Electronic Recording
OPERATING PROCEDURES

A Tradition of Stewardship
A Commitment to Service

NAPA COUNTY RECORDER DIVISION
900 COOMBS ST. RM 116
NAPA, CA. 94559

UPDATED: NOVEMBER 8, 2017

1.0—WELCOME

Welcome from John Tuteur

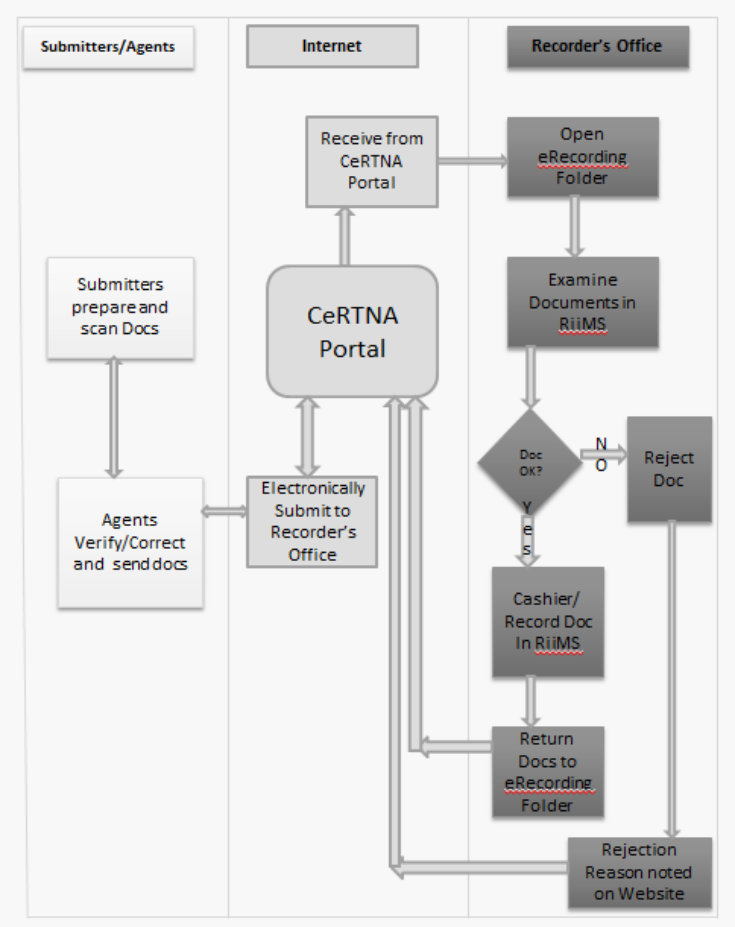
Welcome to the Napa County Recorder Division Electronic Recording and Delivery System (ERDS.) Electronic recording is the electronic submission of official documents for recording from an outside source to the Recorder Division. Electronic recording is a logical progression in our ongoing effort to provide the best service possible. We are confident that both the County Recorder and the Submitters and Agents who take advantage of this enhanced service will experience both improved performance and reduced cost in carrying out document recording.

John Tuteur
Assessor-Recorder-County Clerk

2.0—OVERVIEW OF ELECTRONIC RECORDING

Electronic Recording (ER) is a process that provides the capability of submitting documents electronically from the Submitting Organization to the Napa County Recorder Division.

2.1—ELECTRONIC RECORDING FLOWCHART
2.2—THE ELECTRONIC RECORDING PROCESS



2.2.1—The Process for Electronic Recording is simple. Once the documents are ready to be recorded, the Submitting Organization:

- Prepares the documents for scanning,
- Scans the documents and enters minimal information,
- Verifies/corrects any scanning errors, and
- Submits the documents to the Recorder Division electronically.

The original documents never leave the Submitter's office.

2.2.2—At the Recorder Division: The Recorder:

- Allocates document numbers, if the Submitter has chosen to record at 8:00 am, or other times, otherwise document numbers are assigned as live sets,
- Examines the documents for recording requirements,
    - Documents which meet the recording requirements:
        - Enter the cashiering information, and
        - Record the documents
    - Documents which do NOT meet the recording requirements:
        - Reject the document and note the reject reason(s) online
- Recording information is immediately available on the CeRTNA Website for all authorized Submitter employees to access.

2.2.3—At the Submitter's Office, after the documents have been recorded or rejected:

- If the documents met the recording requirements:
    - The first page of each document (face sheet) with the recording information is ready to be printed in the Submitter's office
    - The face sheet is attached to the original document and is mailed to the person named on the document.
- If the documents were rejected:
    - The reason for rejection is noted for all rejections so that the problem/deficiency can be corrected.
    - After the problem/deficiency is corrected, the document is resubmitted. As the Submitter has the original document, the turn-around for this re-submission can be very quick.

- Upon recording, information (document number, time recorded, fees, etc.) is immediately posted on the CERTNA website for access by all authorized Submitter employees.

Formatted: Font color: Auto

3.0—BENEFITS

The benefits of using this process for submitters can be significant:

- The documents never leave your office; they are always under your complete control. This lessens the possibility of lost or misplaced documents.
- You are immediately notified of recorded or rejected documents, allowing productivity in your office to improve by giving you the capability to immediately react to the situation. No more waiting for documents to go back and forth between your office and the Recorder Division.
- You have the ability to monitor and track all documents through the process of recording. This tracking gives you up-to-the-minute information regarding the time the submission was received by the Recorder Division, the time it was recorded, the fees involved, and notification of and reason for a rejected document.
- Rejected documents can immediately be corrected and re-submitted. There is no waiting for the paper documents to be returned to your office before they can be re-submitted.
- The documents can be submitted between 8 a.m. and 3 p.m on regular business days..
- With each batch submitted, your office has the choice of submitting documents for an 8:00 AM recording, or of submitting documents for recording throughout the day.
- The recording process, from beginning to end, operates much faster for both offices.
- There is no need to transport, sometimes from long distances, documents from your office to the Recorder Division.

- The recording costs can actually be less:
    - Prior to submission, you can eliminate pages scanned in error. For example, stamps on some documents “bleed through” to the other side of the paper. The scanner senses there is something on the page, and so creates an image. These can be deleted in your office prior to there being a recording charge. “DO NOT RECORD” pages may be removed if the Submitter wishes, thereby eliminated a recording charge for those pages.
    - Issues are addressed at the “front” of the process, rather than at the “back end”, after Recording fees have been assessed.

- As rejections can be easily tracked and evaluated, your office may find ways to lessen the number of rejections. For example, if your office has a high number of rejections due to illegible notary seals, you may decide to implement new internal procedures to correct this.

- Document transportation costs and time involved are lessened and/or eliminated.

Live recordings are available in Electronic Recording only.

Live recording hours are from 8:00 am to 3:00 pm daily.

Blanks or fillers to replace rejected documents in Electronic Recording batches will be charged a regular recording fee if numbers have been preassigned to the batch.

4.0—ROLES AND RESPONSIBILITIES

Both the Napa County Recorder Division and the Submitter play a vital and active role in the success of this electronic recording system. It is essential that the procedure for electronic recording is consistent with all applicable laws, regulations, standards, and procedures used in the conventional method of recording. Failure to comply may result in the revoking of the privilege of using electronic recording.

4.1—SUBMITTER

The Submitter will:

- Execute ~~a~~ Unified Memorandum of Understanding (MOU) with the Recorder Division VIA AGENT and CeRTNA. ~~.~~
- Ensure only original documents are scanned and submitted. These documents must bear original signatures and notary seals, except as provided by law.
- Ensure the integrity of all notary acknowledgments. Acknowledgments must have original signatures and seals and must not be cut and pasted onto the document.
- Safeguard the integrity and security of the electronic recording operational system by preventing fraud and deceit in recording.
- Ensure that all users of the system have been authorized to do so by the County Recorder Division and that user access will be modified only by the Recorder Division.
- Verify that no unauthorized users be permitted to access or use the system at any time.
- Appoint a Security Liaison who is authorized to request changes to add/delete user access to the system.
- Immediately notify the County Recorder Division when an individual that has access to the system is no longer employed by your office or is no longer authorized to use the system so that the Recorder Division can remove that person's access rights.
- Establish and enforce procedures to safeguard user ID's and passwords. This should include periodically changing passwords.
- Notify the County Recorder Division within one (1) working day, in writing and by telephone of any problems or potential problems that could affect the quality of the work, services, or performance levels.

- Perform the functions of document scanning preparation, scanning, and entering data for transmitting the documents.
- Perform the functions of online viewing of recording information, and distributing document face sheets.
- Return recorded original documents to applicable parties with a copy of the first recorded page affixed thereto as a new cover page.
- Verify staff has the required basic skills prior to training. These skills include:
  - Basic Windows PC skills, including the operation of a mouse.
  - Ability to operate a web browser; in particular: Internet Explorer.
- Provide first level technical support for Submitter's staff on hardware, software, and use of the system.
- Provide up-to-date anti-virus protection on all PC's connected to the electronic recording system.
- Support and maintain the hardware and software, including up-to-date patches.
- Promptly install/apply enhancements/changes to all necessary PC's upon instruction from the Recorder Division.
- Provide physical access of the electronic recording equipment to the Recorder Division upon request.
- Provide Internet access for the stations using this system.
- Ensure that only those software applications which are pre-approved by the Recorder are installed on the scanning workstation.
- Ensure that all software applications are updated and that any conflicts with software/hardware are resolved.
- Only submit documents through an approved CERTNA Agent

4.2—RECORDER DIVISION

The Recorder Division will:

- Examine and record electronic documents under the same criteria, statute, and regulations as that of paper submission.
- Provide timely confirmation of recordings, rejections, and fees.
- Recorder Division to retain ownership of the electronic recording software.

- Be responsible for and provide to the Submitter, via CERTNA or the Agent, all upgrades, modifications, or enhancements to the electronic recording software.

4.3—CeRTNA

The California Electronic Recording Transaction Network Authority (CeRTNA) is the legal entity established to govern the California Electronic Recording Transaction Network. It is established as a Joint Powers Authority, enabling member counties to collectively govern.

4.3.1—CeRTNA User Counties

As of the time of publishing, CeRTNA User counties include the following (in alphabetical order):

- Butte County
- Contra Costa
- El Dorado
- Fresno County
- Kern County
- Merced
- Monterey
- Napa
- Sacramento
- San Bernardino County
- San Francisco County
- San Joaquin
- San Luis Obispo
- Santa Clara County
- Santa Cruz County
- Shasta County
- Sonoma
- Tehama

Formatted: Bulleted + Level: 1 + Aligned at: 0.53" + Indent at: 0.78"

4.3.2—THE CeRTNA Portal

- The California Electronic Recording Transaction Network Portal is the Electronic Recording Delivery System built by CeRTNA. The CeRTNA Portal is authorized by the Electronic Recording Delivery Act of 2004.

4.4—AGENTS

A representative – and his/her employees who are authorized by CERTNA to submit documents on behalf of an Authorized Submitter. Agents deliver, and, when applicable, return the submitted payloads via an Electronic Recording Delivery System (ERDS). An Agent may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software.

5.0—GETTING STARTED

The following is a checklist to outline the steps necessary for preparing and enabling a Submitter to participate in Electronic Recording.

5.1—SUBMITTER PROVISIONING CHECKLIST

MILESTONES:

1. Select an Agent
2. Receive Electronic packet, Unified MOU, and Declaration from Agent
3. Return completed and signed MOU and Declaration to Agent
4. Receive confirmation of signed Unified MOU by ~~County Recorder~~CeRTNA Executive Director after submission to ~~Recorder~~CeRTNA by Agent
5. Select Secure Access individuals
6. Selected individuals complete the following forms:
    a. Live Scan
    b. ERDS Form 12 (Acknowledgment of Responsibilities)
7. Selected individuals are Live Scanned at a location chosen by the Submitter. Return selected individual scanned Live Scan copies and signed ERDS Form 0012 to CERTNA (Agent?)
8. Selected individuals cleared by ERDS program receive user accounts, passwords, and Security Tokens from CERTNA

9. Receive Technical Contact from CERTNA and Agent
10. Develop internal policies and procedures
11. Provision equipment per workstation requirements
12. Coordinate equipment testing with CERTNA and Agent
13. Attend necessary training provided by CERTNA or Agent
~~13.~~14. Agent to set up ACH payment with Recorder.
~~14.~~15. Go Live with CeRTNA

6.0—DECLARATION

6.1—INSTRUCTIONS

Complete the Declaration form in Section 15.1 and return it as soon as possible to the AGENT along with your MOU.

7.0—MOU/DECLARATION

The Unified Memorandum of Understanding (MOU) and Declaration used by the Napa County Recorder will be delivered to Authorized Submitters by their Agent.

7.1—INSTRUCTIONS

- The agent coordinates obtaining the appropriate signed originals and copies of the Unified MOU from the Submitters and forwards to the CeRTNA Executive Director for approval. The CeRTNA Executive Director communicates to Counties those newly approved submitters for specific agents.~~The Submitter will complete and sign TWO copies of the Electronic Recording Memorandum of Understanding (MOU), and one original signed copy of the Declaration.~~
- ~~The MOU should be considered carefully; it outlines the specific requirements expected of the Submitter by Certna, Agent and RecorderThe Submitter delivers both of the forms to the Agent.~~
- ~~The Recorder receives a copy of the MOU from the AGent.~~
- ~~One of the originals is kept by the Agent, and one of the original MOU's is returned to the Submitter by the Agent.~~

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

7.2—WHAT HAPPENS NEXT?

- Shortly thereafter, the Submitter will be contacted by the Agent and CERTNA to set up the security workstation, accounts, payment methods, training sessions, and begin the electronic recording process.

8.0—ACCOUNTS

Under Government Code 27391(b), only Title Insurers (Insurance Code 12340.4), Underwritten Title Companies (Insurance Code 12340.5), Institutional Lenders (Financial Code Section 50003 Subdivision J Paragraphs 1, 2, and 4), or government agencies are eligible for Electronic Recording.

8.1—METHODS OF PAYMENT

Only ACH (Automated Clearing House) payments are accepted from Agents on behalf of submitters

ACH Payments for any given business day's transactions must be received by the county within 48 hours.

Formatted: Font color: Auto

9.0—EMPLOYEE SELECTION GUIDELINES

9.1—TABLE OF DISQUALIFYING OFFENSES

9.2.1—Text of the Law

Title 11, Division 1, Chapter 18, Article 4, Section 999.121:

"If the state or federal criminal records contain a conviction of a felony, or a misdemeanor related to theft, fraud, or a crime of moral turpitude, or a pending criminal charge for any of these crimes shall be justification for denial to an individual to serve in an ERDS role that requires fingerprinting. A plea of guilty or no contest, a verdict resulting in conviction, or the forfeiture of bail, shall be a conviction pursuant to Government Code section, 27395(a), irrespective of a subsequent order under section 1203.4 of the Penal Code. All other state or federal criminal records containing a felony or misdemeanor conviction involving dishonesty, fraud or deceit, 'moral turpitude' [People v. Castro (1985) 38 Cal. 3d 301], including pending charges, shall be justification for denial to an individual to serve in an ERDS role that requires fingerprinting."

9.2.2—Felony Conviction/Pending Charges

A felony conviction or pending charges involving the following offenses shall be justification for denial:

• Homicide	• Forgery
• Robbery	• Arson
• Assault	• Drugs (Sale of)
• Kidnapping	• Sex
• Burglary	• Driving under the Influence
• Theft	• Hit and Run
• Motor Vehicle Theft	• Weapons
• Escape	• Bookmaking
• Identity Theft	• Unauthorized Access to Computers

9.2.3—Misdemeanor Conviction/Pending Charges

A misdemeanor conviction or pending charges involving the following offenses shall be justification for denial:

• Misdemeanor manslaughter	• Liquor Laws
• Assault and Battery	• Disturbing the Peace
• Theft	• Malicious Mischief

• Drugs (Sale of)	• Driving under the Influence
• Sex	• Gambling
• Checks and Access Cards	• Trespassing
• Vandalism	• Contributing to the delinquency of a minor
• Identity Theft	• Unauthorized Access to Computers

9.3—LIVE SCAN INSTRUCTIONS (to be handled by Agent)

9.4—USER MANAGEMENT (Overseen by Agent and Certna)

According to the MOU signed between the Submitter and the County Recorder, it is the responsibility and duty of the Submitter to complete these forms with their Agent as soon as possible upon any staff changes in order to maintain the highest level of security in the system.

10.0—TECHNICAL REQUIREMENTS

10.1—HARDWARE

Refer to CeRTNA Website for further information regarding hardware requirements and recommendations:

http://www.certnportal.com/home.html

10.2—WORKSTATION SECURITY REQUIREMENTS

For all ERDS that serve both Type 1 or Type 2 instruments (i.e., every type of document), the County Recorder/Submitter shall ensure that all endpoints are secure. As such, workstations used to submit, retrieve, or if applicable, return the ERDS payloads must be protected from unauthorized use and access. At a minimum, all workstations shall meet all the following requirements:

1. Anti-malware software configured to start on system boot-up.
2. Operating system software with the most up-to-date patches and hot-fixes.
3. Host-base firewall configured to restrict inbound and outbound connections.

For ERDS that serve Type 1 instruments only (i.e., only those documents affecting title, such as Deeds, Deeds of Trust, etc.), installed applications shall be limited to the purpose of performing the necessary operational needs of the recording process as defined by the County Recorder.

The County Recorder shall include this requirement as a mandatory provision in all contracts with Authorized Submitters. All Submitters shall ensure that an Agent, if any, complies with these requirements. The contents of the contract provision are subject to audits and local inspections.

11.0—DOCUMENT PREPARATION

The preparation of the documents for scanning is an essential, and often, the most time-consuming part of electronic recording. Documents not prepared correctly may require rescanning, additional work, additional fees, and can cause paper jams in the scanner.

11.1—DOCUMENT PREPARATION TIPS

- Verify that each document has original signatures, original notary seals, and an original notary signature as appropriate.
- Carefully remove all paperclips and staples, taking care to not tear or damage the documents.
- Verify dark highlighters, such as blue, green, purple, or red, have not been used on any of the pages. These will not be legible when scanned; the document must be redone.
- Verify any stamps have not "bled through" to the other side of the page. Cover the back of the page with white tape or a white label.
- Repair any damaged or torn corners or edges of the documents with tape, ensuring that the tape does not cover any printed areas of the document. The tape must not extend beyond the edge of the document, as this may cause the paper to jam in the scanner.
- Remove any post-it notes, or "sign-here" tabs.
- Verify document does not contain any social security numbers (prohibited by law).

11.2—SCANNING TIPS

- Place the documents in the scanner's feeder in the order in which they are to be submitted for recording. Documents may then be saved as files in a pre-assigned folder/destination on the secured workstation for later or immediate submission to the Recorder Division.
- The images will appear briefly on the page as they are scanned. Monitor the quality of the images as they appear. Watch for:
    - Poor images

- Streak lines through the image
- Skewed images
- Blurred images
- Bleed throughs (If a stamp has 'bled through' to the reverse side of a page, the scanner will sense that there is something on the page and will create an image for it. It may also obscure text on the reverse side.)
- Missing signatures
- Missing seals or markings (Sometimes, some scanners will not recognize certain colors or will not recognize very light information. Contact your technical support if this occurs.)

- When the document has been completely scanned, verify that the page count is correct.

11.3—QUALITY CHECKING SCANNED DOCUMENTS

- **Legibility:** Make certain that EVERY page of the file is clearly legible. Legibility does **not** mean that it can simply be read, but that the image can be reduced to microfilm size and successfully enlarged back to normal size without any loss of content. This includes any and all individual letters and numbers that appear throughout the document, including all information on any map.

- **Direction:** Make certain that all pages are right-side-up in the correct direction.

- **Page Count:** Ensure that every page of the document was scanned, including any reverse side pages (containing vital information, certification seals, etc.).

- **Page Size:** The only two sizes allowed for recording are letter size (8½ in. by 11 in.), or legal size (8½ in. by 14 in.).

- **Margins:** A ½ in. margin is required on EVERY page on ALL four sides of the page.

- **Label Space Reservation:** A 2½ in. tall by 5 in. wide blank space is required in the upper right-hand side of the first page of EVERY document. NOTHING can appear in this space or the document will be rejected (parts of notary seals, signatures, etc.).

- **Notary Seals:** Every number/letter in the notary seal must be legible. Be certain that every notary seal is present and legible for recording.

- **Notary Seal Ink:** Only use dark inks for scanning purposes; light inks will not show and may cause the document to be rejected.

- **Embossed Seals:** Very lightly use the side of a pencil tip to shade over the embossed seal to ensure that they scan (at least in part). Otherwise, it may cause the document to be rejected for a missing notary seal.

- **Double-sided Pages:** Make certain that every page is scanned in order for all double-sided page documents. This also applies to court documents (with court seals) and death certificates from other states.

- **Death Certificates:** Because most death certificates are printed on security paper (bank note), special attention must be given to all death certificates (contained in Affidavits of Death, etc.). Be certain that the "void" marks are light and that any shading does not obscure any text to prevent the document from being rendered illegible for recording.

- **Preliminary Change of Ownership Reports (PCOR):** The two pages of the PCOR should be scanned and submitted with the document(s).

- **Claim for Reassessment Exclusion:** The two page Reassessment Exclusion is to be scanned and submitted along with the PCOR.

11.4—MANUAL SUBMISSIONS

Some documents cannot be processed through the scanner. These documents must be submitted in paper form to the Recorder Division via the Agent. Examples of these types of documents are:

- Documents that have tears or holes which cannot be repaired
- Bankruptcy papers (or foreign documents) with brads and ribbons
- Documents with attachments or labels that are taped onto the paper
- Fragile paper documents (old documents), or documents which cannot be put through the scanner
- Documents with very large page counts
- Documents with "fill-ins" (i.e., those which require recording information to be inserted immediately after recording)

Documents that are larger than 8½" x 14" are NOT acceptable for recording.

Documents larger than 8½" x 14", even if scanned to 8½" x 11" size, will not convert legibly when going to microfilm and are also not acceptable for recording.

12.0—DOCUMENT SUBMISSION

12.1—TYPE 1 & TYPE 2

A "Type 1" instrument is defined as an instrument affecting a right, title, or interest in real property. Type 1 instruments shall be delivered as digitized electronic records. **"Digitized"** means an actual paper document being scanned into an electronic file form.

A "Type 2" instrument is defined as an instrument of Reconveyance, Substitution of Trustee, or Assignment of Deed of Trust. Type 2 instruments may be delivered as digitized electronic records or digital electronic records. **"Digital"** means that there is no actual paper document; the digital document exists in electronic form only on a computer system.

To summarize:

Type 1—an instrument affecting a right, title, or interest in real property.
Type 1 documents MUST be digitized.

Type 2—an instrument of Reconveyance, Substitution of Trustee, or Assignment of Deed of Trust.
Type 2 documents MAY be digital OR digitized.

12.2—CeRTNA DOCUMENT TYPES

12.2.1—TYPE 1

(Recordable)

- Abstract of Judgment
- Affidavit of Death
- Agreement (any type of agreement document)
- Assignment (all general assignments other than an Asgt. of DOT)
- Deeds (any and all types, Grant, Quitclaim, etc)
- Deed of Trust
- Judgment
- Modification (of any type)
- Notice (of any type)

- Power of Attorney
- Request (of any type)
- Lien Satisfaction (of any type)
- Subordination Agreement
- Other

(NON-Recordable but can be submitted with recorded document??)

- Preliminary Change of Ownership Report (PCOR)
- Any other Unrecorded Disclosure

12.2.2—TYPE 2

- Assignment of Deed of Trust
- Reconveyance
- Substitution of Trustee

12.3—CeRTNA STANDARD REJECTION REASONS

- A.P.N. not found
- Acceptance required
- All-Purpose Acknowledgment required
- Attachment part of document
- Insufficient space for recording stamp
- Unaltered death certificate required
- Document image is illegible
- Document is incomplete
- Document requires verification
- Documentary Transfer Tax (DTT) is incomplete
- Legal description missing
- Missing completion date
- Name and return address missing
- Name must be typed or printed
- Name or company or trust missing
- No name set out for…
- Notary acknowledgment incomplete
- Notary acknowledgment required
- Notary seal illegible/altered
- Notary signature and/or seal missing
- Preliminary Change of Ownership Report (PCOR) missing

- Property not in this county
- Recording reference missing/incorrect
- Re-recording problem
- Signature missing
- Tax statement address required
- UCC perfect security interest
- Type 1/2 mixed in transaction
- Original document required
- Original certified copy required
- No provision to record
- Names must agree
- Multiple reject reasons
- Pulled with order
- Free form

12.4—MANUAL SUBMISSIONS

There are always reasons why Manual Submissions may be necessary from time to time. While the goal of Electronic Recording is to record as many documents electronically as possible for efficiency, the Recorder recognizes the following exceptions:

- Power Outage or Natural Disaster at the Agent or Submitter or Recorder
- Hardware Malfunctions
- Voluminous Documents
- Fragile Documents
- Documents with Brads and Ribbons
- Documents with Fill-ins

13.0—USER GUIDE (will be provided by Agent or Certna)

User guides will be provided during the User's training by Agent or Certna to better provide for a full working knowledge of the system and its reporting capabilities. The following manuals will be made available:

- ERDS Bulk Submitter User Guide
- ERDS Direct Submitter User Guide
- ERDS Workstation, IKey Token Configuration and Installation
- ERDS Report User Guide
- *(Other Guides as they become available)*

14.0—SUPPORT PROCEDURES (all support issues will be handled via Agent)

14.1—HELP SUPPORT PROTOCOL

14.1.1—At the Submitter's Office

RECORDING ISSUES:

- Submitters must try to resolve the recording issue first within their own office.
- If the submitters and their supervisors are unable to resolve the recording issue, they may then contact the Recording Staff at the Recorder Division for further assistance.

  Napa County Recording Department:

  Telephone: (707) 253-4105

  E-mail: recorder-clerkMB@countyofnapa.org
- If the issue must be addressed by technical support, the Recording Staff will refer the call to the IT Staff at the Recorder Division.

- TECHNICAL ISSUES:
  - Submitters must try to resolve the technical issue first within their own office.
  - If the submitters and their technical support are unable to resolve the issue, they may then contact the Staff at the Recorder Division for further assistance.
  - If the issue must be addressed by technical support, the Recording Staff will refer the call to the IT Staff at the Recorder Division.

14.1.2—At the Recorder Division

- RECORDING ISSUES:
  - Recording Staff will address the issue or refer the matter over to their immediate supervisor.
  - If the Recording Staff is unable to resolve the issue, it will contact the Submitter for the batch in question.

- TECHNICAL ISSUES:
  - The Recorder's IT Staff will address the issue or refer the matter over to their immediate supervisor.
  - If the Recorder's IT Staff is unable to resolve the issue, it will contact CeRTNA staff directly.

14.2—WHOM TO CALL (Agent will handle all contacts with Recorder except in special circumstances where Submitter must be involved with Agent participation)

14.3—COUNTY CONTACT LIST

14.3.1—Recording Administration

- John Tuteur, Assessor-Recorder-County Clerk (707) 253-4459
- Vicki Poli, Assessment Records Supervisor (707) 253-4618
- LaVanda Schneider, Senior Doc Recorder (707) 299-1370

14.3.2—Recording Staff -707-253-4105

14.4—TROUBLE SHOOTING (handled with Agent)

15.2—ERDS Form 12 (Acknowledgment of Responsibilities)

STATE OF CALIFORNIA
Electronic Recording Delivery System (ERDS)
Acknowledgment of Responsibilities
ERDS 0012
(Rev. 09/07)

DEPARTMENT OF JUSTICE
California Justice Information Services Division
CJIS Operations Support Bureau
Electronic Recording Delivery System Program
Telephone: (916) 227-8907
FAX: (916) 227-0595
E-mail: erds@doj.ca.gov

Electronic Recording Delivery System
Acknowledgment of Responsibilities

*EMPLOYEE*_____ *EMPLOYED BY:*
(Print Name)

☐ *COUNTY RECORDER*
☐ *AUTHORIZED SUBMITTER OR AGENT*
☐ *VENDOR OF ERDS SOFTWARE*

The Electronic Recording Delivery Act of 2004 authorizes a county recorder, upon approval by resolution of the Board of Supervisors and system certification by the ERDS Program, to establish an Electronic Recording Delivery System for the delivery, and, when applicable, return of specified digitized and digital electronic records that are an instrument of real estate transactions, subject to specified conditions, including system certification, regulation and oversight by the ERDS Program.

ERDS users shall comply with the California Code of Regulations, Title 11, Division 1, Chapter 18, Articles 1 - 9 governing the use of an ERDS and the County Recorder's ERDS operating procedures relating to the appropriate use of the ERDS.

ERDS users are responsible for taking the appropriate steps to secure their ERDS password. General requirements for your password are:

- Do not share your password with anyone.
- Do not convey your password to anyone via telephone, e-mail, verbally, etc.
- Do not insert your password into e-mail messages or other forms of electronic communications where the password is in clear, readable text that can be read by someone else or posted where it can be compromised.
- Do not write down your password and store it anywhere in your work area (i.e., taped to the bottom of the keyboard, under the front of the monitor, in a desk drawer, under the desk itself, etc.) where it can be compromised. Store your password in a secure location.
- Do not talk about your password in front of other people.

You will be held accountable if you fail to comply with the password policy and protection standards. If you suspect that your account or password was compromised, report the incident to your supervisor.

Any individual who is responsible for misuse may be subject to having access to the ERDS terminated or suspended by the ERDS Program.

I have read the above and understand regarding the use of the ERDS. This document will be kept in my personnel folder or pertinent file subject for review during local inspections.

Signature: _____ Date: _____

17.0—GLOSSARY

ACH	*See "Automated Clearing House"*
Automated Clearing House	An electronic network for financial transactions in the United States; processing large volumes of both credit and debit transactions, payroll, and payments.
AG	*See "Attorney General"*
Agent	A representative and his/her employees who are authorized to submit documents on behalf of an Authorized Submitter who has entered into a contract with a County Recorder and assigned a role by the County Recorder, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Agent may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator, or Vendor of ERDS Software. (Refer to the definition of "Vendor of ERDS software (or Developer)" within this section.)
Approved Escrow Company	An escrow company approved pursuant to the California Code of Regulations, Title 2, Division 7, Chapter 6, Article 3, D, List of Approved Companies and Facilities, Section 20639.
Attorney General	The Attorney General of the State of California. Acronym: "AG".
Authorized Access	A role assigned by the County Recorder to an Authorized Submitter and Agent, if any, who is authorized to use ERDS for only Type 2 instruments. This role does not require fingerprinting.
Authorized Security Representative	AKA: "Security Liaison". The person in the Title Office ?? authorized to request the AGENT or CERTNA to add, change, or delete User security for the system.
Authorized Submitter	A party and his/her employees that has entered into a contract with a County Recorder and assigned a role by the County Recorder through an Agent, to deliver, and, when applicable, return the submitted ERDS payloads via an ERDS. An Authorized Submitter may not be a Computer Security Auditor, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vendor of ERDS Software.
CCISDA	California County Information Services Directors Association
CCR	California Code of Regulations
Certificate Authority	A certificate authority that issues digital certificates for the purpose of establishing secure Internet sessions between an Authorized Submitter and an ERDS. Certificate authorities also validate digital certificates presented as proof of identity.
CFE	Certified Fraud Examiner
CeRTNA	Acronym for "California E-Recording Transaction Network Authority". The provider of the ERDS for the County Recorder.
CIA	Certified Internal Auditor
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
Computer Security Auditor	(1) California DOJ approved computer security personnel hired by the County Recorder to perform independent audits. (2) A role assigned by the County Recorder to the Computer Security Auditor who is authorized to review transaction logs and conduct tests on computer security mechanisms. A Computer Security Auditor may not be an Authorized

	Submitter, Agent, County Recorder Designee, ERDS Account Administrator, ERDS System Administrator or Vender of ERDS Software. This role requires fingerprinting. A Computer Security Auditor shall be issued a certificate of approval by the ERDS Program.
County Recorder	A public official responsible for administering an ERDS, ensuring that all ERDS requirements are met and who oversees the assignment and delegation of the responsibilities by determining the necessary resources and means.
County Recorder Designee	A Secure Access role assigned by the County Recorder to retrieve, and, when applicable, return submitted ERDS payloads. A County Recorder Designee may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.
Department of Justice	The Department of Justice of the State of California. Acronym: "DOJ".
Developer	Refer to Vendor of ERDS Software.
Digital Electronic Record	A record containing information that is created, generated, sent, communicated, received or stored by electronic means, but not created in original paper form.
Digital Signature	A set of electronic symbols attached to, included in, or logically associated with one or more Type 1 and/or Type 2 instruments, inclusive of information related to and intended for association with the Type 1 and/or Type 2 instruments, that is the result of a process, or processes, designed and employed for the purpose of verifying the integrity, accuracy or authenticity of the Type 1 and/or Type 2 instruments with related information. For the purpose of an ERDS, a digital signature is generated by encrypting the hash value of an ERDS payload.
Digitized Electronic Record	A scanned image of the original paper document.
DOJ	*See "Department of Justice"*
Electronic Signature of the Notary	A field or set of fields, containing information about the electronic signature of the notary who notarized a Type 1 or Type 2 instrument.
Electronic Recording	AKA: "ER". The electronic submission of official documents for recording from an Agent to the Recorder Division.
ER	*See "Electronic Recording"*
ERDA	Electronic Recording Delivery Act of 2004.
ERDS	*See "Electronic Recording Delivery System"*
Electronic Recording Delivery System	Electronic Recording Delivery System – An ERDS Program certified system to deliver digitized Type 1 and/or Type 2 instruments to a County Recorder, and, when applicable, return to the Authorized Submitter.
ERDS Account Administrator	A secure access role assigned by the County Recorder to an individual authorized to configure accounts, assign roles and issue credentials. An ERDS Account Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.

ERDS Payload	An electronic structure designed for the purpose of delivering Type 1 or Type 2 instruments to a County Recorder via an ERDS. The structure is also used to return, and, when applicable, Type 1 or Type 2 instruments to an Authorized Submitter via an ERDS.
ERDS Program	The program within DOJ designated by the Attorney General to certify, implement, regulate and monitor an ERDS.
ERDS Server	Computer hardware, software and storage media used by the County Recorder to implement an ERDS. The ERDS server executes the primary functionality of the application software associated with an ERDS. The ERDS Server includes software for encrypting, decrypting, hashing, submitting, and, when applicable, returning the ERDS payloads. It also includes storage media for the ERDS payloads in the process of being delivered to the County Recorder or, when applicable, being returned to the Authorized Submitter via the Agent. Separate physical servers dedicated to performing ERDS server functions are not required provided that the ERDS server functions can be isolated from other server functions, as evidenced by audit.
ERDS System Administrator	A secure access role assigned by the County Recorder to an individual who is authorized to configure hardware, software, network settings and to maintain ERDS security functions. An ERDS System Administrator may not be a Computer Security Auditor, Authorized Submitter, Agent or Vendor of ERDS Software. This role requires fingerprinting.
FIPS	Federal Information Processing Standard
GIAC	Global Information Assurance Certification
GSNA	GIAC Systems and Network Auditor
HMAC	Hash Message Authentication Code
Incident	An event that may have compromised the safety or security of an ERDS.
Instrument	A “Type 1” instrument is defined to mean an instrument affecting a right, title or interest in real property. Type 1 instruments shall be delivered as digitized electronic records. Individuals given role-based privileges for a Type 1 instrument shall be fingerprinted. A “Type 2” instrument is defined to mean an instrument of reconveyance, substitution of trustee or assignment of deed of trust. Type 2 instruments may be delivered as digitized electronic records or digital electronic records. Individuals given role-based privileges for a Type 2 only instrument shall not be fingerprinted.
Lead County	The County Recorder in a Multi-County ERDS responsible for administering an ERDS, ensuring that all ERDS requirements are met and who oversees the assignment and delegation of the responsibilities by determining the necessary resources and means.
Live Scan	A DOJ system used for the electronic submission of applicant fingerprints. This system is outside of the ERDS Program.
Logged	An auditable ERDS event.
Logical	The way data or systems are organized. For example, a logical description of a file is that it is a collection of data stored together.
MAC	Message Authentication Codes

Multi-County	An ERDS application where County Recorders collaborate and make use of a single ERDS serving multiple counties.
NIST	National Institute of Standards and Technology
Non-Substantive Modification	A change that does not affect the functionality of an ERDS.
ORI	Originating Agency Identifier
Physical Access	Access granted to an individual who has physical access to an ERDS server. This level of access requires fingerprinting with the exception of a county data center or an outsourced county data center in which physical access is already managed by security controls.
Public Entity	Includes the State, the Regents of the University of California, a county, city, district, public authority, public agency, any other political subdivision or public corporation in the State and federal government entities.
PKI	A Public Key Infrastructure is a framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority, which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages, which ensure that messages have not been tampered with.
Reportable	An incident that has resulted in the compromise of the safety or the security of an ERDS and shall be reported to the ERDS Program.
RSA	A public-key encryption technology developed by Rivest, Shamir and Adelman (RSA). The RSA algorithm has become the de facto standard for industrial-strength encryption especially for data sent over the Internet.
Role	A security mechanism, method, process or procedure that defines specific privileges controlling the level of access to an ERDS.
SANS Institute	Systems and Network Security Institute
Secure Access	A role assigned by the County Recorder to an individual which requires fingerprinting to: 1) an Authorized Submitter and Agent, if any, who are authorized to use an ERDS for both Type 1 and 2 instruments (excludes Type 2 instruments only) or Type 1 instruments only; 2) a Computer Security Auditor hired by the County Recorder to perform independent audits; 3) an ERDS System Administrator authorized to configure hardware, software and network settings; 4) an ERDS Account Administrator authorized to configure accounts, assign roles and issue credentials; 5) an individual who is granted physical access to an ERDS server; 6) a County Recorder Designee authorized to retrieve, and, when applicable, return submitted ERDS payloads.
Security Liaison	*See "Authorized Security Representative"*
Security Testing	An independent security audit by a Computer Security Auditor, including, but not limited to, attempts to penetrate an ERDS for the purpose of testing the security of that system.
SHA	Secure Hash Algorithm
Source Code	A program or set of programs, readable and maintainable by humans, translated or interpreted into a form that an ERDS can execute.

Source Code Materials	Source Code Materials must include, but, are not limited to: 1) a copy of all source code that implements ERDS functionality; 2) a copy of the compiler needed to compile the ERDS source code in escrow; 3) instructions for installation and use of the ERDS source code compiler; and 4) instructions that facilitate reviews, modification and/or recompiling the source code.
Sub-County	The collaborating County Recorder(s) in a Multi-County ERDS operation.
Substantive Modification	A change that affects the functionality of an ERDS.
TLS	Transport Layer Security (formerly known as Secure Socket Layer)
Type 1 Instrument	A Type 1 Instrument is defined to mean an instrument affecting a right, title, or interest in real property. Type 1 instruments shall be delivered as digitized electronic records. Individuals given role-based privileges for a Type 1 Instrument shall be fingerprinted.
Type 2 Instrument	A Type 2 Instrument is defined to mean an instrument of Reconveyance, Substitution of Trustee, or Assignment of Deed of Trust. Type 2 Instruments may be delivered as digitized electronic records or digital electronic records. Individuals given role-based privileges for a Type 2 only instrument shall not be fingerprinted.
Uniform Index Information	Information collected by a County Recorder in the recording process. Every Type 1 and Type 2 Instruments delivered through an ERDS shall be capable of including uniform index information. The County Recorder shall decide on the content of uniform index information.
User	A person who uses a computer to access, submit, retrieve, or, when applicable, return an ERDS payload.
Vendor of ERDS Software (or Developer)	A person and personnel, supporting and/or acting on behalf of the certified Vendor of ERDS Software who sells, leases, or grants use of, with or without compensation therefore, a software program for use by counties for establishing an ERDS A Vendor of ERDS Software may not be a Computer Security Auditor, Authorized Submitter, Agent, ERDS Account Administrator, ERDS System Administrator, County Recorder Designee, or internal county resources used as a Developer of an ERDS in lieu of a Vendor. This role requires fingerprinting.
Workstation	A computer used to connect to and interact with an ERDS.