1. Records and documents in attachment cases: At the time of filing, the plaintiff can request that records in the action not be made publicly available. In such a case, the clerk must maintain the records as confidential until 30 days after the filing of the complaint, or until the filing of the return of service of the notice of hearing and any temporary protective order, or of the writ of attachment if issued without notice, whichever occurs first. (Code Civ. Proc., § 482.050, subd. (a).)

[4] Any Judicial Council form that is now or hereafter labeled or entitled "CONFIDENTIAL" should not be disclosed except as ordered by a judge.

Confidentiality Provisions Relevant to Both Criminal and Civil Cases

Records that are confidential

1. Records of mental health treatment or services for the developmentally disabled, including LPS proceedings: Under Welfare and Institutions Code sections 5328 and 5330, the following records are confidential and can be disclosed only to recipients authorized in Welfare and Institutions Code section 5328: records related to the Department of Mental Health (Welf. & Inst. Code, § 4000 et seq.); Developmental Services (Welf. & Inst. Code, § 4400 et seq.); Community Mental Health Services (Welf. & Inst. Code, § 5000 et seq.); services for the developmentally disabled (Welf. & Inst. Code, § 4500 et seq.); voluntary admission to mental hospitals (Welf. & Inst. Code,§ 6000 et seq.); and mental institutions (Welf. & Inst. Code,§ 7100 et seq.).
2. Subpoenaed business records: Subpoenaed business records of nonparty entities are confidential until introduced as evidence or entered into the record. (Evid. Code, § 1560, subd. (d).)
3. Social security numbers and financial account numbers: California Rules of Court, rule 1.20**,** imposes a duty on the parties or their attorneys to redact certain identifiers from documents filed with the court. It is the responsibility of the filers to exclude or redact the identifiers. The rule states that court clerks will not review each pleading or other paper for compliance with the requirements of the rule. In an appropriate case, the court on a showing of good cause may order a party filing a redacted document to file a Confidential Reference List (form MC-120) identifying the redacted information. This form is confidential.
~~3.~~4. Special Immigrant Juvenile Findings: In any judicial proceedings in response to a request that the superior court make the findings necessary to support a petition for classification as a special immigrant juvenile, information regarding the child's immigration status that is not otherwise protected by the state confidentiality laws must remain confidential and must be available for inspection only by the court, the child who is the subject of the proceeding, the parties, the attorneys for the parties, the child's counsel, and the child's guardian. (Code Civ. Proc., § 155(c).)

Records that may be confidential

1. Special Immigrant Juvenile Findings: In any judicial proceedings in response to a request that the superior court make the findings necessary to support a petition for classification as a special immigrant juvenile, records of the proceedings that are not otherwise protected by state confidentiality laws may be sealed using the procedure in California Rules of Court, rules 2.550 and 2.551. (Code Civ. Proc., § 155(d).)

Family and Juvenile Court Records

Records that are confidential

1. Juvenile Court records: Welfare and Institutions Code section 827 and California Rules of Court, rule 5.552**,** establish broad restrictions on the disclosure of juvenile

court records. These laws reflect a general policy that, with certain limited exceptions, juvenile court records should remain confidential. (*In re Keisha T.* (1995) 38 Cal.App.4th 220, 225.) Specifically, section 827(a)(1)(P) permits juvenile court records to be inspected only by certain specified persons and "any other person who may be designated by court order of the judge of the juvenile court upon filing a petition." There is also an exception to this rule of confidentiality for certain records in cases brought under Welfare and Institutions Code section 602, in which the minor is charged with one or more specified violent offenses. (Welf. & Inst. Code, § 676.) In such cases, the charging petition, the minutes, and the jurisdictional and dispositional orders are available for public inspection (Welf. & Inst. Code, § 676, subd. (d)), unless the juvenile court judge enters an order prohibiting disclosure (Welf. & Inst. Code, § 676, subd. (e)). Thus, except for records enumerated in Welfare and Institutions Code section 676, if a record is part of a juvenile court file, it should be kept confidential and disclosed only as permitted under Welfare and Institutions Code section 827 and rule 5.552.

2. Immigration status: Juvenile court records should remain confidential regardless of a juvenile's immigration status. (Welf. & Inst. Code, § 831(a).) Juvenile information may not be disclosed or disseminated to federal officials absent a court order upon filing a petition under Welfare and Institutions Code section 827(a). (Welf. & Inst. Code, § 831(b)–(c).) Juvenile information may not be attached to any documents given to or provided by federal officials absent prior approval of the presiding judge of the juvenile court under Welfare and Institutions Code section 827(a)(4). (Welf. & Inst. Code, § 831(d).) "Juvenile information" includes the "juvenile case file" as defined in Welfare and Institutions Code section 827(e), as well as information regarding the juvenile such as the juvenile's name, date or place of birth, and immigration status. (Welf. & Inst. Code, § 831(e).)

~~1.~~3. Dismissed petitions: The court must order sealed all records related to any petition dismissed under Welfare and Institutions Code section 786 that are in the custody of the juvenile court, law enforcement agencies, the probation department, and the Department of Justice. The procedures for sealing these records are stated in Welfare and Institutions Code section 786.

~~2.~~4. Records of adoption proceedings: Documents related to an adoption proceeding are not open to the public. Only the parties, their attorneys, and the Department of Social Services may review the records. The judge can authorize review by a requestor only in "exceptional circumstances and for good cause approaching the necessitous." (Fam. Code, § 9200, subd. (a).) Any party to the proceeding can petition the court to have redacted from the records, before copy or inspection by the public, the name of the birth parents and information tending to identify the birth parents. (Fam. Code, § 9200, subd. (b).)

~~3.~~5. Child custody evaluation reports: These reports must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officer, court employee or family court facilitator for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person upon order of the court for good cause. (Fam. Code, §§ 3025.5 and 3111.)

4.6. Child custody mediator recommendations: These recommendations must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officer, court employee or family court facilitator for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person upon order of the court for good cause. (Fam. Code, §§ 3025.5 and 3183.)

5.7. Written statements of issues and contentions by counsel appointed for child: These written statements must be kept in the confidential portion of the family law file and are available only to the court, the parties, their attorneys, federal or state law enforcement, judicial officers, court employees or family court facilitators for the county in which the action was filed (or employee or agent of facilitator), counsel for the child, and any other person, upon order of the court, for good cause. (Fam. Code, §§ 3025.5, 3151(b).)

6.8. Uniform Parentage Act documents: Records in Uniform Parentage Act proceedings, except the final judgment, are not open to the public. (Fam. Code, § 7643, subd. (a).) If a judge finds that a third party has shown good cause and finds exceptional circumstances, the court may grant that person access to the records. (*Ibid*.) This includes records from paternity actions.

7.9. Family conciliation court records: These records are confidential. The judge of the family conciliation court can grant permission for a party to review certain documents. (Fam. Code, § 1818, subd. (b).)

8.10. Proceeding to terminate parental rights: Documents related to such proceedings are confidential; only persons specified by law may review the records. (Fam. Code, § 7805.)

9.11. Support enforcement and child abduction records: Support enforcement and child abduction records are generally confidential; these records may be disclosed to persons specified by statute only under limited circumstances. In certain instances, the whereabouts of a party or a child must not be revealed to the other party or his or her attorneys. A local child support agency must redact such information from documents filed with the court. (Fam. Code, § 17212.)

10.12. Income tax returns in support cases: In a proceeding involving child, family, or spousal support, if a judge finds that a tax return is relevant to disposition of the case, the tax return must be sealed and maintained as a confidential record of the court. (Fam. Code, § 3552.)

Records that may be confidential

1. Sealed juvenile records: The court may order the records of a former ward of the court to be sealed. (Welf. & Inst. Code, § 781; Cal. Rules of Court, rule 5.830.) If the court so orders, all the records described in section 781 must be sealed. (See 10.3.2, "Sealed Records.")

Probate Case Records

Records that are confidential

1. *Confidential Guardian Screening Form* (form GC-212): This mandatory Judicial Council form regarding the proposed guardian is confidential. It is used by the court and by persons or agencies designated by the court to assist in determining whether a proposed guardian should be appointed. (Cal. Rules of Court, rule 7.1001(c).)
2. *Confidential Supplemental Information* (form GC-312). This form regarding the proposed conservatee is confidential. It shall be separate and distinct from the form for the petition. The form shall be made available only to parties, persons given notice of the petition who have requested this supplemental information, or who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, 1821(a).)
3. *Confidential Conservator Screening Form* (form GC-314): This mandatory Judicial Council form is confidential. (Cal. Rules of Court, rule 7.1050(c).)
4. Reports regarding proposed conservators or guardianship: An investigative report created pursuant to Probate Code section 1513 concerning a proposed guardianship is confidential and available only to parties served in the action or their attorneys (generally, parents, legal custodian of child). An investigative report created pursuant to Probate Code section 1826 regarding the proposed conservatee is confidential and available only to those persons specified by statute. Under the statute, the reports on proposed conservatees shall be made available only to parties, persons given notice of the petition who have requested the report, or who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the reports on guardianships and conservatorships exclusively to persons entitled thereto. (Prob. Code, §§ 1513, subd. (d) and 1826, subd. (n).)
5. Investigator's review reports in conservatorships: These reports are confidential. The information in the reports may be made available only to parties, persons identified in section 1851(b), persons given notice who have requested the report or appeared in the proceeding, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interests of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, §§ 1851, subd. (b) and (e).) Subdivision (b) provides for special restricted treatment of attachments containing medical information and confidential criminal information from California Law Enforcement Telecommunications System (CLETS). Although the attachments are not mentioned in (e), it is recommended, to be consistent with (b), that they be treated as confidential except to the conservator, conservatee, and their attorneys.
6. Certification of counsel of their qualifications (form GC-010) and certification of completion of continuing education (form GC-011): The forms state that they are "confidential for court use only." They are governed by rule 7.1101, which states only that the certifications must be submitted to the court but not lodged or filed in a case file. (Cal. Rules of Court, rule 7.1101.)

Protective Orders

Records that are confidential

1. *Confidential CLETS Information* **(**form~~s DV-260/CH-102/EA-102/JV-248/SV-102, and WV-102~~CLETS-0001): A Judicial Council form~~s have~~ has been developed for petitioners in protective order proceedings to use to submit information about themselves and the respondents to be entered through the CLETS into the California Restraining and Protective Order System (CARPOS), a statewide database used to enforce protective orders. ~~These~~ This form~~s are~~ is submitted to the courts by petitioners in many types of protective order proceedings, including proceedings to prevent domestic violence, civil harassment, elder and dependent adult abuse, private postsecondary school violence, and juvenile cases. The information on the forms is intended for the use of law enforcement. The form~~s are~~is confidential. Access to the information on the form~~s~~ is limited to authorized court personnel, law enforcement, and other personnel authorized by the California Department of Justice to transmit or receive CLETS information. The form~~s~~ must not be included in the court file. (Cal. Rules of Court, rule 1.51.)

Jury Information

Records that are confidential

1. Juror questionnaires of those jurors not called: The questionnaires of jurors not called to the jury box for voir dire are not open to the public. (*Copley Press, Inc. v. Superior Court* (1991) 228 Cal.App.3d 77, 87–88); but cf. *Bellas v. Superior Court of Alameda County* (2000) 85 Cal.App.4th 636, 645, fn.6 [suggesting a contrary rule].)
2. Sealed juror records in criminal courts: After the jury reaches a verdict in a criminal case, the court's record of personal juror identifying information (including names, addresses, and telephone numbers) must be sealed. (Code Civ. Proc., § 237(a)(2).) This is often accomplished by replacing juror names with numbers. Indeed, that is how appellate court records contain the relevant information while conforming to the requirements of Code of Civil Procedure section 237. The defendant or his or her counsel can petition the court for access to this information to aid in developing a motion for a new trial or for any other lawful purpose. (Code Civ. Proc., § 206(f).)

Records that may be confidential

1. Records of grand jury proceedings: These records are not open to the public unless an indictment is returned. If an indictment is returned, records of the grand jury proceeding are not open to the public until 10 days after a copy of the indictment has been delivered to the defendant or his or her attorney. (Pen. Code, § 938.1 (b); *Daily Journal Corp. v. Superior Court* (1999) 20 Cal.4th 1117, 1124–1135.) If there is a "reasonable likelihood" that release of all or part of the transcript would prejudice the accused's right to a fair trial, a judge may seal the records. (Pen. Code, §§ 938.1, 929; and see *Rosato v. Superior Court* (1975) 51 Cal.App.3d 190.) Notwithstanding the confidential status of a record, in civil grand juries, a judge may order disclosure of

certain evidentiary materials, as long as information identifying any person who provided information to the grand jury is removed. (Pen. Code, § 929.) Also, after an indictment is returned, the judge may order disclosure of nontestimonial portions of the grand jury proceedings to aid preparation of a motion to dismiss the indictment. (*People v. Superior Court (Mouchaourab)* (2000) 78 Cal.App.4th 403, 434–436.)

2. Courts' inherent power to protect jurors: Courts may exercise their discretion to seal juror records where a "compelling interest" exists, such as protecting jurors' safety or privacy, protecting litigants' rights, or protecting the public from injury. (*Pantos v. City and County of San Francisco* (1984) 151 Cal.App.3d 258, 262; Code of Civ. Proc., § 237; see also *Townsel v. Superior Court* (1999) 20 Cal.4th 1084, 1091).) Thus any juror information that a judge orders sealed is not open to the public.

10.3.2 Sealed Records

The rules on sealed records in the trial courts are contained in rules 2.550 and 2.251 of the California Rules of Court. The content and scope of the sealing is specified in the sealing order. The sealed records rules provide that the court's order should seal only those documents and pages, or if reasonably practical, portions of those documents and pages, that contain the materials that need to be placed under seal. All other portions of each document or page must be included in the public file. (Cal. Rules of Court, rule 2.550(e)).

Sealed records must be securely filed and kept separate from the public file in the case. (Cal. Rules of Court, rule 2.551(f).)

There are also a specific statute and rule on sealing juvenile records. (Welf. & Inst. Code, § 781; Cal. Rules of Court, rule 5.830.) These allow a former ward of the court to petition the court to order juvenile records sealed. If the petition is granted, the court must order the sealing of all records described in section 781. The order must apply in the county of the court hearing the petition and all other counties in which there are juvenile records concerning the petitioner. (Cal. Rules of Court, rule 5.830(a)(4).) All records sealed must be destroyed according to section 781(d).

10.4 Fees and Fee Waiver Guidelines for Requested Records

(The content for this section will be addressed in the next version of TCRM.)

10.5 Judicial Administrative Records

Judicial administrative records are not "court records," as defined in the Government Code. Administrative records are outside the scope of this manual. For those interested in administrative records of the courts, rule 10.500 of the California Rules of Court sets forth requirements for public access to judicial administrative records (e.g., nondeliberative, nonadjudicative records and information relating to the administration of the courts).

11. Retention, Preservation, and Destruction of Court Records

11.1 Retention, Preservation, and Destruction Practices

This section provides guidance for the retention, preservation, and destruction of court case records only. Courts are required by law to maintain listings of destroyed court records. This information should be readily available to the ~~Administrative Office of the Courts~~Judicial Council or the state archivist, upon request.

Records managers may systematically destroy records in accordance with statutes and rules enumerated in the "Schedule of Records Retention and Destruction and Special Case Type Characteristics," found in section 11.4. Courts are encouraged to include a records destruction process in their comprehensive records management program. Case records may be classified and segregated in accordance with retention requirements so that like records can be easily identified for purging when retention periods have elapsed.

Court records that are being destroyed may be either (1) recycled or (2) shredded and then recycled. All confidential records must be shredded prior to recycling. Because of environmental issues and the California Integrated Waste Management Act, recycling paper from court case records is highly recommended. Paper to be recycled should be maintained in a secure area until picked up by a recycling vendor.

Government Code section 68150(a) states that trial court records may be created, maintained, and preserved in any form or forms of communication or representation, including paper, optical, electronic, magnetic, micrographic, or photographic media or other technology. As authorized in Government Code section 68152, the clerk of the court may destroy court records pursuant to Government Code section 68153 following notice of destruction and no request and order for transfer of the records.

The five conditions for the destruction of records required by Government Code section 68152 and 68153 are as follows:

1. The applicable retention time has expired (Gov. Code, § 68152).
2. After (there must be) final disposition of the case (defined in Gov. Code, § 68151) (Gov. Code, § 68152).
3. Notice of destruction (intention) has been given (Gov. Code, § 68152).
4. There is no request and order for transfer of the records (Gov. Code, § 68152).
5. The records are destroyed on the order of the presiding judge of the court (required by Gov. Code, § 68153).

Copies of the notice of intent to destroy records and the notice of hearing when a record entity requests transfer of records to its possession include the following:

1. Notice of Intent to Destroy Superior Court Records (form REC-001(N))
2. Offer to Transfer Possession (form REC-001(N))
3. Notice of Hearing on Request for Transfer or Extension of Time for Retention of Superior Court Records (form REC-001(R))
4. Notice of Hearing on Request for Transfer or Extension of Time for Retention of Superior Court Records; Court Order; Release and Receipt of Superior Court Records (form REC-002(N))
5. Release and Receipt of Superior Court Record (form REC-002(R))

Once records have been destroyed or transferred, the court is required to file a notice with the Judicial Council, apprising the council of this action. The notification is made on the following form:

1. Report to the Judicial Council: Superior Court Records Destroyed, Preserved and Transferred (form REC-003)

11.1.1 Court Records Sampling Program

The Judicial Council has adopted the superior court records sampling program (Cal. Rules of Court, rule 10.855) to ensure the preservation of records in the trial courts. This legislatively mandated action concerns all superior court records filed before 1911 and a sample of superior court records filed after December 31, 1910.

Superior court records, as used in this context, do not include records of limited civil, small claims, misdemeanor, or infraction cases.

Sampling Technique

Three superior courts are assigned in rotation by the Judicial Council to preserve 100 percent of their court records for a calendar year. This is called a "longitudinal sample." (Cal. Rules of Court, rule 10.855(f).) The schedule of the comprehensive sampling program is included in the Appendix to the TCRM.

All other courts are required to preserve a "systematic sample" of 10 percent or more of each year's court records scheduled to be destroyed. (Cal. Rules of Court, rule 10.855(f).) If fewer than 100 cases of a filing year are scheduled to be destroyed, all of the cases must be preserved. (Cal. Rules of Court, rule 10.855(f)(1)(c).)

Courts must also preserve a 2 percent "subjective sample" of court records scheduled to be destroyed (but not fewer than the court records for 20 cases). This "subjective sample" must include

- All cases accepted for review by the California Supreme Court;
- "Fat files" or the thickest perceived case files; and
- Cases deemed by the court to be of local, national, or international significance.

These cases must be identified by stamp or mark to distinguish them from the systematic sample. (Cal. Rules of Court, rule 10.855(f)(2).)

Reporting Requirement

Under rule 10.855*(l)* of the California Rules of Court, superior courts are required to provide semiannually to the Judicial Council a list by year of filing of court records destroyed, filing and location of the court records of the comprehensive and sample court records preserved, and filing and location of the court records transferred to entities under rule 10.856 of the California Rules of Court. The council adopted form REC-003, *Report to the Judicial Council: Superior Court Records Destroyed, Preserved, and Transferred*, effective January 1, 2007, to implement the reporting requirements.

Notice Requirement

Under rule 10.856(b) of the California Rules of Court, superior courts are required to give 30 days' written notice of intent to destroy court records open to public inspection. The notice is sent to entities maintained on the council's master list and to others who directly requested notification.

Records Management Clearinghouse

As a result of the actions outlined above, a Records Management Clearinghouse was established to receive superior court records disposition reports required under legislation and council rule; keep courts informed of their responsibilities under the records management statutes and rules; serve as a referral center for historians and researchers seeking to study court records in superior courts; and respond to questions on the standards, rules, reporting forms, and new records management legislation. The address for the Records Management Clearinghouse is

Records Management Clearinghouse
c/o ~~Administrative Office of the Courts~~Judicial Council of California
Legal Services ~~Office~~
455 Golden Gate Avenue
San Francisco, CA 94102-3688

11.2 Inactive Records Storage

By definition and design, an active filing system will lead to a continuous movement of records from active to inactive filing systems or records storage areas. Records are subject to much less activity in an inactive records storage area than in an active filing system, but records are still being added, individual records continue to be accessed periodically, and records may be moved out for destruction or transferred to another location, such as an archive.

The purpose of inactive records storage is simply to move inactive or closed case records from prime filing system space to lower-cost space where records may be more densely packed with the understanding that they are accessed with decreasing frequency as they become older. An inactive system may be expanded as the need arises. The records retention and destruction schedule is the primary tool used to manage the inventory of inactive records. It identifies records that can be destroyed and those that must be retained.

11.3 Cases Accepted for Review by the Supreme Court

Pursuant to rule 10.855 of the California Rules of Court, case records accepted for review by the California Supreme Court must be retained in a trial court's records sampling program. Each year, the ~~AOC~~ Judicial Council places a list of such cases on the Serranus Web site at http://serranus.courtinfo.ca.gov/programs/courtrec/.

It is the responsibility of every court to check the list annually and flag the cases that, as a result of Supreme Court review, must be permanently retained in the sampling program.

11.4 Schedule of Records Retention and Destruction and Special Case Type Characteristics

11.4.1 Records Retention and Destruction Schedule under Government Code Sections 68152 and 68153

Government Code sections 68152 and 68153 authorize the retention periods and destruction of court records. The new and amended record retention and destruction periods provided in this section became effective January 1, 2014 and apply to all court records in existence. The chart below provides listings of the various types of records, grouped into major case categories.

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
CIVIL ACTIONS AND PROCEEDINGS			
(1)	Civil actions and proceedings, except as otherwise specified	Retain 10 years.	
(2)	Civil unlimited cases, limited cases, small claims cases, including after trial de novo, if any, except as otherwise specified	Retain 10 years.	
(3)	Civil judgments for unlimited civil cases	Retain permanently.	
(4)	Civil judgments for limited and small claims	Retain 10 years, unless judgment is renewed. If judgment is renewed, retain judgment for length of renewal pursuant to Article 2 (commencing with Section 683.110) of Chapter 3 of Division 1 of Title 9 of Part 2 of the Code of Civil Procedure.	
(5)	If a party in civil case appears by a guardian ad litem	Retain 10 years after termination of the court's jurisdiction.	
(6)	Civil harassment, domestic violence, elder and	Retain same period of time as the duration	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
	dependent adult abuse, private postsecondary school violence, and workplace violence cases	of the restraining or other orders and any renewal thereof, then retain the restraining or other orders permanently as a judgment. Retain 60 days after expiration of the temporary restraining or other temporary order. Retain permanently judgments establishing paternity under Section 6323 of the Family Code.	
(7)	Family law, except as otherwise specified	Retain 30 years.	
(8)	Adoption	Retain permanently.	Confidential pursuant to Family Code section 9200–9209 — Parties to the action or the attorney of record may view the court file. Family Code section 9200(c) states upon the request of the adoptive parents or the child a clerk of the court can issue a certificate of adoption, provided the birth parents' names are omitted, unless a stepparent adoption.
(9)	Parentage	Retain permanently.	Family Code section 7643, subd. (a) Records in Uniform Parentage Act proceedings, except the final judgment is not open to the public. Pursuant to Family Code section 7643(b) parties to the action, attorneys of record, or upon written consent as defined can inspect the court file.

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
(10)	Change of name, gender, or name and gender	Retain permanently.	
(11)	Probate		
	(A) Decedent estates	Retain permanently all orders, judgments, and decrees of the court, all inventories and appraisals, and all wills and codicils of the decedent filed in the case, including those not admitted to probate. All other records retain for 5 years after final disposition of the estate proceeding.	
	(B) Wills and codicils		
	(i) Wills and codicils transferred or delivered to the court pursuant to Section 732, 734, or 8203 of the Probate Code:	Retain permanently.	
	(ii) Wills and codicils delivered to the clerk of the court under Section 8200 of the Probate Code	Retain the original documents as provided in Section 26810 of the Government Code.	
	(C) Substitutes for decedent estate administration		
	(i) Affidavit procedures for real property of small value under Chapter 3 (commencing with Section 13100) of Part 1 of Division 8 of the Probate Code	Retain permanently.	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
	(ii) Proceedings for determining succession to property under Chapter 4 (commencing with Section 13150) of Part 1 of Division 8 of the Probate Code	Retain permanently all inventories and appraisals and court orders. Other records retain for 5 years after final disposition of the proceeding.	
	(iii) Proceedings for determination of property passing or belonging to surviving spouse under Chapter 5 (commencing with Section 13650) of Part 2 of Division 8 of the Probate Code	Retain permanently all inventories and appraisals and court order. Other records retain for 5 years after final disposition of the proceeding.	
	(D) Conservatorships	Retain permanently all court orders. Retain documents of trusts established under substituted judgment pursuant to Section 2580 of the Probate Code as provided in clause (iii) of subparagraph (11)(G) of Section 68152 of the Government Code. Other records retain for 5 years after the later of either (1) the final disposition of the conservatorship proceeding, or (2) the date of the conservatee's death, if that date is disclosed in the court's file.	
	(E) Guardianships	Retain permanently orders terminating the guardianship, if any, and court orders settling final account and ordering distribution of the estate. Other records retain for 5 years after the later of (1) the	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
		final disposition of the guardianship proceeding, or (2) the earlier of the date of the ward's death, if that date is disclosed in the court's file, or the date the ward reaches 23 years of age.	
	(F) Compromise of minor's or disabled person's claim or action, and disposition of judgment for minors and disabled persons under Section 372 of the Code of Civil Procedure and Chapter 4 (commencing with Section 3600) of Part 8 of Division 4 of the Probate Code		
	(i) Judgments in favor of minors or disabled persons, orders approving compromises of claims and actions and disposition of the proceeds of judgments, orders directing payment of expenses, costs, and fees, orders directing deposits into blocked accounts and receipts and acknowledgments of those orders, and orders for the withdrawal of funds from blocked accounts.	Retain permanently	
	(ii) Other records.	Retain for the same retention period as for records in the underlying case. If there is no underlying case, retain for 5 years after the later of either (1) the date the order for	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
		payment or delivery of the final balance of the money or property is entered, or (2) the earlier of the date of the minor's death, if that date is disclosed in the court's file, or the date the minor reaches 23 years of age.	
	(G) Trusts		
	(i) Proceedings under Part 5 (commencing with Section 17000) of Division 9 of the Probate Code	Retain permanently.	
	(ii) Trusts created by substituted judgment under Section 2580 of the Probate Code	Retain permanently all trust instruments and court orders. Other records retain as long as the underlying conservatorship file is retained.	
	(iii) Special needs trusts	Retain permanently all trust instruments and court orders. Other records retain until the later of either (1) the retention date of "other records" in the beneficiary's conservatorship or guardianship file under subparagraph (11)(D) or (E) of Section 68152 of the Government Code, if any, or (2) 5 years after the date of the beneficiary's death, if that date is disclosed in the court's file.	
	(H) All other proceedings under the Probate Code	Retain as provided for civil cases.	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
(12)	Mental Health (A) Lanterman Developmental Disabilities Services Act (B) Lanterman-Petris-Short Act (C) Riese (capacity) hearings under Sections 5333 and 5334 of the Welfare and Institutions Code (D) Petitions under Chapter 3 (commencing with Section 8100) of Division 8 of the Welfare and Institutions Code for the return of firearms to petitioners who relinquished them to law enforcement while detained in a mental health facility	 Retain 10 years. Retain 20 years. Retain for the later of either (1) 20 years after the date of the capacity determination order, or (2) the court records retention date of the underlying involuntary treatment or commitment proceeding, if any. Retain 10 years.	
(13)	Eminent domain	Retain permanently.	
(14)	Real property other than unlawful detainer	Retain permanently if the action affects title or an interest in real property.	
(15)	Unlawful detainer	Retain for 1 year if judgment is only for possession of the premises. Retain for 10 years if judgment is for money, or money and possession.	Confidential pursuant to Code of Civil Procedure section 1161.2(a)(1-4) —The following are allowed to view the court file: parties to the action, the attorneys for the parties, any person who provides the clerk with the names of at least one plaintiff and one defendant and the address of the

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
			premises, including the apartment number or unit, if any. A resident of the premises who provides the clerk with the name of one of the parties or the case number and shows proof of residency.
	Any civil or small claims case in the trial courts (1) Involuntarily dismissed by the court for delay in prosecution or failure to comply with state or local rules (2) Voluntary dismissed by a party without entry of judgment	 Retain 1 year. Retain 1 year.	
CRIMINAL ACTIONS AND PROCEEDINGS			
(1)	Capital felony in which the defendant is sentenced to death, and any felony resulting in a sentence of life or life without the possibility of parole "Capital felony" means murder with special circumstances when the prosecution seeks the death penalty. Records of the cases of codefendants and related cases required to be retained shall be limited to those cases that are factually linked or related to the charged offense, that are identified in the courtroom, and that are placed on the record.	Retain permanently, including records of the cases of any codefendants and any related cases, regardless of the disposition. If a capital felony is disposed of by a sentence less than death, or imprisonment for life or life without the possibility of parole, the judgment shall be retained permanently, and the record shall be retained for 50 years or for 10 years after the official written notification of the death of the defendant. If a capital felony is disposed of by an	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
		acquittal, the record shall be retained for 10 years.	
(2)	Felony, except as otherwise specified, and in any felony or misdemeanor case resulting in a requirement that the defendant register as a sex offender under Section 290 of the Penal Code	Retain judgment permanently. For all other documents: retain for 50 years or the maximum term of the sentence, whichever is longer. However, any record other than the judgment may be destroyed 10 years after the death of the defendant. Felony case files that do not include final sentencing or other final disposition because the case was bound over from a former municipal court to the superior court and not already consolidated with the superior court felony case file, retain for 10 years from the disposition of the superior court case.	
(3)	Felony reduced to a misdemeanor	Retain in accordance with the retention period for the relevant misdemeanor.	
(4)	Felony, if the charge is dismissed, except under Section 1203.4 or 1203.4a of the Penal Code	Retain 3 years.	
(5)	Misdemeanor, if the charge is dismissed, except under Section 1203.4 or 1203.4a of the Penal Code	Retain 1 year.	
(6)	Dismissal under Section 1203.4 or 1203.4a of the Penal Code	Retain for the same retention period as for records of the underlying case. If the	This retention period applies to expungement petitions under Penal Code

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
		records in the underlying case have been destroyed, retain for 5years after dismissal.	sections 1203.4 and 1203.4a.
(7)	Misdemeanor, except as otherwise specified For misdemeanors alleging a violation of Section 23109, 23109.5, 23152, or 23153 of the Vehicle Code	Retain 5 years. Retain 10 years.	
(8)	Misdemeanor alleging a marijuana violation under subdivision (c), (d), or (e) of Section 11357 of the Health and Safety Code, or subdivision (b) of Section 11360 of the Health and Safety Code	Records shall be destroyed, or redacted in accordance with subdivision (c) of Section 11361.5 of the Health and Safety Code, 2 years from the date of conviction, or from the date of arrest if no conviction, if the case is no longer subject to review on appeal, all applicable fines and fees have been paid, and the defendant has complied with all terms and conditions of the sentence or grant of probation. However, as provided in subdivision (a) of Section 11361.5 of the Health and Safety Code and subdivision (e)(5) of Section 68152 of the Government Code, records of a misdemeanor alleging a marijuana violation under subdivision (e) of Section 11357 of the Health and Safety Code shall be retained until the offender attains 18 years of age, at which time the records shall be destroyed as provided in subdivision (c) of Section 11361.5 of the	The requirements of section 11361.5 do not apply to the destruction of records of a conviction that remains subject to review on appeal; to a conviction that is the basis of (1) a term of imprisonment that has not been fully served, (2) a fine that has not been wholly paid, or (3) periods or conditions of parole or probation that have not been satisfactorily completed; or the destruction of records of an arrest while the underlying charges remain outstanding. (*Younger v. Superior Court* (1978) 21 Cal.3d 102, 111–114.)

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
		Health and Safety Code.	
(9)	Misdemeanor reduced to an infraction	Retain in accordance with the retention period for the relevant infraction.	
(10)	Infraction, except as otherwise specified Vehicle Code infraction Infraction alleging a marijuana violation under subdivision (b) of Section 11357 of the Health and Safety Code	Retain for 1 year. Retain for 3 years. If records are retained past the 1 year minimum retention period, the records shall be destroyed or redacted in accordance with subdivision (c) of Section 11361.5 of the Health and Safety Code 2 years from the date of conviction, or from the date of arrest if no conviction, if the case is no longer subject to review on appeal, all applicable fines and fees have been paid, and the defendant has complied with all terms and conditions of the sentence or grant of probation.	The requirements of section 11361.5 do not apply to the destruction of records of a conviction that remains subject to review on appeal; to a conviction that is the basis of (1) a term of imprisonment that has not been fully served, (2) a fine that has not been wholly paid, or (3) periods or conditions of parole or probation that have not been satisfactorily completed; or the destruction of records of an arrest while the underlying charges remain outstanding. (*Younger v. Superior Court* (1978) 21 Cal.3d 102, 111–114.)
(11)	Criminal protective order	Retain until the order expires or is terminated.	
(12)	Arrest warrant	Retain for the same retention period as for records in the underlying case. If there is no underlying case, retain for 1 year from the date of issue.	Penal Code section 168 provides punishment for willful disclosure by the district attorney, clerk, judge, or peace officer prior to execution of warrant.
(13)	Search warrant	If there is any underlying case, retain for 10	Confidential pursuant to Penal Code section

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
		years from the date of issue or, if the retention period for records in the underlying case is less than 10 years or if the underlying case is a capital felony described in subdivision (c)(1) of Section 68152 of the Government Code, retain for the same retention period as for records in the underlying case. If there is no underlying case, retain for 5 years from the date of issue.	1524 (d)(1)—Information can be only divulged upon direct inquiry by the court. Penal Code section 168 provides punishment for willful disclosure by the district attorney, clerk, judge, or peace officer prior to execution of warrant.
(14)	Probable cause declarations	Retain for the same retention period as for records in the underlying case. If there is no underlying case, retain for one year from the date of declaration.	Penal Code section 168 provides punishment for willful disclosure by the district attorney, clerk, judge, or peace officer prior to execution of warrant.
(15)	Proceedings for revocation of postrelease community supervision or postrelease parole supervision	Retain for five years after the period of supervision expires or is terminated.	
HABEAS CORPUS			
(1)	Habeas corpus in criminal and family law matters	Retain for the same retention period as for records in the underlying case, whether granted or denied.	
(2)	Habeas corpus in mental health matters	Retain all records for the same retention period as for records in the underlying case, whether granted or denied.	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
		If there is no underlying case, retain records for 20 years.	
JUVENILES			
(1)	Dependent pursuant to Section 300 of the Welfare and Institutions Code	Upon reaching 28 years of age, or on written request, shall be released to the juvenile five years after jurisdiction over the person has terminated under subdivision (a) of Section 826 of the Welfare and Institutions Code. Sealed records shall be destroyed upon court order five years after the records have been sealed pursuant to subdivision (c) of Section 389 of the Welfare and Institutions Code.	Confidential pursuant to California Rules of Court, rule 5.552, and Welfare and Institution Code section 827 (a)(1)(A –P) —The parents or guardian of the minor, the minor, attorneys to the action, child protective agencies, social service agencies as defined, local child support agencies as defined, school superintendent as defined, authorized legal staff or special investigators as defined, are allowed to view the court file. Refer to Welfare & Institution Code, section 827, for details regarding access to these records.
(2)	Ward pursuant to Section 601 of the Welfare and Institutions Code	Upon reaching 21 years of age, or on written request, shall be released to the juvenile five years after jurisdiction over the person has terminated under subdivision (a) of Section 826 of the Welfare and Institutions Code. Sealed records shall be destroyed upon court order five years after the records have been sealed under subdivision (d) of Section 781 of the Welfare and Institutions Code.	Confidential pursuant to California Rules of Court, rule 5.552, and Welfare and Institution Code, section 827 (a)(1)(A – P)—The parents or guardian of the minor, the minor, attorneys to the action, child protective agencies, social service agencies as defined, local child support agencies as defined, school superintendent as defined, authorized legal staff or special investigators as defined, are allowed to view the court file. Refer to Welfare and Institution Code, section 827, for details

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
			regarding access to these records.
(3)	Ward pursuant to Section 602 of the Welfare and Institutions Code	Upon reaching 38 years of age under subdivision (a) of Section 826 of the Welfare and Institutions Code. Sealed records shall be destroyed upon court order when the subject of the record reaches 38 years of age under subdivision (d) of Section 781 of the Welfare and Institutions Code.	Confidential pursuant to California Rules of Court, rule 5.552, and Welfare and Institution Code, section 827 (a)(1)(A – P)—The parents or guardian of the minor, the minor, attorneys to the action, child protective agencies, social service agencies as defined, local child support agencies as defined, school superintendent as defined, authorized legal staff or special investigators as defined, are allowed to view the court file. Refer to Welfare and Institution Code, section 827, for details regarding access to these records.
(4)	Traffic and some nontraffic misdemeanors and infractions pursuant to Section 601 of the Welfare and Institutions Code	Upon reaching 21 years of age, or five years after jurisdiction over the person has terminated under subdivision (c) of Section 826 of the Welfare and Institutions Code. Records may be microfilmed or photocopied.	
(5)	Marijuana misdemeanor under subdivision (e) of Section 11357 of the Health and Safety Code in accordance with procedures specified in subdivision (a) of Section 11361.5 of the Health and Safety Code	Upon reaching 18 years of age, the records shall be destroyed.	
COURT RECORDS OF THE APPELLATE DIVISION OF THE SUPERIOR COURT			
	Court records of the appellate division of the	Retain 5 years.	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
	superior court		
OTHER TRIAL COURT RECORDS			
(1)	Bench warrant Bench warrant issued for a misdemeanor	Retain for the same retention period as for records in the underlying case. Retain records for the same retention period as for records in the underlying misdemeanor following issuance. If there is no return on the warrant, court may dismiss on its own motion and immediately destroy the records.	
(2)	Body attachment	Retain for same retention period as for records in the underlying case.	
(3)	Bond	Retain for 3 years after exoneration and release.	
(4)	Court reporter notes (A) Criminal and juvenile proceedings	Retain notes for 10 years, except as otherwise specified. Notes reporting proceedings in capital felony cases (murder with special circumstances when the prosecution seeks the death penalty and the sentence is death), including notes reporting the preliminary hearing, shall be retained permanently, unless the Supreme Court on request of the court clerk authorizes the destruction.	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
	(B) Civil and all other proceedings	Retain notes for 5 years.	
(5)	Electronic recordings made as the official record of the oral proceedings under the California Rules of Court		
	(A) Infraction and misdemeanor proceedings	May be destroyed or deleted any time after final disposition of the case.	
	(B) Criminal proceedings	May be destroyed or deleted after 10 years.	
	(C) All other proceedings	May be destroyed or deleted after 5 years.	
(6)	Electronic recordings not made as the official record of the oral proceedings under the California Rules of Court	May be destroyed at any time at the discretion of the court.	
(7)	Fee waiver applications	Retain for the same retention period as for records in the underlying case.	
(8)	Judgments within the jurisdiction of the superior court other than in a limited civil case, misdemeanor case, or infraction case	Retain permanently.	
(9)	Judgments in misdemeanor cases, infraction cases, and limited civil cases	Retain for the same retention period as for records in the underlying case.	
(10)	Juror proceedings, including sanctions	Retain 1 year.	
(11)	Minutes	Retain for the same retention period as for records in the underlying case.	
(12)	Orders not associated with an underlying case,	Retain 1 year.	

	CASE TYPE	NEW MINIMUM RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS/REFERENCES/NOTES
	such as orders for the destruction of court records for telephone taps, orders to destroy drugs, and other miscellaneous court orders		
(13)	Naturalization index	Retain permanently.	
(14)	Index for cases alleging traffic violations	Retain for the same retention period as for records in the underlying case.	
(15)	Index, except as otherwise specified	Retain permanently.	
(16)	Register of actions or docket	Retain for the same retention period as for records in the underlying case, but in no event less than 10 years for civil and small claims cases.	

11.4.2 Records Retention and Destruction Schedule for Other Case Types

This section includes case types that are not contained in Government Code section 68152. Accordingly, there is no statutory or rule guidance on the retention and destruction of these case types. Below are recommended retention periods, derived from retention periods of similar or closely related case types that are described in Government Code section 68152.

CASE TYPE	RECOMMENDED RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS
Disclosure of juvenile records (Sections 827 and 828 of the Welfare and Institutions Code)	Same retention period as the disclosed documents. See Government Code, section 68152(g), for juvenile record retention times.	Confidential pursuant to California Rules of Court, rule 5.552(c–f), and Welfare and Institutions Code, sections 827 and 828 as defined—Upon a showing of good cause and court order may allow the petitioning party all or limited dissemination of the juvenile court file or information retained by law enforcement agency.
Mental health petition (Section 5275 of the Welfare and Institutions Code)	Retain 30 years	Confidential pursuant to Welfare and Institutions Code section 5328.15 as defined; in summary the Judicial Officer and the parties to the action are allowed to view the court file.
Riese Hearings (Section 5332 of the Welfare and Institutions Code)	Retain 30 years	Confidential pursuant to Welfare and Institutions Code section 5328.15 as defined; in summary the Judicial Officer and the parties to the action are allowed to view the court file.
Terminate Parental Rights	Retain 30 years	Confidential pursuant to Family Code section 7805—The child who is subject of the proceeding, the parents or guardian of the child, attorneys for the parties, and any other person designated by the judge are allowed to view the court file.
Subpoenaed Records (EC 1560(d))	Unless admitted as evidence or required as part of the record: (1) Original subpoenaed records should be returned to the custodian of records at the conclusion of trial/hearing; or (2) copies of subpoenaed records should be destroyed at the conclusion of trial/hearing.	

11.4.3 Records Retention and Destruction Schedule for Prefiled and Juror Records

This section includes case types that are not contained in Government Code section 68152. Accordingly, there is no statutory or rule guidance on the retention and destruction of these case types.

CASE TYPE	RECOMMENDED RETENTION PERIOD	SPECIAL CASE TYPE CHARACTERISTICS
Grand Jury Indictments under Penal Code sections 889 and 940	Same period as period for retention of the records in the underlying case category.	Confidential pursuant to Penal Code section 939 as defined—See persons to be permitted during sessions. Penal Code section 939.1 as defined—Public sessions on request under court order.
Jury Questionnaire under Code of Civil Procedure 205(c–d)	Same period as period for retention of the records in the underlying case category.	Jury questionnaires are public information. Except as provided in section 10.3.1, "Confidential Records, Jury Information."
Probation Reports under California Rules of Court, rule 4.411, et seq. and Penal Code section 1203, et seq.	Same period as period for retention of the records in the underlying case category.	Penal Code section 1203.05 as defined, public from date of judgment or probation granted for 60 days; by district attorney or defendant at any time; or by court order after 60 days.
Qualification of Jurors under Code of Civil Procedure sections 203 and 198	Same period as period for retention of the records in the underlying case category.	Code of Civil Procedure section 237 as defined names of qualified jurors are public information upon request. Code of Civil Procedure section 237 (2) as defined, juror personal indentifying information is sealed.
Wire Taps under Penal Code section 629.50	Mandatory 10 years minimum.	Confidential pursuant to Penal Code section 629.66—Applications and orders granted shall be sealed by the judge and shall be disclosed only upon a showing of good cause before a judge.

Appendices

APPENDIX 1—COURT RECORDS DESIGNATED CONFIDENTIAL BY STATUTE OR RULE

	GENERAL		
1	Information that must be excluded from court calendars, indexes, and registers of actions	Cal. Rules of Court, rule 2.507(c)	"The following information must be excluded from a court's electronic calendar, index, and register of actions: (1) Social security number; (2) Any financial information; (3) Arrest warrant information; (4) Search warrant information; (5) Victim information; (6) Witness information; (7) Ethnicity; (8) Age; (9) Gender; (10) Government-issued identification card numbers (i.e., military); (11) Driver's license number; and (12) Date of birth."
2	Subpoenaed Records (EC 1560(d))	Evidence Code Section 1560 (d).	Unless the parties to the proceeding otherwise agree, or unless the sealed envelope or wrapper is returned to a witness who is to appear personally, the copy of the records shall remain sealed and shall be opened only at the time of trial, deposition, or upon direction of the judge.
14	Special Immigrant Juvenile Findings	Code Civ. Proc, § 155(c)	If not otherwise protected by state confidentiality laws, information regarding the child's immigration status must remain confidential and must be available for inspection only by the court, the child who is the subject of the proceeding, the parties, the attorneys for the parties, the child's counsel, and the child's guardian.
	CIVIL LAW		
1	Request for accommodations by persons with disabilities	Cal. Rules of Court, rule 1.100(c)(4)	"The court must keep confidential all information of the applicant concerning the request for accommodation"; this includes the identity of the applicant, all medical information, and all communications from the applicant.
2	Application to proceed *in forma pauperis* (aka application for waiver of fees and costs)	Cal. Rules of Court, rule 3.54	Access to the application and to the information in the application is limited to court and authorized persons only.
3	Documents filed under seal (per court order)	Cal. Rules of Court, rule 2.550	A sealed record is a record that by court order is not open to inspection by the public.
4	Documents that are the subject of a motion to seal	Cal. Rules of Court, rule 2.551(b)	A party requesting that a record be filed under seal must lodge it with the court. Pending the court's ruling, the lodged record will be conditionally under seal. In addition, unredacted memoranda and other documents filed in support of and opposition to the motion must be lodged, conditionally under seal, with redacted versions filed publicly.

5	Confidential documents that may be the subject of a motion to seal	Cal. Rules of Court, rule 2.551(b)	A party that intends to file documents that are subject to a confidentiality agreement or protective order, but does not intend to request that they be filed under seal, must lodge the records, as well as any pleadings or other documents that disclose the contents of the records, with the court. Redacted versions of those documents are filed publicly. Unredacted records are lodged, with notice to parties that the records will be placed in the court file unless a motion to seal is filed and granted. The documents are conditionally under seal for 10 days. If a party moves to seal the documents within that period, or longer if extended by the court, the documents remain conditionally under seal pending the court's ruling on the motion.
6	Records examined by the court in confidence during a confidential *in-camera* proceeding in which a party is excluded	Cal. Rules of Court, rule 2.585	Such records must be filed under seal and must not be disclosed without court order.
7	Records in unlawful detainer actions	Code Civ. Proc., § 1161.2 (a)	For 60 days after the complaint has been filed, access is limited to specific enumerated persons set forth in the statute, including parties and residents of the property. If the defendant prevails in the action within 60 days of the filing of the complaint, access is permanently limited to those specific enumerated persons. An exception excludes records of mobilehome park tenancies from this code section; those records are not confidential. In addition, effective January 1, 2011, access to court records is permanently limited to those specified enumerated persons in unlawful detainer cases involving residential property based on section 1161a (holding over after sale under execution, mortgage, or trust deed [foreclosures]) as indicated in the caption of the complaint, unless judgment has been entered, after a trial, for the plaintiff and against all defendants.
8	Records of actions brought under False Claims Act (aka *qui tam* actions)	Gov't. Code, § 12652(c)(2); Cal. Rules of Court, rule 2.570	A complaint that is filed by a private person is automatically filed under seal (no sealing order required) for 60 days, longer if extended by the court. During that period, all records in the action are filed under seal and are confidential until the seal is lifted. Access to sealed records is limited to specifically enumerated parties.
9	All information regarding complaints about the conduct of mediators in court-connected mediation programs	Cal. Rules of Court, rule 3.867	All communications, inquiries, complaints, investigations, procedures, deliberations, and decisions about the conduct of a mediator under rule 3.865 must occur in private and must be kept confidential. The presiding judge or a person designated by the presiding judge for this purpose may, at his or her discretion, authorize the disclosure of information or records concerning rule 3.865 complaint procedures that do not reveal any mediation communications.
10	Confidential name change because of domestic violence, stalking, or sexual assault	Code Civ. Proc., § 1277; Gov't Code § 6205 et seq.	The Secretary of State shall keep confidential name changes because of domestic violence, stalking, or sexual assault. Petitions for change of name because of domestic violence, stalking, or sexual assault shall, in lieu of reciting the proposed name, state that the proposed name is confidential and will be on file with the Secretary of State.
11	All certificates of corroborative fact filed in a civil action based on childhood sexual abuse	Code Civ. Proc., § 340.1(p)	Confidential from the public *and all parties* (except the plaintiff).
12	Social security numbers	Cal. Rules of Court,	Rule of court 2.507(c) requires that SSNs, along with other personal data, be excluded from any

	(SSNs)	rule 2.507(c)(1); see also Gov't Code, § 68107	electronic court calendar, index, or register of action. (See the criminal law section below for list of all categories of data to be excluded.) Section 68107 of the Government Code specifically addresses court collection efforts in criminal cases but does state that an SSN obtained for that purpose "is not a public record and shall not be disclosed except for collection purposes."
13	Records in an action in which prejudgment attachment is sought	Code Civ. Proc., § 482.050; Cal. Rules of Court, rule 2.580	Upon request by the plaintiff at the time the complaint is filed, the clerk of the court shall not make the records in the action or the fact of the filing of the action available to the public for as long as 30 days, or sooner upon the filing of the return of service of the notice of hearing and any temporary protective order or writ of attachment. Notwithstanding the above, the clerk shall make the entire file available to any named party or his or her attorney.
	CRIMINAL		
1	Sealed juror identification information	Pen. Code, § 95.2	This section makes it a misdemeanor for any person, without court authorization and juror consent, to intentionally provide a defendant juror identification information sealed by the court under Code of Civil Procedure § 237, where that information is in turn used to commit certain crimes.
2	Criminal juror identifying information	Code Civ. Proc., § 237	Upon the recording of a jury's verdict in a criminal jury proceeding, the court's record of personal juror identifying information of trial jurors shall be sealed until further order of the court. Please see criminal section (below) for further details.
3	Sex offense victim address information	Pen. Code, § 293	Allows victims of sex offenses to request that their names remain private and prohibits disclosure of their address information (with enumerated exceptions).
4	All records containing the identity of an alleged sex offense victim	Pen. Code, § 293.5	The court, at the request of the alleged victim, may order the identity of the alleged victim in all records and during all proceedings to be either Jane Doe or John Doe, if the court finds that such an order is reasonably necessary to protect the privacy of the person and will not unduly prejudice the prosecution or the defense.
5	Obscene matter	Pen. Code, § 312	When a conviction becomes final, the court may order any obscene matter or advertisement in its possession or under its control to be destroyed.
6	Two specific records involving victims of identity theft: (1) The police report generated on behalf of the victim under Pen. Code, § 530.6; and (2) The victim's written request for records regarding the unauthorized use of the victim's identity made upon the person or entity in possession of the records	Pen. Code, § 530.8(d)(1)	The aforementioned documents "shall be kept confidential by the court" pending the victim's petition to receive information pertaining to the unauthorized use of his or her identity.
7	Applications and orders	Pen. Code, § 629.66	Applications and orders for wiretaps "shall be sealed by the judge" and "shall be disclosed only

	regarding wiretaps		upon a showing of good cause before a judge."
8	Peace or custodial officer personnel records	Pen. Code, § 832.7	Peace officer and/or custodial officer personnel records, and records maintained by any state or local agency, or information obtained from these records, are confidential and shall not be disclosed in any criminal or civil proceeding except by discovery pursuant to Evidence Code sections 1043 and 1046.
9	Records of juvenile arrests for misdemeanors	Pen. Code, § 851.7	Any person previously arrested for a misdemeanor while a minor may petition the court for an order sealing the records in the case, including any records of arrest and detention.
10	Records of arrest	Pen. Code, § 851.8	This section sets forth various provisions for sealing and destroying the arrest records of persons subsequently deemed "factually innocent."
11	Criminal case records following acquittal	Pen. Code, § 851.85	A judge presiding at a trial resulting in an acquittal may order that the records in the case be sealed, including any record of arrest or detention, whenever it appears to the judge that the defendant was "factually innocent."
12	Arrest records and related court files and records, including court indexes and registers of actions	Pen. Code, § 851.90	Whenever a case is dismissed following a defendant's successful completion of drug diversion under Penal Code section 1000 et seq., the court may, in the interest of justice, seal the records of the arresting agency and related court files and records, including any record of arrest or detention. If the order is made, the clerk of the court shall thereafter not allow access to any records concerning the case, including the court file, index, register of actions, or other similar records.
13	Grand jury reports containing unprivileged materials and findings	Pen. Code, § 929	This section sets forth the circumstances under which a grand jury may make available to the public certain information relied on for its "final report" and provides that a judge may require redaction or "masking" of any part of the evidentiary material, findings, or other information to be released, including "the identity of witnesses and any testimony or materials of a defamatory or libelous nature."
14	Personal information regarding witnesses or victims	Pen. Code, § 964	The court and district attorney shall establish a mutually agreeable procedure to protect the confidential personal information of any witness or victim contained in police reports submitted to a court in support of a complaint, indictment, information, search warrant and/or arrest warrant.
15	Financial statements and/or other financial information of criminal defendants	Pen. Code, § 987(c)	To determine if a defendant qualifies for a public defender, the court may require the defendant to file a financial statement with the court under penalty of perjury, which must remain "confidential and privileged" unless certain, enumerated exceptions apply.
16	Applications by indigent defendants for funds for investigators and/or experts	Pen. Code, § 987.9	"The fact that an application has been made shall be confidential and the contents of the application shall be confidential." (See subd. (d) for exception(s).)
17	Specified victim statements, including statements in lieu of personal appearance	Pen. Code, § 1191.15	With certain, enumerated exceptions, "[w]henever a written, audio, or video statement or statement stored on a CD ROM, DVD, or other medium is filed with the court, it shall remain sealed until the time set for imposition of judgment and sentence …"
18	Results of mandatory AIDS testing	Pen. Code, § 1202.6(f)	With certain, specified exceptions, the results of mandatory AIDS testing for defendants convicted of violating Penal Code section 647(b) "shall be confidential."
19	Diagnostic reports from the Director of the Department of Corrections	Pen. Code, § 1203.03	The reports from the Director of the Department of Corrections concerning defendants considered for "treatment services as can be provided at a diagnostic facility" shall "be served only upon the defendant or his counsel, the probation officer, and the prosecuting attorney by the court receiving

			such report … [and] … the information contained therein shall not be disclosed to anyone else without the consent of the defendant. After disposition of the case, all copies of the report, except the one delivered to the defendant or his counsel, shall be filed in a sealed file …"
20	Probation reports filed with the court	Pen. Code, § 1203.05	This section sets forth limitations on who may inspect probation reports filed with the court, and when those reports may be inspected.
21	Records of misdemeanor convictions of minors	Pen. Code, § 1203.45	With a few stated exceptions and/or limitations, this section allows for the sealing of "the record of conviction and other official records in the case, including records of arrests resulting in the criminal proceeding and records relating to other offenses charged in the accusatory pleading, whether defendant was acquitted or charges were dismissed."
22	Three specific sets of records: (1) Any written report of any law enforcement officer or witness to any offense; (2) Any information reflecting the arrest or conviction record of a defendant; and (3) Any affidavit or representation of any kind, verbal or written	Pen. Code, § 1204.5	With certain, specified exceptions, this section prohibits a judge from reading or considering the above records without the defendant's consent given in open court.
23	State summary criminal history information (i.e., rap sheets.)	Pen. Code, § 11142	Makes it a misdemeanor for a person authorized to receive state criminal history information to furnish it to an unauthorized person.
24	State summary criminal history information (i.e., rap sheets.)	Pen. Code, § 11143	Generally makes it a misdemeanor for any person to improperly buy, receive, or possess criminal history information.
25	State summary criminal history information (i.e., rap sheets.)	Pen. Code, § 11144	Prescribes when information from criminal histories may be disseminated without violation.
26	Local summary criminal history information (i.e., rap sheets.)	Pen. Code, § 13300	Prescribes who may have access to local summary criminal history information.
27	Local summary criminal history information (i.e., rap sheets.)	Pen. Code, § 13302	Makes it a misdemeanor for a criminal justice agency employee to improperly furnish a person's criminal history to an unauthorized recipient.
28	Local summary criminal history information (i.e., rap sheets.)	Pen. Code, § 13303	Makes it a misdemeanor for an authorized recipient of criminal history information to improperly furnish it to an unauthorized recipient.
29	Local summary criminal	Pen. Code, § 13304	Generally makes it a misdemeanor for any person to improperly buy, receive, or possess criminal

	history information (i.e., rap sheets.)		history information.
30	Local summary criminal history information (i.e., rap sheets.)	Pen. Code, § 13305	Prescribes when information from criminal histories may be disseminated without violation.
31	Court records and documents relating to search warrants	Pen. Code, § 1534	"The documents and records of the court relating to the warrant need not be open to the public until the execution and return of the warrant or the expiration of the 10-day period after issuance. Thereafter, if the warrant has been executed, the documents and records shall be open to the public as a judicial record."
32	Peace and custodial officer personnel records	Evid. Code, §§ 1043, 1045–1047	In conjunction with Penal Code section 832.5, these sections restrict how the court may review and disclose peace officer personnel records.
33	Exhibits	Cal. Rules of Court, rule 2.400(c)(1)	"The clerk must not release any exhibit except on order of the court."
34	Reporters' transcripts of *Marsden* hearings	Cal. Rules of Court, rule 8.328	"The reporter's transcript of any hearing held under *People v. Marsden* (1970) 2 Cal.3d 118 must be kept confidential."
35	Records on appeal	Cal. Rules of Court, rule 8.610	This rule provides for confidentiality of certain records on appeal.
36	Juvenile court records	Welf. & Inst. Code, § 781	This section sets forth the procedure for—and consequences of—petitions for sealing juvenile records.
	PROBATE		
1	Confidential Guardian Screening Form (form GC-212	Cal. Rules of Court, rule 7.1001(c)	This mandatory Judicial Council form regarding the proposed guardian is confidential. It is used by the court and by persons or agencies designated by the court to assist in determining whether a proposed guardian should be appointed. (Cal. Rules of Court, rule 7.1001(c))
2	Confidential Supplemental Information (form GC-312)	Prob. Code, § 1821(a)	This form regarding the proposed conservatee is confidential. It shall be separate and distinct from the form for the petition. The form shall be made available only to parties, persons given notice of the petition who have requested this supplemental information, or who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Probate Code, § 1821(a))
3	Confidential Conservator Screening Form (form GC-314)	Cal. Rules of Court, rule 7.1050(c)	This mandatory Judicial Council form is confidential. (Cal. Rules of Court, rule 7.1050(c)).
4	Reports regarding proposed guardianship or conservators	Prob. Code, §§ 1513, 1826	An investigative report created pursuant to Probate Code section 1513 concerning a proposed guardianship is confidential and available only to parties served in the action or their attorneys (generally, parents, legal custodian of child). An investigative report created pursuant to Probate Code section 1826 regarding the proposed conservatee is confidential and available only to those persons specified by statute. Under the statute, the reports on proposed conservatees shall be made available only to parties, persons given notice of the petition who have requested the report, or

			who have appeared in the proceedings, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interest of the conservatee. The clerk shall make provisions for limiting the disclosure of the reports on guardianships and conservatorships exclusively to persons entitled thereto. (Prob. Code, §§ 1513, subd. (d) & 1826, subd. (n))
5	Investigator's review reports in conservatorships	Prob. Code, § 1851	These reports are confidential. The information in the reports may be made available only to parties, persons identified in section 1851(b), persons given notice who have requested the report or appeared in the proceeding, their attorneys, and the court. The court has the discretion to release the information to others if it would serve the interests of the conservatee. The clerk shall make provisions for limiting the disclosure of the report exclusively to persons entitled thereto. (Prob. Code, §§ 1851, subd. (b) and (e).) Subdivision (b) provides for special restricted treatment of attachments containing medical information and confidential criminal information from CLETS. Although the attachments are not mentioned in (e), it is recommended, to be consistent with (b), that they be treated as confidential except to the conservator, conservatee, and their attorneys.
6	Certification of counsel of their qualifications (form GC-010) and certification of completion of continuing education (form GC-011)	Cal. Rules of Court, rule 7.1101	The forms state that they are "confidential for court use only." They are governed by rule 7.1101, which states only that the certifications must be submitted to the court but not lodged or filed in a case file.
	FAMILY		
1	Family conciliation court records	Fam. Code, § 1818	Records and proceedings in Family Conciliation Courts are confidential.
2	Psychological evaluations of children and recommendations regarding custody and visitation; confidentiality; exceptions	Fam. Code, § 3025.5	Any psychological evaluations of children or recommendations regarding custody and visitation proceedings that are submitted to the court shall remain confidential and may be disclosed only to certain people (parties, attorneys, law enforcement officers, judicial officers, family law facilitator).
3	Controlled substances or alcohol abuse testing of persons seeking custody or visitation; grounds for testing; confidentiality of results; penalties for unauthorized disclosure	Fam. Code, § 3041.5	Test results for controlled substances or alcohol abuse of persons seeking custody or visitation shall remain confidential and maintained in a sealed record in the court file. These results may not be released to anyone except the court, the parties, their attorneys, the Judicial Council, and any other person whom the court expressly grants access by written order made with prior notice to all parties.
4	Child custody evaluations; reports; confidentiality, and use	Fam. Code, § 3111	Child custody evaluation reports are available only to the court, the parties, and their attorneys.
5	Confidentiality of mediation proceedings	Fam. Code, § 3177	Mediation proceedings shall be held in private and shall be confidential. All communications, verbal or written, from the parties to the mediator made in the proceeding are official information

			within the meaning of Evidence Code §1040.
6	Recommendations to court as to custody or visitation, investigation, restraining orders, and minor's counsel	Fam. Code, §§ 3183 and 3184	Mediator may submit recommendations to the court as to the custody of or visitation with the child except as is provided in Family Code section 3188.
7	Confidential mediation program	Fam. Code, § 3188 (not operative pursuant to (b) because of lack of budget allocation)	In a court that adopts a confidential mediation program, the mediator may not make a recommendation as to custody or visitation to anyone other than the disputing parties, exceptions noted in statute.
8	State and federal income tax returns; submission to court; examination and discovery	Fam. Code, § 3552	Tax returns are confidential court records.
9	Criminal history search; prior restraining orders	Fam. Code, § 6306	Information found in a search for person to restrained's prior criminal history must be kept confidential in certain circumstances (see subd. (a)); the information may be reviewed or disclosed to certain persons involved in the case.
10	Hearing or trial in closed court; papers and records, inspection	Fam. Code, § 7643	With the exception of the final judgment, records in Uniform Parentage Act proceedings are closed to the public.
11	Inspection of petitions, reports, and court records and briefs	Fam. Code, § 7805	A petition to terminate parental rights or a report of the probation officer or county social services department may be inspected only by the following persons: (1) Court personnel. (2) The child who is the subject of the proceeding. (3) The parents or guardian of the child. (4) The attorneys for the parties. (5) Any other person designated by the judge. On appeal to the court of appeal or the Supreme Court, the court record and briefs filed by the parties may be inspected only by the following persons: (1) Court personnel. (2) A party to the proceeding. (3) The attorneys for the parties. (4) Any other person designated by the presiding judge of the court before which the matter is pending. The court and/or probation officer may provide information in a termination of parental rights case, if it is believed that the welfare of the child will be promoted, to any of the following: (1) The State Department of Social Services. (2) A county welfare department.

			(3) A public welfare agency. (4) A private welfare agency licensed by the State Department of Social Services.
12	Privacy rights; confidentiality of records	Fam. Code, § 17212	All child and spousal support enforcement records are confidential, and shall not be released for any purpose not directly connected with the administration of the child and spousal support enforcement program. Information regarding the location of one party or the child shall not be disclosed to another party, or to the attorney of any other party, if a protective order has been issued by a court or administrative agency with respect to the party, a good cause claim under Section 11477.04 of the Welfare and Institutions Code has been approved or is pending, or the public agency responsible for establishing paternity or enforcing support has reason to believe that the release of the information may result in physical or emotional harm to the party or the child. The information shall be omitted from any pleading or document to be submitted to the court. A proof of service filed by the local child support agency shall not disclose the address where service of process was accomplished. Instead, the local child support agency shall keep the address in its own records. Authorized disclosures are described in the statute.
13	Inspection of documents; authorization; fee; deletion of identification of birth parents; certificate of adoption	Fam. Code, § 9200	Documents relating to adoption proceedings are confidential and may be seen only by the parties, their attorneys, and the child welfare agency. The name and identifying information regarding the child's birth parents shall not be disclosed to anyone receiving the documents unless the adoption is by a stepparent or second-parent.
14	Confidentiality	Cal. Rules of Court, rule 3.854	This covers guidelines for mediators with respect to confidentiality.
15	Court-connected child custody mediation	Cal. Rules of Court, rule 5.210(d)(1)(F) & (G), (h)(3)	Mediators must protect the confidentiality of the parties and the child by not releasing information about the case except as is authorized.
16	Domestic violence protocol for Family Court Services	Cal. Rules of Court, rule 5.215(e), (f)(2), (g)(3)	Family Court Services (FCS) staff must make reasonable efforts to keep contact/identifying information confidential on FCS documents when dealing with domestic violence cases.
	JUVENILE		
1	Information available for juvenile court proceedings regarding best interest of child; confidentiality	Welf. & Inst. Code, § 204	Any information provided to the court under this section to make a determination regarding the best interest of the child may be released to authorized persons; however, if the information is confidential, it shall remain confidential and not be released to others except as is necessary.
2	Admission of public and persons having interest in case; confidentiality of name; disclosure of court documents	Welf. & Inst. Code, § 676	Unless requested by the minor, the public shall not be admitted to a juvenile court hearing; the name of a minor found who has committed one of the juvenile offenses listed in Welfare and Institutions Code section 676 shall not be confidential unless the court, for good cause, so orders; when a petition is sustained for any of these offenses, the charging petition, the minutes of the proceeding, and the orders of adjudication and disposition of the court contained in the court file may be available for public inspection; the probation officer or any party may petition the juvenile

			court to prohibit disclosure to the public of any file or record.
3	Records related to any petition dismissed under Welf. & Inst. Code, § 786	Welf. & Inst. Code, § 786	The court must order sealed all records related to any petition dismissed under Welfare and Institutions Code section 786 that are in the custody of the juvenile court, law enforcement agencies, the probation department, and the Department of Justice. The procedures for sealing these records are stated in Welfare and Institutions Code section 786.
43	Juvenile court record	Welf. & Inst. Code, § 825	The order and findings of the superior court in each case under the provisions of this chapter shall be entered in a suitable book or other form of written record that shall be kept for that purpose and known as the "juvenile court record."
54	Release or destruction of court record; reproduction	Welf. & Inst. Code, § 826 (et seq.)	The juvenile court records include all records and papers, any minute book entries, dockets, and judgment dockets. These records may be destroyed after five years from the date on which jurisdiction of the juvenile court is terminated; they must be destroyed by order of the court under various circumstances, outlined below; records may also be released to the juvenile who is the subject of the proceeding.
65	Juvenile case file inspection; confidentiality; release; probation reports; destruction of records; liability	Welf. & Inst. Code, § 827	Only certain persons may inspect juvenile case files; special rules apply when a deceased child is involved; further description of protocol for access/release of information in the files.
76	Computerized database system; authorized access; security procedures	Welf. & Inst. Code, § 827.1	A city/county may establish a computerized database system for intercounty/city exchange of information regarding minors under the jurisdiction of the juvenile court and may be accessed by authorized personnel under certain circumstances; this system must have security procedures to block unauthorized personnel from accessing the data.
87	Commission of felony; notice; disclosure of information	Welf. & Inst. Code, § 827.2	Information received regarding a juvenile's commission of a felony shall be held in confidence, with limited exceptions.
98	Commission of serious felony; minor in custody; hearing commenced; disclosure of name	Welf. & Inst. Code, § 827.5	Notwithstanding any other provision of law except sections 389 and 781 of Welfare and Institutions Code and section 1203.45 of the Penal Code, a law enforcement agency may disclose the name of any minor 14 years of age or older taken into custody for the commission of any serious felony, as defined in subdivision (c) of section 1192.7 of the Penal Code, and the offenses allegedly committed, upon the request of interested persons, following the minor's arrest for that offense.
109	Commission for violent offense; release of information	Welf. & Inst. Code, § 827.6	A law enforcement agency may release the name, description, and the alleged offense of any minor alleged to have committed a violent offense, as defined in subdivision (c) of section 667.5 of the Penal Code, and against whom an arrest warrant is outstanding, if the release of this information would assist in apprehending the minor or protecting public safety. Neither the agency nor the city, county, or city and county in which the agency is located, shall be liable for civil damages resulting from release of this information.
1110	Disclosure of juvenile police records	Welf. & Inst. Code, § 827.9	Records or information gathered by law enforcement agencies relating to the taking of a minor into custody, temporary custody, or detention (juvenile police records) should be confidential. See subdivision (b) of the Welfare and Institutions Code for list of persons or entities that law

			enforcement may release a copy of a juvenile police record to.
1211	Disclosure of information gathered by law enforcement agency; release of descriptive information about minor escapees	Welf. & Inst. Code, § 828	With exceptions, information gathered by a law enforcement agency relating to taking the minor into custody can be disclosed to another law enforcement agency; the law enforcement agency may release the name of, and any descriptive information about, the minor.
1312	Confidentiality of records	Cal Rules of Court, rule 5.552	In conjunction with Welfare & Institutions Code sections 827 and 828, this rule sets forth the procedure for review of otherwise confidential juvenile court records.
1413	School district police or security department; disclosure of juvenile criminal records; protection of vulnerable school staff and other students	Welf. & Inst. Code, § 828.1	There is a limitation to the confidentiality of juvenile criminal records in cases involving serious acts of violence—although any dissemination should be as limited as possible and take into consideration school-related issues.
1514	Crimes against property, students, or personnel of school; juvenile custody or commission; information sharing	Welf. & Inst. Code, § 828.3	Notwithstanding any other provision of law, information relating to the taking of a minor into custody on the basis that he or she has committed a crime against the property, students, or personnel of a school district or a finding by the juvenile court that the minor has committed such a crime may be exchanged between law enforcement personnel, the school district superintendent, and the principal of a public school in which the minor is enrolled as a student if the offense was against the property, students, or personnel of that school.
1615	Review of juvenile court records; suitability for release	Welf. & Inst. Code, § 829	Notwithstanding any other provision of law, the Board of Prison Terms, in order to evaluate the suitability for release of a person before the board, shall be entitled to review juvenile court records that have not been sealed, concerning the person before the board, if those records relate to a case in which the person was found to have committed an offense that brought the person within the jurisdiction of the juvenile court pursuant to Section 602.
1716	Nonprivileged information and writings; disclosure among members of juvenile justice multidisciplinary team	Welf. & Inst. Code, § 830.1	Notwithstanding any other provision of law, members of a juvenile justice multidisciplinary team engaged in the prevention, identification, and control of crime, including, but not limited to, criminal street gang activity, may disclose and exchange nonprivileged information and writings to and with one another relating to any incidents of juvenile crime, including criminal street gang activity, that may also be part of a juvenile court record or otherwise designated as confidential under state law if the member of the team having that information or writing reasonably believes it is generally relevant to the prevention, identification, or control of juvenile crime or criminal street gang activity. Every member of a juvenile justice multidisciplinary team who receives such information or writings shall be under the same privacy and confidentiality obligations and subject to the same penalties for violating those obligations as the person disclosing or providing the information or writings. The information obtained shall be maintained in a manner that ensures the protection of confidentiality. As used in this section, “nonprivileged information” means any information not subject to a privilege pursuant to Division 8 (commencing with Section 900) of the Evidence Code.

			As used in this section, "multidisciplinary team" means any team of three or more persons, the members of which are trained in the prevention, identification, and control of juvenile crime, including, but not limited to, criminal street gang activity, and are qualified to provide a broad range of services related to the problems posed by juvenile crime and criminal street gangs. The team may include, but is not limited to, (a) Police officers or other law enforcement agents (b) Prosecutors (c) Probation officers (d) School district personnel with experience or training in juvenile crime or criminal street gang control (e) Counseling personnel with experience or training in juvenile crime or criminal street gang control (f) State, county, city, or special district recreation specialists with experience or training in juvenile crime or criminal street gang control.
18	Immigration status	Welf. & Inst. Code, § 831	Juvenile court records should remain confidential regardless of a juvenile's immigration status. (Welf. & Inst. Code, § 831(a).) Juvenile information may not be disclosed or disseminated to federal officials absent a court order upon filing a petition under Welfare and Institutions Code section 827(a). (Welf. & Inst. Code, § 831(b)–(c).) Juvenile information may not be attached to any documents given to or provided by federal officials absent prior approval of the presiding judge of the juvenile court under Welfare and Institutions Code section 827(a)(4). (Welf. & Inst. Code, § 831(d).) "Juvenile information" includes the "juvenile case file" as defined in Welfare and Institutions Code section 827(e), as well as information regarding the juvenile such as the juvenile's name, date or place of birth, and immigration status. (Welf. & Inst. Code, § 831(e).)
19~~17~~	Records of mental health treatment or services	Welf. & Inst. Code, § 5328 et seq.	Records of mental health treatment, services, or confinement are confidential as described in the Welfare and Institutions Code section 5328 et seq.
20~~18~~	Confidentiality; rules and regulations; violations; disclosure of confidential information regarding criminal act	Welf. & Inst. Code, § 10850 et seq.	All records and information regarding the identity of applicants for or recipients of public social services grants are confidential and not open to examination for any purpose not directly involved with the administration of the grant program or any investigation, prosecution, or criminal or civil proceeding conducted regarding the administration of the program. Exceptions and authorizations of disclosure are listed in the codes.

APPENDIX 2—ROTATION ASSIGNMENT FOR LONGITUDINAL (100%) SAMPLE
California Rules of Court, Rule 10.855
As of January 1, 2014

YEAR OF FILING	CALIFORNIA SUPERIOR COURTS		
	Group 1	**Group 2**	**Group 3**
2014	Calaveras	Yolo	Tuolumne
2015	Colusa	Yuba	Ventura
2016	Del Norte	Alameda	Fresno
2017	Glenn	Butte	Imperial
2018	Inyo	Contra Costa	Kern
2019	Lassen	El Dorado	Kings
2020	Mariposa	Humboldt	Los Angeles
2021	Lake	Madera	Modoc
2022	Marin	Merced	Mono
2023	Mendocino	Monterey	Plumas
2024	Napa	Orange	San Benito
2025	Nevada	Riverside	Sierra
2026	Placer	San Bernardino	Siskiyou
2027	Sacramento	San Diego	Trinity
2028	San Francisco	San Luis Obispo	Alpine
2029	San Joaquin	San Mateo	Amador
2030	Shasta	Santa Barbara	Calaveras
2031	Solano	Santa Clara	Colusa
2032	Sonoma	Santa Cruz	Del Norte
2033	Sutter	Stanislaus	Glenn
2034	Tehama	Tulare	Inyo
2035	Yolo	Tuolumne	Lassen
2036	Yuba	Ventura	Mariposa
2037	Alameda	Fresno	Modoc
2038	Butte	Imperial	Mono
2039	Contra Costa	Kern	Plumas
2040	El Dorado	Kings	San Benito

YEAR OF FILING	CALIFORNIA SUPERIOR COURTS		
	Group 1	**Group 2**	**Group 3**
2041	Humboldt	Los Angeles	Sierra
2042	Madera	Siskiyou	Lake
2043	Merced	Trinity	Marin
2044	Monterey	Alpine	Mendocino
2045	Orange	Amador	Napa
2046	Riverside	Calaveras	Nevada
2047	San Bernardino	Colusa	Placer
2048	San Diego	Del Norte	Sacramento
2049	San Luis Obispo	Glenn	San Francisco
2050	San Mateo	Inyo	San Joaquin
2051	Santa Barbara	Lassen	Shasta
2052	Santa Clara	Mariposa	Solano
2053	Santa Cruz	Modoc	Sonoma
2054	Stanislaus	Mono	Sutter
2055	Tulare	Plumas	Tehama
2056	Tuolumne	San Benito	Yolo
2057	Ventura	Sierra	Yuba
2058	Fresno	Siskiyou	Alameda
2059	Imperial	Trinity	Butte
2060	Kern	Alpine	Contra Costa
2061	Kings	Amador	El Dorado
2062	Los Angeles	Calaveras	Humboldt
2063	Colusa	Lake	Madera
2064	Del Norte	Marin	Merced
2065	Glenn	Mendocino	Monterey

Index

(Index will be developed in the next version of TCRM.)

Annual Agenda
Project 1. CMS Data Exchanges

Develop Standardized Approaches to CMS Interfaces and Data Exchanges with Critical State Justice Partners

ITAC Resource(s):

ITAC Workstream, Executive Sponsor: David Yamasaki

JCC Staff Resource(s):

IT (Neil Payne, Jackie Woods)

Workstream Project Manager: Alan Crouse (Technical Lead)

MAJOR TASKS	STATUS	UPDATES
(a) Identify specific justice partners exchanges required and court interface needs.	In Progress	Primary requirements and needs identified; will be further confirmed and expanded via detailed discussions between justice partners and CMS vendors.
(b) Establish standards for, and define where feasible, common exchange(s), consistent with national standards, and secure methods to share those exchanges for courts wishing to implement them.	In Progress	Justice partner focus sessions complete. Next phase focuses on CMS vendors working more directly with justice partners to refine data. Designated court representatives will lead sessions, capture/share development, and identify issues for resolution.
(c) Work with CMS vendors to facilitate timely implementation of standardized exchanges where needed, consistent with existing court deployment schedules.	In Progress	Implementation continues to be a topic of discussion during the workstream meetings.
(d) Develop governance processes to ensure continuing development and maintenance of statewide data exchanges established, and to maintain on-going communication and cooperation with our justice partners and CMS vendors in this effort.	In Progress	Key objectives identified. Composition of governance membership to be identified by ITAC. Completion projected by February, 2016.

Annual Agenda
Project 2. E-Filing

Update E-Filing Standards, and Develop Provider Certification, Deployment Strategy, and Rules Evaluation

ITAC Resource(s):

(a)-(c): ITAC Workstream, Executive Co-Sponsors: Hon. Sheila F. Hanson and Rob Oyung
(d): Rules & Policy Subcommittee

JCC Staff Resource(s):

IT (Edmund Herbert, Manny Floresca), Legal Services (Patrick O'Donnell, Tara Lundstrom)

Workstream Project Manager: Snorri Ogata

MAJOR TASKS	STATUS	UPDATES
(a) Update the technical standards for court e-filing, namely, the XML specification and related schema.	In Progress	Standards recommendation expected to be Oasis ECF specification (https://www.oasis-open.org/committees/legalxml-courtfiling). Workstream conversations to date (and with vendors) has presupposed California will be following the national standard.
(b) Develop the E-Filing Service Provider (EFSP) selection/certification process.	In Progress	See item (c) below.
(c) Develop the roadmap for an e-filing deployment strategy, approach, and branch solutions/alternatives.	In Progress	E-filing Summit held May 22. Over 70 attendees in person and via phone. Workstream participants being identified. Analysis of different e-filing models continue to be evaluated. Final recommendations now targeted for December 2015/January 2016.
(d) Evaluate current e-filing rules, including provisions for mandatory e-filing.	Not Started	Rules assessment targeted for completion end of November 2015.

Annual Agenda
Project 3. Remote Courtroom Video

Develop Remote Courtroom Video Standards, a Pilot Program, and Update to Rules

ITAC Resource(s):

(a)-(b): ITAC Workstream, Executive Sponsor: Hon. Terence L. Bruiniers
(c): ITAC Rules & Policy Subcommittee

JCC Staff Resource(s):

IT (Fati Farmanfarmaian, Nate Moore), Legal Services (Patrick O'Donnell, Tara Lundstrom)

MAJOR TASKS	STATUS	UPDATES
(a) Develop technical standards for remote courtroom video.	In Progress	The LAP Technological Solutions Subcommittee (TSS) (also chaired by Justice Bruiniers) provisionally approved standards developed by the National Center for State Courts for use in the video remote interpreting (VRI) pilot project (see item (b) below). Refinement of those standards is anticipated as a result of the pilot.
(b) Define and implement, in cooperation with the Language Access Plan (LAP) Implementation Task Force, a Video Remote Interpreting Pilot (VRI) Program for foreign languages.*	In Progress	The LAP TSS approved a programmatic outline for a pilot and is developing an RFP seeking a vendor partner. The chair also seeks operations support for the project. Once a vendor and court participant(s) are selected, the chair expects to staff an ITAC workstream to coordinate implementation.
(c) Seek extension of Rule of Court 4.220 (Remote Video Proceedings in Traffic Infraction Cases). Consider Expansion to other case types.	Completed	The Judicial Council approved the permanent authorization for remote video proceedings in traffic infraction cases, effective September 1, 2015.
*Note: Item (b) was updated (post annual agenda approval) to show cooperation with LAP task force specifically.		

Annual Agenda
Project 4. Next Generation Hosting Strategy Assessment

Assessment of Alternatives for Transition to Next-Generation Branchwide Hosting Model

ITAC Resource(s):

ITAC Projects Subcommittee; workstreams may be required to complete the longer term components

JCC Staff Resource(s):

IT (Fati Farmanfarmaian, Kathy Fink, Raj Talla, Michael Derr), Court Operations Services (Karen Viscia)

MAJOR TASKS	STATUS	UPDATES
(a) Complete hosting needs assessment, develop implementation recommendations, including an evaluation of alternatives and costs.	Completed	Survey results and report distributed to ITAC members for review at its October teleconference.
Note: Limited scope due to resource constraints; additional tasks to be considered in future annual agenda.		

Annual Agenda
Project 4 (new). Next Generation Hosting Strategy Workstream (new)

Assessment of Alternatives for Transition to Next-Generation Branchwide Hosting Model

ITAC Resource(s):
ITAC Workstream, Executive Co-Sponsors: Hon. Kyle Brodie, Brian Cotta

JCC Staff Resource(s):
IT (Donna Keating)

Workstream Project Manager: Heather Pettit

MAJOR TASKS	STATUS	UPDATES
(a) Define workstream project schedule and detailed tasks; gain approval of workstream membership	In Progress	Project approved in May to move forward as a workstream. Volunteer membership list established and approved by ITAC and JCTC (September); is awaiting E&P approval. Sponsors and project manager expect to hold a planning meeting in November to discuss next steps and to update the project schedule.
(b) Outline industry best practices for hosting (including solution matrix with pros, cons, example applications, and costs).	Not Started	Workstream start has been delayed. Expect this task to begin in December/January with a target completion of March/April 2016 or later, depending on how easily information can be gathered without formal procurement process. Costs may not be realistically attainable, which may result in a slight change of strategy.
(c) Produce a roadmap tool for use by courts in evaluating options.	Not Started	
(d) Consider educational summit on hosting options, and hold summit if appropriate.	Not Started	
(e) Identify requirements for centralized hosting.	Not Started	

Annual Agenda
Project 5. Information Security Framework

Document and Adopt Court Information Systems Security Policy Framework

ITAC Resource(s):
ITAC Workstream, Executive Sponsor: Rob Oyung

JCC Staff Resource(s):
IT (Michael Derr)

Workstream Project Manager: Rob Oyung

MAJOR TASKS	STATUS	UPDATES
(a) Finish the work that was started on the Court Information Systems Security Policy Framework.	Completed	"How to Use the Framework" document distributed broadly inside the branch (CEOs, CIOs, PJs, ITAC, JCTC) for input. Final version approved by ITAC; and will proceed to the JCTC for review and approval.
(b) Initially adopt the framework at a select group of pilot courts.	Completed	The 7 courts participating in the workstream piloted the framework and performed an initial assessment. Those courts have already completely or partially implemented 75% of the framework.
(c) Adopt the framework at the remaining courts, as needed.	Not Started	Expected after document approval/publication.

Annual Agenda
Project 6. Disaster Recovery Framework Assessment

Survey and Assessment for Court Disaster Recovery Framework and Pilot

ITAC Resource(s):
ITAC Projects Subcommittee

JCC Staff Resource(s):
IT (Fati Farmanfarmaian, Kathy Fink, Raj Talla, Michael Derr)

MAJOR TASKS	STATUS	UPDATES
(a) Survey and provide a disaster recovery needs assessment and gap analysis for the major technology components in the trial and appellate courts.	Completed	Survey results and report distributed to ITAC members for review at its October teleconference.
Note: Limited scope due to resource constraints; additional tasks to be considered in future annual agenda.		

Annual Agenda
Project 7. Privacy Policy

Develop Branch & Model Court Privacy Policies on Electronic Court Records and Access

ITAC Resource(s):
ITAC Rules & Policy Subcommittee

JCC Staff Resource(s):
IT (Manny Floresca), Legal Services (Patrick O'Donnell, Tara Lundstrom)

MAJOR TASKS	STATUS	UPDATES
(a) Continue development of a comprehensive statewide privacy policy addressing electronic access to court records and data to align with both state and federal requirements.	In Progress	A subgroup has been formed to develop the policy, but this project has been on hold due to staffing limitations. Work on this project is expected to resume in fall, 2015.
(b) Continue development of a model (local) court privacy policy, outlining the key contents and provisions to address within a local court's specific policy.	Not Started	

Annual Agenda
Project 8. SRL E-Services Portal

Evaluate Feasibility and Desirability of Establishing a Branch Self-Represented Litigants (SRL) E-Services Portal

ITAC Resource(s):

ITAC Projects Subcommittee; workstreams may be required to complete the longer term components

JCC Staff Resource(s):

IT (Fati Farmanfarmaian), Legal Services (Patrick O'Donnell, Tara Lundstrom), and CFCC (Karen Cannata, Diana Glick)

MAJOR TASKS	STATUS	UPDATES
(a) Determine and validate both litigant needs (including LEP litigants) and court requirements.	Completed	In its July 2015 report to ITAC assessing the need and approach for developing an SRL E-Services Portal, CFCC staff recommended ITAC establish a new workstream to develop requirements for a statewide portal that is e-delivery/e-filing ready. The ITAC chair approved this recommendation and assigned Judge Freedman and Judge Mize as workstream co-sponsors.
(b) Identify available existing technology and infrastructure components to leverage.	Completed	The CFCC study included some assessment of existing infrastructure. If necessary, this work will continue as part of the newly formed SRL workstream.
(c) Identify information resources to assist litigants.	Not Started	This effort will be part of the newly formed SRL workstream.
Note: Limited scope due to resource constraints; additional tasks to be considered in future annual agenda.		Staffing the new workstream is expected later in 2015, or as part of the 2016 ITAC annual agenda.

Annual Agenda
Project 9. E-Signatures

Develop Standards for Electronic Signatures

ITAC Resource(s):
ITAC Rules & Policy Subcommittee

JCC Staff Resource(s):
IT (Manny Floresca), Legal Services (Patrick O'Donnell, Tara Lundstrom)

MAJOR TASKS	STATUS	UPDATES
(a) Develop procedures and standards for use of electronic and digital signatures for court documents, as specified in Government Code section 68150(g), for inclusion in the Court Records Manual.	In Progress	Proposed standards were circulated to the trial courts for comment. ITAC will review the comments during its October 30 meeting. The standards are set to be considered by the Judicial Council during its December meeting.
(b) Recommend rule proposal incorporating standards into Rules of Court, as appropriate.	Withdrawn	The subcommittee determined that this task is not necessary.
Note: This project is distinct from developing standards for court (digital) records certification, i.e., the authentication of court documents and the true certification thereof (per ITAC's 2013 annual agenda review meeting).		

Annual Agenda
Project 10. Tactical Plan for Technology

Update Tactical Plan for Technology for Effective Date 2016-2018

ITAC Resource(s):
Chair and full committee

JCC Staff Resource(s):
IT (Jamel Jones)

MAJOR TASKS	STATUS	UPDATES
(a) Review and update the Tactical Plan for Technology.	On Hold	In September 2015, Chairs reviewed existing Tactical Plan for progress to-date. Found that prioritized projects were underway; and committee was on track to complete. No major gaps exist. Updating the Tactical Plan will begin mid-year 2016.
(b) Circulate for branch and public comment.	On Hold	
(c) Finalize and submit for approval.	On Hold	

Annual Agenda
Project 11. Policy & Rules for E-Access to Appellate Court Records

Develop Branch Policy and Rules on Public Access to Electronic Appellate Court Records

ITAC Resource(s):
Joint Appellate Technology Subcommittee

JCC Staff Resource(s):
IT (Julie Bagoye), Legal Services (Patrick O'Donnell, Tara Lundstrom)

MAJOR TASKS	STATUS	UPDATES
(a) Develop a comprehensive statewide policy addressing reasonable public access to electronic appellate court records to align with access rules for the trial courts.	Completed	JATS' recommendations for rules on access to electronic court records is complete. Rule proposals are in progress (see below).
(b) Draft rule proposal to incorporate standards into Rules of Court, as appropriate.	Completed	JATS developed proposed rules (8.80-8.85) on electronic access to appellate court records. The rules were circulated for public comment from April 17 to June 17. JATS recommended revisions in response to the comments received, and CTAC and the Appellate Advisory Committee have approved those recommendations. The revised rules will be considered by the Judicial Council at its October 27 meeting.
Note: This project corresponds to the Appellate Advisory Committee annual agenda item #8.		

Annual Agenda
Project 12. Rules for Electronic Service

Evaluate Amendment to Rules of Court to Allow Electronic Service Upon Courts if the Court Consents

ITAC Resource(s):
Joint Appellate Technology Subcommittee and the ITAC Rules & Policy Subcommittee

JCC Staff Resource(s):
IT (Julie Bagoye, Manny Floresca), Legal Services (Patrick O'Donnell, Tara Lundstrom)

MAJOR TASKS	STATUS	UPDATES
(a) Consider whether to recommend rule amendments to clarify that a court may be served electronically if the court consents to receive this form of service.	Completed	At its October 27 meeting, the Judicial Council will consider adopting the amendments to rules 2.251 and 8.71 per ITAC recommendation. If approved as expected, this task will be complete by the October 30 ITAC meeting.
Note: This project applies at both the appellate and trial court levels. Also, this project is intended to correspond to the Appellate Advisory Committee agenda item #9.		

Annual Agenda
Project 13. Modernize Rules of Court: Phase I

Modernize Trial and Appellate Court Rules to Support E-Business

ITAC Resource(s):

ITAC Rules & Policy Subcommittee and the Joint Appellate Technology Subcommittee

JCC Staff Resource(s):

IT (Manny Floresca, Julie Bagoye), Legal Services (Patrick O'Donnell, Tara Lundstrom)

MAJOR TASKS	STATUS	UPDATES
(a) In collaboration with other advisory committees, review rules and statutes in a systematic manner and develop recommendations for comprehensive changes to align with modern business practices (e.g., eliminating paper dependencies).	Completed	Phase I of the Rules Modernization Project is complete. At its October meeting, the Judicial Council adopted the rule amendments sponsored by ITAC. Work on Phase II is already underway and includes more substantive legislative and rules proposals intended to further promote e-practices.
Note: This project corresponds to the Appellate Advisory Committee agenda item #10, as well as on the annual agendas of the additional (subject matter) advisory bodies listed under Resources.		

Annual Agenda
Project 14. Collaborations and Information Exchange

Liaise with Advisory Bodies and the Branch on Technology Intitiatives, Rules and Implementations

ITAC Resource(s):
Liaisons

JCC Staff Resource(s):
IT (Jamel Jones)

MAJOR TASKS	STATUS	UPDATES
(a) Share the Judicial Branch Technology Report with advisory bodies and attend liaison committee meetings.	In Progress	Liaisons are in progress of attending meetings, as appropriate.
(b) Identify opportunaties to collaborate and share liaison feedback to ITAC, the JCTC, the Judicial Council, and the branch, as appropriate.	In Progress	Liaisons will have an opportunity to provide oral reports during the October ITAC meeting.

IT Security Framework Overview

November 2015

ITAC Workstream

- Sponsor: Robert Oyung, CIO Santa Clara
- Members:
  - Paras Gupta, CIO Monterey
  - Brett Howard, CIO Orange
  - Dorothy McCarthy, CIO Marin
  - Jim Brock, CIO Santa Barbara
  - Russ Catalan, CIO Humboldt
  - Pat Patterson, CIO Ventura
  - Michael Derr, Judicial Council IT
  - Raul Ortega, Judicial Council IT

Project Scope

- Publish a “how to use” guide for trial courts.
- Identifies specific sections in the Information Systems Controls Framework published by the Judicial Council that are most relevant to the trial courts.

IT Security Framework

- A model that courts can choose to adopt, NOT mandated.
- Provides context for a local court when they create their local IT security policies.
- Demonstrates that local policies are in alignment with an agreed upon framework.
- Framework is modular and individual sections can be ignored if they do not apply to a local court's specific environment.
- Does not require any funding to implement the framework.
- Local policies that the court decides to implement may require local funding.

“How to Use” Guide Example

- Information Systems Controls Framework document is 138 pages and contains 187 sections.
- Workstream has identified 84 sections most relevant to trial courts.

Access Control			
5.1	Access Control Policy and Procedures	Document an access control policy.	Policy
5.2	Account Management	Identify account managers and create, modify, and disable system accounts based on authorized access	Process
5.6	Least Privilege	Provide only necessary access	Process
5.7	Unsuccessful Logon Attempts	Enforce a limit of invalid logon attempts when appropriate	Technical
5.9	Concurrent Session Control	Limit the number of concurrent session when appropriate	Technical
5.10	Session Lock	Automatically lock session after a defined period	Technical
5.11	Session Termination	Automatically terminate session when appropriate	Technical
5.13	Remote Access	Establish remote access security policy	Policy

Non-IT Example

Domain: Physical Security
Framework recommendation
Court facilities should be secure
Local court policy
Non-public accessible areas can only be entered through a locked entrance
Local court implementation
Option 1: Install locks with physical keys Option 2: Install keypad lock Option 3: Install locks with card key readers

- A local court can decide if they wish to adopt the framework recommendation.
- The local court determines the local court policy.
- The local court determines how to implement the policy.
- The local court identifies if resources exist to implement the local policy.

IT Example

Domain: Access control for mobile devices
Framework recommendation
Establish usage restrictions and configuration and connection requirements for branch entity-controlled mobile devices
Local court policy
Mobile devices must enforce a lock screen PIN. Only email and calendar synchronization allowed. Direct access to court network and other court applications prohibited.
Local court implementation
Option 1: Court IT configures court mobile devices per policy Option 2: Software and configuration settings downloaded by end-user Option 3: Mobile device management software manages device remotely

- A local court can decide if they wish to adopt the framework recommendation.
- The local court determines the local court policy.
- The local court determines how to implement the policy.
- The local court identifies if resources exist to implement the local policy.

IT Security Framework

What it is

- A model that courts can leverage.
- Provides context for a local court's IT security policies.
- Modular – courts can refer to only the sections that are relevant to them.
- Additional documentation to justify the local policy decisions made by a court.

What it is not

- A mandated set of policies.
- A specific list of technologies that should be implemented.
- Requirements for local court policies to be in compliance.

IT Security Checklist

	A	B	C	D	E	F	G	H
1	ISCF Section	Title	Summary	Category	Relevant to this court? (Y/N)	Implemented? (Fully, Partially, No, Not Planned)	If not implemented, how difficult to implement? (Easy, Average, Difficult)	Comments
11	5.7	Unsuccessful Logon Attempts	Enforce a limit of invalid logon attempts when appropriate	Technical				
12	5.8	System use Notification	Display logon message that displays privacy and security notices	Technical				
13	5.9	Concurrent Session Control	Limit the number of concurrent session when appropriate	Technical				
14	5.10	Session Lock	Automatically lock session after a defined period	Technical				
15	5.11	Session Termination	Automatically terminate session when appropriate	Technical				
16	5.12	Permitted Actions Without Identification or Authentication	Document actions that can be performed without identification or authentication	Technical				

- Self-assessment tool for courts to identify areas for potential action.
- Checklist piloted by 7 courts participating in the workstream.
- On average 75% of items on checklist have been fully or partially implemented at the pilot courts.
- Courts estimated that it would take an “average” amount of effort to implement open items (on a scale of “low”, “average”, “high” effort).

Timeline

Milestone	Completion Date (2015)
First draft of “How to Use” guide	April 22
Distribute to CIO for review	May 8
CIO complete review of the guide	May 22
Distribute to CEO for review	May 26
CEO complete review of the guide	June 15
Distribute for Judicial Branch internal review (PJ, CEO, CIO, CTAC, JCTC)	June 29
Complete internal Judicial Branch review	July 20
CTAC approval of final document	October 9
JCTC approval of final document	November 9

JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
Telephone 415-865-4200 • Fax 415-865-4205 • TDD 415-865-4272

MEMORANDUM

Date
October 22, 2015

To
Members of the Judicial Council Technology Committee

Recommended by
Information Technology Advisory Committee
Hon. Terence L. Bruiniers, Chair

Information Security Framework Workstream
Mr. Rob Oyung, Executive Sponsor
Chief Information Officer
Superior Court of California,
County of Santa Clara

Subject
How to Use the Information Systems Controls Framework

Action Requested
Review and Approve

Deadline
November 9, 2015

Contact
Ms. Jamel Jones
Senior Business Systems Analyst
Information Services
jamel.jones@jud.ca.gov

Executive Summary

The Information Security Framework Workstream is pleased to present the "How to Use the Information Systems Controls Framework" and "Information Security Framework Checklist" documents. These deliverables complete the "Court Information Systems Security Policy Framework" tactical initiative outlined in the *California Judicial Branch Tactical Plan for Technology (2014-2016)*. The "How to Use" guide acts as a reference for superior courts to assist them with establishing local policies and procedures based upon the Information Systems Controls Framework Template published by the Judicial Council. Superior courts are not required to implement the framework in its entirety, rather the intent is to encourage superior

courts to use the framework as a template to develop security policies appropriate to their unique local business requirements.

Recommendation

The Information Technology Advisory Committee and its Information Security Framework Workstream recommends approval and publication of the "How to Use the Information Systems Controls Framework" and the associated "Information Security Framework Checklist".

Previous Council Action

The Information Systems Controls Framework Template was developed as a resource for judicial branch entities to use in the adoption and implementation of a standardized information security framework within their organizations. Work to develop this framework began in 2007, when in response to requests from courts, the Judicial Council initiated a court information systems security policy framework that integrated best practices from representative trial courts, appellate courts, and Judicial Council staff into a reference document for use throughout the judicial branch.

The initial project was suspended in 2009 due to budget limitations, however focus resumed on this effort with the *Judicial Branch Strategic Plan for Technology (2014-2018)*. The Information Systems Controls Framework Template was published in August 2014 and the Judicial Council Technology Committee approved the Court Technology Advisory Committee Annual Plan on February 9, 2015 which outlined the work needed to facilitate the adoption of the Information Systems Controls Framework Template through the creation of the Information Security Framework Workstream.

Rationale for Recommendation

Information security is essential to ensure the proper operation and protection of information systems. The Information Security Framework Workstream includes information technology representatives from small, medium, and large courts from both northern and southern California as well as members of the Judicial Council staff. The following courts participated in the workstream: Humboldt, Marin, Monterey, Orange, Santa Barbara, Santa Clara, and Ventura. The workstream members identified specific sections of the Information Systems Controls Framework Template published by the Judicial Council that are most relevant to the trial courts. Of the 187 security controls in the Information Systems Controls Framework Template document, the workstream identified 84 that are most relevant to the trial courts. The "How to Use" guide acts as a reference for superior courts to assist them with establishing local policies and procedures. Because each court has unique local business requirements, superior courts are not required to implement the framework in its entirety, rather the intent is to encourage superior courts to use the framework as a template to develop local security policies appropriate for their environment. It is intended to be used as a guide, not a benchmark, of what should be done.

The Information Security Framework checklist provides courts with a simple tool to help individual courts assess their current information technology environment and determine an action plan. The checklist was piloted by the seven courts participating in the workstream.

Those courts determined that on average, about 75% of the items on the checklist have already been fully or partially implemented at those courts. Of the items that had not been implemented, courts estimated that it would take an "average" amount of effort to implement them (on a scale of "low", "average", "high" effort). The goal is not necessarily to have all courts implement all items 100%. The goal is for all courts to have assessed the areas in the checklist and determine if and when items need to be addressed. The individual court can then determine what they need to implement based upon the business requirements and resource constraints at their court.

Comments, Alternatives Considered, and Policy Implications

Comments were solicited from and received by superior court Presiding Judges, Court Executive Officers, Court Information Officers, and the Trial Court Presiding Judges Advisory Committee/Court Executive Advisory Committee Joint Technology Subcommittee. Overall feedback was positive and supportive. The main comments centered around the need to ensure that the "How to Use" guide was not a mandated policy that required implementation and that it would not be used as a benchmark for auditing purposes.

The Information Security Workstream considered creating an entirely separate document to describe specific information security controls for the superior courts. The workstream recognized that a separate document would duplicate a large portion of the already published Information Systems Control Framework Template. Therefore, the workstream decided to create the "How to Use" guide which focuses on highlighting the most relevant controls for superior courts.

There are no policy implications associated with this recommendation. However, the proposed documents are intended to support a local court in its creation of local information systems security policies.

Implementation Requirements, Costs, and Operational Impacts

Because each court differs in their local information security environment, policies, business requirements, and resource constraints, the recommended documents do not require, suggest, nor recommend that specific technologies or solutions be implemented. The "How to Use" guide focuses on subject areas that should be considered and it is up to the local court to decide what policies should be implemented and what tools or processes will be used to support those policies based upon what the local court can afford to implement.

Relevant Strategic Plan Goals and Operational Plan Objectives

The "How to Use" guide and "Information Security Framework checklist" support goal 3, Optimize Infrastructure, of the *Judicial Branch Strategic Plan for Technology (2014-2018).* In particular, they support objectives 3.1, Ensure secure and reliable data network connectivity throughout the branch and 3.2, Provide a consistent level of infrastructure security across the branch.

Attachments

1. "How to Use the Information Systems Controls Framework"

2. “Information Security Framework Checklist”

CALIFORNIA JUDICIAL BRANCH

How to Use the Information Systems Controls Framework

A Guide for the California Superior Courts

VERSION 1.3

SEPTEMBER 28, 2015

Table of Contents

1.0 Introduction 1
2.0 Information Systems Controls Framework 1
2.1 Scope 1
2.2 Organizational Characteristics 2
2.3 Documentation Structure 2
3.0 Purpose of Information Security 3
4.0 Information System Controls 4
5.0 Using the Framework 4
6.0 Recommended Controls for Superior Courts 6

1.0 INTRODUCTION

This "How to Use" guide acts as a reference for superior courts to assist them with establishing local policies and procedures based upon the Information Systems Controls Framework published by the Judicial Council. Since the framework was developed to establish a basic security approach at the branch level, this guide identifies the sections of the Information Systems Controls Framework that are most relevant to the superior courts. Superior courts are not required to implement the framework in its entirety, rather the intent is to encourage superior courts to use the framework as a template to develop security policies appropriate to their unique local business requirements. It is intended to be used as a guide, not a benchmark, of what should be done.

This guide is intended to provide a roadmap for courts and does not include all the details required for implementing specific local policies and procedures. Courts should refer to the complete framework document for specific recommendations and best practices.

2.0 INFORMATION SYSTEMS CONTROLS FRAMEWORK

2.1 SCOPE

The information systems controls framework has been developed for the establishment of a standard security approach within the Judicial Branch of California. In order to produce the framework, input was solicited from multiple courts ranging from small to large in size so that a comprehensive framework could be developed that is suitable to all entities within the judicial branch. The framework is designed to set a direction, identify and address areas of concern expressed by entities within the judicial branch, and to document policies and practices that can assist judicial branch entities with their concerns by providing a framework for creating entity-specific security policies and procedures.

The goals of the framework are:

- To suggest an overall information security policy, governance and compliance model for the judicial branch to leverage in building their security programs including roles, responsibilities, and major activities.
- To provide a holistic information security framework that the judicial branch entities can leverage in creating local policies.
- To provide guidance to all members of the judicial branch on the proper handling of sensitive information.
- To provide a basis for security training and educational awareness programs developed by judicial branch entities.

- To provide the basis for the development of implementation standards, procedures, and guidelines for each platform, operating system, application, and security device that can then be monitored and enforced against the policies defined in the framework.

2.2 ORGANIZATIONAL CHARACTERISTICS

The framework establishes how information is to be handled and secured within individual judicial branch entities, how it is exchanged between the judicial branch and local and state justice partners and with the public. Therefore, security controls (administrative and technical) related to access management are of particular importance.

2.3 DOCUMENTATION STRUCTURE

An information security program is supported by a collection of documentation capturing differing levels of detail while maintaining consistent guidance for all participants. The information security program will consist of the following categories of documents:

- **Organizational Policy** – Expresses management's expectations with regard to security and data protection. Generally limited to identification of base principles, roles and responsibilities, and the security framework. This framework provides the organizational policy for individual judicial branch entities.

- **Implementing Policy** – Further refines management's expectations; usually issued by a subordinate business or organizational unit for the purpose of interpreting the organizational policy to local entity practices. These policies will be developed as needed by the local entity.

- **Standards** – Identify specific hardware and software features and products whose use has been determined to be in support of policy. Standards may be established by local entities as needed to support policy objectives and to streamline operations.

- **Procedures** – Support standards and policy by providing step-by-step instructions for the execution of a security process. Judicial branch entities will develop and document procedures to ensure the quality and repeatability of security processes.

- **Guidelines** – Provide recommendations which can be used when other guidance has not been established. Guidelines are usually created at lower operational levels such as departments to address immediate needs until consensus is reached on broader direction.

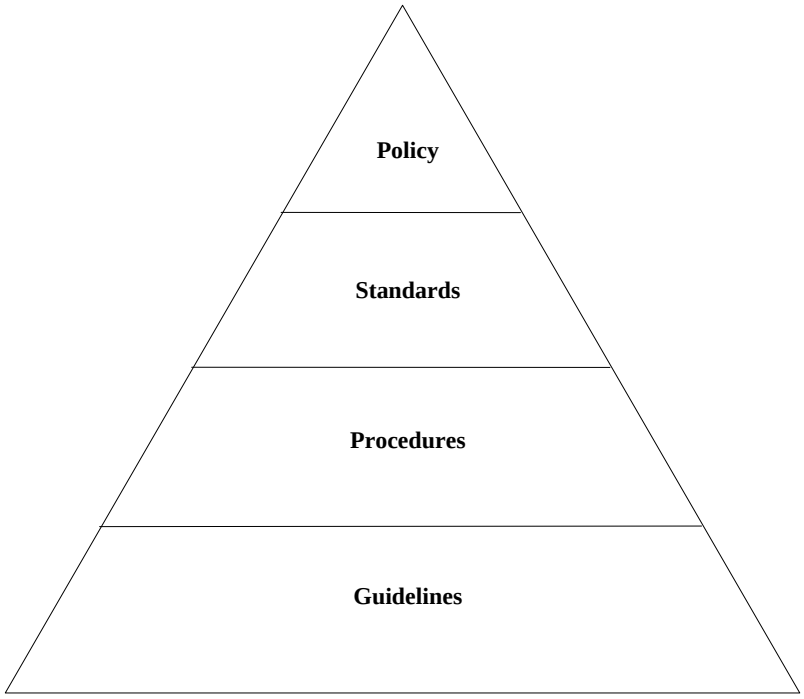


Figure 1: Security Documentation Hierarchy

3.0 PURPOSE OF INFORMATION SECURITY

Information and the supporting processes, systems, and networks are important assets. Defining, achieving, maintaining, and improving information security may be essential to maintain legal compliance, confidentiality, integrity, and availability of information and systems.

Judicial branch entities and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage (such as malicious code, computer hacking, and denial of service attacks) have become more common, more ambitious, and increasingly sophisticated.

Many information systems have not been designed with security in mind. The security that can be achieved through technical means is limited, and should be supported by appropriate management policies and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, at a minimum, participation by all employees in the branch. It may also require participation from local and state justice partners, the public suppliers, third parties, contract labor, or other external parties. Information Security is a continually evolving area and courts are encouraged to stay informed and educated on current topics and ensure security policies are up to date. Although there is no requirement, it is also a best practice to establish an escalation path to ensure that incidents receive the proper attention based on severity and are processed in a timely manner.

4.0 INFORMATION SYSTEM CONTROLS

Information is an asset, which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Judicial branch entities, as part of their on-going program to maintain adequate and effective controls, want to ensure that the Information Systems - the devices, operating systems, applications, and the sensitive and confidential information - are adequately protected from the risk of loss due to:

- Intentional acts by third-parties inside or outside the organization.
- Inappropriate access by individuals or groups untrained in correct local policies or procedures.
- Accidental loss of a portable device containing confidential information.
- Accidents, natural disasters, or other force majeure.

The document entitled Information Systems Controls Framework, published 08/12/2014 shall serve as the official information security document for the California judicial branch. This framework represents "best practices" and is recommended as a security framework to be used by all judicial branch entities.

5.0 USING THE FRAMEWORK

The Information Systems Controls Framework published by the Judicial Council provides a model that courts can leverage. Superior courts are not required to implement the recommendations contained in the framework but they are encouraged to leverage the framework as appropriate for their unique local business requirements. The framework provides context for a court's local IT security policies. The framework is designed to be modular so that courts can refer only to the sections that are relevant to them. The framework does not recommend any specific technologies that should be implemented nor is the framework of set of policies required for audit compliance.

A local court can utilize the framework and this "how to use" guide in the following manner:

1. Review this "how to use" guide and determine which of the "Recommended Controls for Superior Courts" listed in the next section are relevant to the court's local business environment.
2. The local court then decides what their local policy will be.
3. The local court identifies options for implementing the policy.
4. The local court determines if resources exist to implement the local policy.

Even if there are not enough resources to implement the local policy, steps 1-3 are still useful for documenting a roadmap and plan for when resources become available.

Here is a non-IT example of how the framework could be used:

Domain: Physical Security		
	Recommendation	Source of Recommendation
Step 1: Determine relevant control	Court facilities should be secure	Framework
Step 2: Set local policy	Non-public accessible areas can only be entered through a locked entrance	Local court
Step 3: Identify implementation options	Option 1: Install locks with physical keys Option 2: Install keypad lock Option 3: Install locks with card key readers	Local court
Step 4: Determine available resources	Available resources can only support Option 1.	Local court

Here is an IT example of how the framework could be used:

Domain: Access Control for Mobile Devices		
	Recommendation	Source of Recommendation
Step 1: Determine relevant control	Establish mobile device security policy	Framework
Step 2: Set local policy	▪ Mobile devices must enforce a lock screen PIN. ▪ Only email and calendar synchronization allowed. ▪ Direct access to court network and other court applications prohibited.	Local court
Step 3: Identify implementation options	Option 1: Court IT configures court mobile devices per policy Option 2: Software and configuration settings downloaded by end-user Option 3: Mobile device management software manages device remotely	Local court
Step 4: Determine available resources	No resources available to implement at this time.	Local court

6.0 RECOMMENDED CONTROLS FOR SUPERIOR COURTS

The following chart summarizes the sections of the Information Systems Controls Framework (ISCF) that are most relevant to the superior courts. Courts are encouraged to review the entire framework to determine if other sections could apply to their local business environment.

Each section has been categorized to indicate the primary focus for each section:

- Process – this item generally involves the implementation of a business process if one does not already exist
- Policy – this item generally involves the creation of a policy if one does not already exist
- Technical – this item generally involves the implementation or configuration of technology

Some sections may involve multiple categories of activity. In those cases, the section has been categorized based upon the primary focus for that area.

When creating a set of local IT policies, courts can decide if they prefer to have a single document that contains all the selected sections relevant to their local environment or if they prefer to publish individual policy documents for a particular section or group of sections. Individual documents may make it easier to update a particular section without the need to republish the entire policy document while a single document can used as an all-inclusive publication.

ISCF Section	Title	Summary	Category
Program Management			
4.2	Senior Information Security Officer	Identify someone in the organization that has responsibility for IT security.	Process
4.5	Information System Inventory	Maintain an inventory of information systems.	Process
4.8	Critical Infrastructure Plan	Document critical IT infrastructure and key resources.	Process
4.15	Contacts with Security Groups and Associations	Establish contact with the security community.	Process
Access Control			
5.1	Access Control Policy and Procedures	Document an access control policy.	Policy
5.2	Account Management	Identify account managers and create, modify, and disable system accounts based on authorized access	Process
5.3	Access Enforcement	Enforce system access	Process
5.4	Information Flow Enforcement	Manage the flow of information between systems	Technical
5.6	Least Privilege	Provide only necessary access	Process

5.7	Unsuccessful Logon Attempts	Enforce a limit of invalid logon attempts when appropriate	Technical
5.8	System use Notification	Display logon message that displays privacy and security notices	Technical
5.9	Concurrent Session Control	Limit the number of concurrent session when appropriate	Technical
5.10	Session Lock	Automatically lock session after a defined period	Technical
5.11	Session Termination	Automatically terminate session when appropriate	Technical
5.12	Permitted Actions Without Identification or Authentication	Document actions that can be performed without identification or authentication	Technical
5.13	Remote Access	Establish remote access security policy	Policy
5.14	Wireless Access	Establish wireless access security policy	Policy
5.15	Access Control for Mobile Devices	Establish mobile device security policy	Policy
5.16	Use of External Information Systems	Establish policy for accessing non-Court systems	Policy
5.17	Information Sharing	Establish information distribution rules (e.g. confidential, public, etc.)	Policy
5.18	Publicly Accessible Content	Determine who can publish publicly accessible information	Policy
Awareness and Training			
6.1	Security Awareness and Training Policy and Procedures	Determine how to provide security training and information to personnel	Process
Audit and Accountability			
7.1	Audit and Accountability Policy and Procedures	Determine policy for managing audit information	Policy
7.2	Audit Events	Identify key audit data (e.g. log files)	Technical
7.3	Content of Audit Records	System should generate audit information when appropriate	Technical
7.4	Audit Storage Capacity	Ensure enough capacity for storing audit data	Technical
7.5	Response to Audit Processing Failures	Ensure system audit function is performing	Technical
7.6	Audit Review, Analysis, and Reporting	Review audit data regularly	Process
7.7	Audit Reduction and Report Generation	Ensure ability to generate audit reports	Technical
7.8	Time Stamps	Ensure audit records are time stamped	Technical
7.9	Protection of Audit Information	Ensure authorized access to audit records	Technical
7.10	Non-Repudiation	Ensure validity of audit data cannot be challenged	Technical
7.11	Audit Record Retention	Determine retention period for audit records	Policy

7.12	Audit Generation	Ensure systems generate audit records when required	Technical
Security Assessment and Authorization			
8.3	System Interconnections	Document connections to other systems	Technical
Configuration Management			
9.1	Configuration Management Policy and Procedures	Document roles for managing system configuration	Process
9.2	Baseline Configuration	Document baseline configuration	Process
9.3	Configuration Change Control	Document changes to the system	Process
9.4	Security Impact Analysis	Determine if system changes will impact security	Process
9.5	Access Restrictions for Change	Determine how to restrict system changes	Process
9.6	Configuration Settings	Document key configuration settings	Technical
9.7	Least Functionality	Configure system to provide only essential capabilities	Technical
9.8	Information System Component Inventory	Develop information systems inventory	Process
9.10	Software Usage Restrictions	Ensure software use is consistent with use contract	Process
9.11	User-Installed Software	Establish policy for user-installed software	Policy
Contingency Planning			
10.1	Contingency Planning Policy and Procedures	Document policy for maintaining contingency plan	Policy
10.2	Contingency Plan	Document information system contingency plan (e.g. Continuity of Operations Plans, COOP)	Process
10.3	Contingency Training	Provide contingency training	Process
10.4	Contingency Plan Testing	Test the contingency plan	Process
10.5	Alternate Storage Site	Establish alternate storage site for system backups	Process
10.7	Telecommunications Services	Establish alternate telecommunications services if possible	Technical
10.8	Information System Backup	Conduct system backups	Technical
10.9	Information System Recovery and Reconstitution	Ensure ability to restore from backup	Technical
Identification and Authentication			
11.1	Identification and Authentication Policy and Procedures	Establish identification and authentication policy	Policy
11.2	Identification and Authentication (Organizational Users)	System uniquely identifies and authenticates users acting on behalf of the court	Technical
11.3	Device Identification and Authentication	System uniquely identifies and authenticates devices	Technical
11.4	Identifier Management	Manage device and user names	Technical

11.5	Authenticator Management	Manage authenticators (e.g. passwords, tokens)	Technical
11.6	Identification and Authentication (Non-Organizational Users)	System uniquely identifies and authenticates users who do not act on behalf of the court	Technical
Media Protection			
14.1	Media Protection Policy and Procedures	Establish system media protection policy (e.g. tape, disc)	Policy
14.2	Media Access	Determine who has access to system media	Process
14.3	Media Marking	Mark media for identification and protection	Process
14.4	Media Storage	Protect and store media	Process
14.5	Media Transport	Protect and track media during transport	Process
14.6	Media Sanitization	Sanitize media prior to disposal	Technical
14.7	Media Use	Identify any prohibited media (e.g portable storage)	Policy
Physical and Environmental Protection			
15.1	Physical and Environmental Protection Policy and Procedures	Establish policy for physical environment where information systems are located	Policy
15.2	Physical Access Authorizations	Develop list of individuals who have authorized physical access to information systems	Process
15.3	Physical Access Control	Ensure physical access to information systems is controlled	Technical
15.4	Access Control for Transmission Medium	Ensure physical access to data transmission systems is controlled	Technical
15.6.	Monitoring Physical Access	Enable physical access monitoring	Technical
15.7	Visitor Access Records	Document visitor access to facilities where information systems reside	Process
15.8	Power Equipment and Cabling	Protect power equipment and cabling from damage	Process
15.9	Emergency Shutoff	Provide the capability of shutting off power in emergency situations	Technical
15.13	Temperature and Humidity Controls	Maintain appropriate temperature and humidity levels at information systems facilities	Technical
15.15	Delivery and Removal	Control delivery and removal of information system components to and from the facility as appropriate	Process
15.16	Alternate Work Site	Document information systems requirements, if any, when an alternate work site is used during contingency operations	Process
15.17	Location of Information System Components	Place information systems to minimize potential damage	Process
System and Information Integrity			
21.3	Malicious Code Protection	Employ malicious code protection (e.g. anti-virus)	Technical
21.4	Information System Monitoring	Monitor information systems	Technical

21.5	Security Alerts, Advisories, and Directives	Receive information system security alerts	Process
21.6	Security Function Verification	Control ability to startup, shutdown, and restart systems	Technical
21.8	Spam Protection	Employ spam protection mechanism	Technical
Policy Exceptions			
22.1	Policy Exceptions	Exceptions to published local policies at the discretion of the court CIO or equivalent.	Process

ISCF Section	Title	Summary	Category	Relevant to this court? (Y/N)	Implemented? (Fully, Partially, No, Not Planned)	If not implemented, how difficult to implement? (Easy, Average, Difficult)	Comments
4.2	Senior Information Security Officer	Identify someone in the organization that has responsibility for IT security.	Process				
4.5	Information System Inventory	Maintain an inventory of information systems.	Process				
4.8	Critical Infrastructure Plan	Document critical IT infrastructure and key resources.	Process				
4.15	Contacts with Security Groups and Associations	Establish contact with the security community.	Process				
5.1	Access Control Policy and Procedures	Document an access control policy.	Policy				
5.2	Account Management	Identify account managers and create, modify, and disable system accounts based on authorized access	Process				
5.3	Access Enforcement	Enforce system access	Process				
5.4	Information Flow Enforcement	Manage the flow of information between systems	Technical				
5.6	Least Privilege	Provide only necessary access	Process				
5.7	Unsuccessful Logon Attempts	Enforce a limit of invalid logon attempts when appropriate	Technical				
5.8	System use Notification	Display logon message that displays privacy and security notices	Technical				
5.9	Concurrent Session Control	Limit the number of concurrent session when appropriate	Technical				
5.10	Session Lock	Automatically lock session after a defined period	Technical				
5.11	Session Termination	Automatically terminate session when appropriate	Technical				
5.12	Permitted Actions Without Identification or Authentication	Document actions that can be performed without identification or authentication	Technical				
5.13	Remote Access	Establish remote access security policy	Policy				
5.14	Wireless Access	Establish wireless access security policy	Policy				
5.15	Access Control for Mobile Devices	Establish mobile device security policy	Policy				
5.16	Use of External Information Systems	Establish policy for accessing non-Court systems	Policy				
5.17	Information Sharing	Establish information distribution rules (e.g. confidential, public, etc.)	Policy				
5.18	Publicly Accessible Content	Determine who can publish publicly accessible information	Policy				
6.1	Security Awareness and Training Policy and Procedures	Determine how to provide security training and information to personnel	Process				
7.1	Audit and Accountability Policy and Procedures	Determine policy for managing audit information	Policy				
7.2	Audit Events	Identify key audit data (e.g. log files)	Technical				
7.3	Content of Audit Records	System should generate audit information when appropriate	Technical				
7.4	Audit Storage Capacity	Ensure enough capacity for storing audit data	Technical				
7.5	Response to Audit Processing Failures	Ensure system audit function is performing	Technical				
7.6	Audit Review, Analysis, and Reporting	Review audit data regularly	Process				
7.7	Audit Reduction and Report Generation	Ensure ability to generate audit reports	Technical				
7.8	Time Stamps	Ensure audit records are time stamped	Technical				
7.9	Protection of Audit Information	Ensure authorized access to audit records	Technical				
7.10	Non-Repudiation	Ensure validity of audit data cannot be challenged	Technical				
7.11	Audit Record Retention	Determine retention period for audit records	Policy				
7.12	Audit Generation	Ensure systems generate audit records when required	Technical				
8.3	System Interconnections	Document connections to other systems	Technical				
9.1	Configuration Management Policy and Procedures	Document roles for managing system configuration	Process				
9.2	Baseline Configuration	Document baseline configuration	Process				
9.3	Configuration Change Control	Document changes to the system	Process				
9.4	Security Impact Analysis	Determine if system changes will impact security	Process				
9.5	Access Restrictions for Change	Determine how to restrict system changes	Process				
9.6	Configuration Settings	Document key configuration settings	Technical				
9.7	Least Functionality	Configure system to provide only essential capabilities	Technical				
9.8	Information System Component Inventory	Develop information systems inventory	Process				
9.10	Software Usage Restrictions	Ensure software use is consistent with use contract	Process				
9.11	User-Installed Software	Establish policy for user-installed software	Policy				

ISCF Section	Title	Summary	Category	Relevant to this court? (Y/N)	Implemented? (Fully, Partially, No, Not Planned)	If not implemented, how difficult to implement? (Easy, Average, Difficult)	Comments
10.1	Contingency Planning Policy and Procedures	Document policy for maintaining contingency plan	Policy				
10.2	Contingency Plan	Document information system contingency plan (e.g. Continuity of Operations Plans, COOP)	Process				
10.3	Contingency Training	Provide contingency training	Process				
10.4	Contingency Plan Testing	Test the contingency plan	Process				
10.5	Alternate Storage Site	Establish alternate storage site for system backups	Process				
10.7	Telecommunications Services	Establish alternate telecommunications services if possible	Technical				
10.8	Information System Backup	Conduct system backups	Technical				
10.9	Information System Recovery and Reconstitution	Ensure ability to restore from backup	Technical				
11.1	Identification and Authentication Policy and Procedures	Establish identification and authentication policy	Policy				
11.2	Identification and Authentication (Organizational Users)	System uniquely identifies and authenticates users acting on behalf of the court	Technical				
11.3	Device Identification and Authentication	System uniquely identifies and authenticates devices	Technical				
11.4	Identifier Management	Manage device and user names	Technical				
11.5	Authenticator Management	Manage authenticators (e.g. passwords, tokens)	Technical				
11.6	Identification and Authentication (Non-Organizational Users)	System uniquely identifies and authenticates users who do not act on behalf of the court	Technical				
14.1	Media Protection Policy and Procedures	Establish system media protection policy (e.g. tape, disc)	Policy				
14.2	Media Access	Determine who has access to system media	Process				
14.3	Media Marking	Mark media for identification and protection	Process				
14.4	Media Storage	Protect and store media	Process				
14.5	Media Transport	Protect and track media during transport	Process				
14.6	Media Sanitization	Sanitize media prior to disposal	Technical				
14.7	Media Use	Identify any prohibited media (e.g portable storage)	Policy				
15.1	Physical and Environmental Protection Policy and Procedures	Establish policy for physical environment where information systems are located	Policy				
15.2	Physical Access Authorizations	Develop list of individuals who have authorized physical access to information systems	Process				
15.3	Physical Access Control	Ensure physical access to information systems is controlled	Technical				
15.4	Access Control for Transmission Medium	Ensure physical access to data transmission systems is controlled	Technical				
15.6.	Monitoring Physical Access	Enable physical access monitoring	Technical				
15.7	Visitor Access Records	Document visitor access to facilities where information systems reside	Process				
15.8	Power Equipment and Cabling	Protect power equipment and cabling from damage	Process				
15.9	Emergency Shutoff	Provide the capability of shutting off power in emergency situations	Technical				
15.13	Temperature and Humidity Controls	Maintain appropriate temperature and humidity levels at information systems facilities	Technical				
15.15	Delivery and Removal	Control delivery and removal of information system components to and from the facility as appropriate	Process				
15.16	Alternate Work Site	Document information systems requirements, if any, when an alternate work site is used during contingency operations	Process				
15.17	Location of Information System Components	Place information systems to minimize potential damage	Process				
21.3	Malicious Code Protection	Employ malicious code protection (e.g. anti-virus)	Technical				
21.4	Information System Monitoring	Monitor information systems	Technical				
21.5	Security Alerts, Advisories, and Directives	Receive information system security alerts	Process				
21.6	Security Function Verification	Control ability to startup, shutdown, and restart systems	Technical				
21.8	Spam Protection	Employ spam protection mechanism	Technical				
22.1	Policy Exceptions	Exceptions to published local policies at the discretion of the court CIO or equivalent.	Process				

The Judicial Council proposes a one-time General Fund augmentation for FY 2016/17, FY 2017/18, and FY 2018/19 for transfer to the Trial Court Trust Fund to replace V3 with a vendor-supplied CMS in the California Superior Courts of Orange, Sacramento, San Diego, and Ventura Counties.

These courts have made substantial contributions to the development of a CMS intended for use by all superior courts. The project to deploy this statewide system was terminated in March 2012, leaving these four courts with an aging civil CMS that cannot be improved without legislative approval.

Because of a projected deficit in the State Trial Court Improvement and Modernization Fund (IMF), and taking into consideration a court survey conducted by the Trial Court Budget Advisory Committee in preparation for the FY 2015/16 budget, the Judicial Council determined a need to eliminate funding from the IMF for V3. Therefore, by July 2019, the four identified courts will be responsible for self-funding their CMSs.

V3 is a robust application that automates processing for the civil, small claims, probate, and mental health case types and is used to manage approximately 25% of these cases statewide. However, the cost to maintain and support V3 is comparatively high for use in just four courts. Consequently, these courts have determined that replacing V3 with a vendor-supplied CMS will be more cost-effective.

More importantly, action by the California State Legislature in July 2012, Senate Bill 1021 (Stats. 2012, ch. 41), prohibits the Judicial Council from expending any funds on the statewide CMS without the Legislature's consent, except for maintenance and operation of the V2 and V3 CMSs (Government Code, section 68085(o)). This effectively prohibits the Judicial Council from making significant improvements to V3 and impacts the V3 courts' ability to manage and process cases more effectively and efficiently. In effect, V3 is a legacy system.

In 2013, the courts participated in a statewide effort to evaluate and develop master services agreements with judicial CMS vendors. Three vendors were selected: Thomson-Reuters, Tyler Technologies, and Justice Systems Incorporated. Each of the four courts on V3 has selected a single system vendor from among those three that best fits their needs for all of their case types. The Orange, San Diego, and Ventura County courts have selected Odyssey from Tyler Technologies. Sacramento County court has selected C-Track from Thomson-Reuters.

The V3 courts worked with Tyler Technologies (Orange County court) and Thomson-Reuters (Sacramento County court) to perform comparisons of the functionality of the Odyssey and C-Track CMSs against V3. Functional gaps were identified in the vendor CMSs that should be remediated to ensure that the courts retain their current efficiency. Additionally, these changes

would benefit all courts implementing these new CMSs (a total of 29 superior courts to date), as the improvements would be available at no additional licensing or development cost from the vendors.

Although ongoing support costs for a vendor CMS would be lower, neither the judicial branch nor the courts are able to support the one-time deployment costs.

Three alternatives have been analyzed for this proposal:

1. Alternative One (Recommended Solution): Deploy a vendor CMS to replace V3. Remediate functional gaps in vendor CMS functionality as compared to V3.

   The deployment costs in this scenario are high; however, ongoing costs are lowest of the three alternatives. In addition, this alternative enables the courts to work with the vendor to continue to improve the new CMSs.

2. Alternative Two (Status Quo): Courts continue to use V3.

   There is no deployment cost. However, total ongoing costs are very high, in part because V3 was initially architected to support a large number of courts. In addition, the Judicial Council is effectively prohibited from improving V3 and cannot expand use of V3 beyond the four courts without approval from the Legislature.

3. Alternative Three: Deploy a vendor CMS, base product. Functional gaps not remediated.

   The deployment cost in this scenario is lower than Alternative 1. However, ongoing costs are almost as high as Alternative 2, as the courts will see declines in efficiency and operational productivity. This will necessitate hiring additional operations staff or accepting the inevitable increase in backlogs.