FORM APPROVED COUNTY COUNSEL 2/24/15
BY: GREGORY P. PRIAMOS DATE

243

SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FROM: SHERIFF'S DEPARTMENT

SUBMITTAL DATE:
February 11, 2015

SUBJECT: Resolution 2015-054, Approval of the Riverside County Sheriff's Department Retention of Electronic Documents System (REDS) as an Electronic Content Management Trusted System and Authorizing Sheriff to Destroy Original Hardcopies and Maintain Official Records Electronically in REDS

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve and adopt Resolution 2015-054 approving Riverside County Sheriff's Department Retention of Electronic Documents System (REDS) as an Electronic Content Management trusted system, and pursuant to Government Code section 26205.1(a), authorizing the Sheriff to destroy original hardcopies and maintain official records electronically in REDS.

BACKGROUND:

Summary

In July 2011, the Board of Supervisors approved Board Policy A-68, which recognized the need to establish countywide standards to ensure that official County records that are maintained electronically comply with state law trusted system requirements. Policy A-68 set forth the process for department heads to demonstrate compliance with the trusted system requirements, including obtaining Board approval by resolution (Attachment A).

(Continued on page 2)

2/18/15
Stan Sniff
Sheriff-Coroner-PA
Jerry Gutierrez, Assistant Sheriff

Departmental Concurrence

APPROVED BY: 2/18/15
SEBRON PARTRIDGE DATE
CHIEF INFORMATION SECURITY OFFICER

FINANCIAL DATA	**Current Fiscal Year:**	**Next Fiscal Year:**	**Total Cost:**	**Ongoing Cost:**	**POLICY/CONSENT (per Exec. Office)**
COST	$ 0	$ 0	$ 0	$ 0	Consent □ Policy ☒
NET COUNTY COST	$ 0	$ 0	$ 0	$ 0	

SOURCE OF FUNDS:	**Budget Adjustment:** No
	For Fiscal Year: N/A

C.E.O. RECOMMENDATION:

APPROVE

County Executive Office Signature BY: Elizabeth J. Olson
Elizabeth J. Olson

MINUTES OF THE BOARD OF SUPERVISORS

□ Positions Added
□ Change Order
□ A-30
□ 4/5 Vote

Prev. Agn. Ref.:	**District:**	**Agenda Number:** 3-33

SUBMITTAL TO THE BOARD OF SUPERVISORS, COUNTY OF RIVERSIDE, STATE OF CALIFORNIA
FORM 11: Resolution 2015-054, Approval of the Riverside County Sheriff's Department Retention of Electronic Documents System (REDS) as an Electronic Content Management Trusted System and Authorizing Sheriff to Destroy Original Hardcopies and Maintain Official Records Electronically in REDS
DATE: February 11, 2015
PAGE: 2 of 2

BACKGROUND:

Summary (continued)

Pursuant to Government Code sections 26205 and 26205.1, the Board of Supervisors may authorize a County officer to cause to be destroyed certain official record if all statutory conditions are complied with, including but not limited to, the record is electronically recorded on a trusted system, is produced in compliance with Government Code section 12168.7, accurately reproduces the original record, and is conveniently accessible.

Over the past two years, the Sheriff's Department has developed REDS with oversight and guidance from the Information Security Office (ISO) and Records Management and Archives Program (RMAP).

In January 2015, the ISO Assessment Team concluded its two year evaluation and issued its final report on REDS (Attachment B), finding it compliant with the requirements of Policy A-68 as a trusted system.

Impact on Residents and Businesses

REDS will not negatively impact citizens and businesses. REDS will improve the accessibility and retrieval of official records facilitating the production of these records as needed for public or business purposes. The funding will be drawn from existing approved budget.

ATTACHMENTS:

A. Resolution 2015-054, A Resolution of the Board of Supervisors of the County of Riverside Approving Riverside County Sheriff's Department Retention of Electronic Documents System (REDS) as an Electronic Content Management trusted system, and pursuant to Government Code section 26205.1(a), authorizing the Sheriff to destroy original hardcopies and maintain official records electronically in REDS; and

B. Trusted System Assessment Report for Sheriff's Retention of Electronic Documents System (REDS).

ATTACHMENT A

Board of Supervisors County of Riverside

RESOLUTION NO. 2015-054

A RESOLUTION OF THE BOARD OF SUPERVISORS OF THE COUNTY OF RIVERSIDE APPROVING RIVERSIDE COUNTY SHERIFF'S DEPARTMENT RETENTION OF ELECTRONIC DOCUMENTS SYSTEM (REDS) AS AN ELECTRONIC CONTENT MANAGEMENT TRUSTED SYSTEM, AND PURSUANT TO GOVERNMENT CODE SECTION 26205.1(A), AUTHORIZING SHERIFF TO DESTROY ORIGINAL HARDCOPIES AND MAINTAIN OFFICIAL RECORDS ELECTRONICALLY IN REDS

WHEREAS, pursuant to Government Code section 12168.7, the term "trusted system" means a combination of techniques, policies and procedures for which there is no plausible scenario in which a document retrieved from or reproduced by the system could differ substantially from the document that is originally stored;

WHEREAS, to implement Government Code section 12168.7, the California Secretary of State adopted California Code of Regulations, Title 2, sections 22620.1 to 22620.8, entitled "Trustworthy Electronic Documents or Record Preservation";

WHEREAS, Government Code section 26205 allows the Board of Supervisors, at the request of a County officer, to authorize the destruction of any County record that is not expressly required by law to be filed and preserved if all of its statutory conditions are complied with, including, but not limited to: (i) the record recorded in the electronic data processing system is a trusted system, does not permit additions, deletions, or changes to the original document images, and is produced in compliance with Government Code section 12168.7; (ii) the device used to reproduce the record accurately reproduces the original record in all details and does not permit additions, deletions, or changes to the original document images; (iii) the records in the electronic data processing system are placed in conveniently accessible files and provision is made for preserving, examining, and using the files; and (iv) a duplicate copy of a record contained in the electronic data processing system that does not permit

FORM APPROVED COUNTY COUNSEL
BY: TAMMY V. DIEU 2/24/15
DATE

additions, deletions or changes to the original document images is also separately maintained;

WHEREAS, the County officer having custody of nonjudicial County records may cause to be destroyed such records if all of the conditions under Government Code section 26205.1 exist, including, but not limited to: (i) the Board of Supervisors has adopted a resolution authorizing said County officer to destroy the records pursuant to Government Code section 26205.1, subdivision (a); (ii) the County officer who destroys any record maintains such records in an electronic data processing system that does not permit additions, deletions, or changes to the original document or other duplicate of the record destroyed; and (iii) the record recorded in the electronic data processing system is a trusted system, does not permit additions, deletions, or changes to the original document, and is produced in compliance with Government Code section 12168.7;

WHEREAS, the Board of Supervisors has established Board Policy A-68, entitled Trustworthy Official Electronic Records Preservation, as amended, ("Board Policy A-68") and the Sheriff's Department has developed and implemented its associated departmental procedures on trusted system;

WHEREAS, the County of Riverside has a Board-approved General Records Retention Schedule (hereafter "GRRS") and the Sheriff's Department has a Board-approved Departmental Records Retention Schedule (hereafter "DRRS");

WHEREAS, subject to the Board's approval, the Sheriff will maintain the official records set forth in Exhibit A (hereafter "Official Records") electronically in the Sheriff's Department Retention of Electronic Documents System (hereafter "REDS"), and subject to the Board's authorization, will destroy and/or cause to be destroyed the original hardcopies of such Official Records that are maintained electronically in REDS, which Official Records are not expressly required by law to be filed and preserved and are not required by law to be retained in hardcopy format;

WHEREAS, REDS, which is an Electronic Content Management System (hereafter "ECMS"), has been evaluated by the Riverside County Information Security Office (hereafter "Assessment Team"), with the participation of Records Management Archives Program ("RMAP"), to the greatest extent technologically and procedurally possible in order to ensure that the Official Records are electronically stored in a trusted system.

WHEREAS, the Assessment Team concluded in its Assessment Report that: (i) at least two separate official electronic records are created in REDS meeting all of the conditions of a trusted system; and (ii) official electronic records maintained in REDS are considered to be true and accurate copies of the original information received;

WHEREAS, the Sheriff has ensured: (i) REDS is a trusted system; (ii) compliance with Government Code sections 26205, 26205.1 and 12168.7, and California Code of Regulations, Title 2, sections 22620.1 to 22620.8; and (iii) compliance with Board Policy A-43, Board Policy A-68, and departmental procedures on trusted system;

WHEREAS, Board Policy A-68 requires the department head to secure the Board of Supervisors' approval of the department's ECMS as a trusted system and a resolution adopted by the Board of Supervisors pursuant to Government Code section 26205.1, subdivision (a), authorizing the department head to cause to be destroyed the original hardcopy of the Official Records that are maintained electronically in the ECMS;

NOW, THEREFORE, BE IT RESOLVED by the Board of Supervisors of the County of Riverside, in regular session assembled on ____________, 20__, that the Sheriff's Department REDS, which is an ECMS, is approved as a trusted system.

BE IT FURTHER RESOLVED that pursuant to California Government Code section 26205.1, subdivision (a), the Board of Supervisors of the County of Riverside hereby authorizes the Sheriff to destroy and/or cause to be destroyed the original hardcopies of the Official Records described in Exhibit A attached hereto and consisting of one page, and maintain such Official Records electronically in REDS for the applicable retention period, provided that the Sheriff shall not destroy and/or caused to be destroyed any Official Records that are expressly required by law to be filed and preserved and/or required by law to be retained in hardcopy format.

BE IT FURTHER RESOLVED that if notice of litigation, reasonably anticipated litigation, audit or records request is received by the Sheriff's Department prior to the expiration of the applicable retention period of the Official Records and/or official electronic records, the scheduled destruction and/or deletion of any relevant Official Records and/or official electronic records maintained in REDS shall be suspended by Sheriff or his/her designee until the final resolution of the litigation, audit and/or records request.

EXHIBIT A

1. All official records described in the current Board-approved Sheriff's Department DRRS, specifically DRRS_SHF_2013_Rev01, and any subsequent Board-approved Sheriff's Department DRRS, with the exception of the following: (i) official records expressly required by law to be filed and preserved; (ii) official records required by law to be retained in hardcopy format; and (iii) official records listed below:

Code	**Title**
SHF-CID100	Latent Fingerprint Case Files – Persons Crimes
SHF-CID150	Latent Fingerprint Case Files – Property Crimes
SHF-CPA750	X-Rays – Natural Deaths
SHF-CPA800	X-Rays – PC187 and Coroner Review Cases
SHF-CPA850	X-Rays – Traumatic Cases
SHF-COR450	Jail Information Management System (JIMS)
SHF-GEN030	Audio, Telephone and Radio Communications
SHF-GEN440	Surveillance / Security Video

Sheriff shall comply with the most recent Board-approved Sheriff's Department DRRS, which supersedes prior versions.

2. To the extent applicable to the Sheriff's Department, official records described in the current Board-approved County of Riverside's GRRS, specifically GRRS_2013_Rev08, and any subsequent Board-approved County of Riverside's GRRS, with the exception of the following: (i) official records expressly required by law to be filed and preserved; (ii) official records required by law to be retained in hardcopy format; and (iii) official records listed below:

Code	**Title**
ADM750	Video Monitoring

Sheriff shall comply with the most recent Board-approved County of Riverside's GRRS, which supersedes prior versions.

ATTACHMENT B

COUNTY OF RIVERSIDE
INFORMATION SECURITY OFFICE

TRUSTED SYSTEM ASSESSMENT REPORT FOR SHERIFF'S RETENTION OF ELECTRONIC DOCUMENTS SYSTEM (REDS)

RIVERSIDE COUNTY INNOVATION CENTER
3450 14TH STREET • RIVERSIDE, CALIFORNIA 92501 • OFFICE (951) 955-8282 • FAX (951) 955-8070

Authority

Health Insurance Portability and Accountability Act (HIPAA) - Privacy, Security, and Breach Notification Rules
U.S. Department of Health and Human Services Title 45 C.F.R. Parts 160 and 164

Health Information Technology for Economic and Clinical Health (HITECH) Act - Enforcement Rule
U.S. Department of Health and Human Services Title 45 C.F.R. Parts 160 and 164

California Confidentiality of Medical Information Act
California Civil Code § 56

California Public Records Act
California Government Code §§ 6250-6276.48

California Security Breach Notification Law
California Civil Code §§ 1798.29 and 1798.82

California Trusted System Laws
California Government Code § 12168.7
California Code of Regulations Title 2 §§ 22620.1-8

Riverside County Records Management and Archives Policy
Riverside County Board of Supervisors Policy A-43

Riverside County Electronic Media and Use Policy
Riverside County Board of Supervisors Policy A-50

Riverside County Information Security Policy
Riverside County Board of Supervisors Policy A-58

Riverside County Trustworthy Official Electronic Records Preservation Policy
Riverside County Board of Supervisors Policy A-68

Riverside County Health Privacy and Security Policy
Riverside County Board of Supervisors Policy B-23

Table of Contents

1 Executive Summary

The Riverside County Sheriff's Department (Sheriff) submitted for review the Retention of Electronic Documents System (REDS) and its associated policies, processes, and procedures to the Riverside County Information Security Office (ISO). REDS will serve as the digital repository for official electronic records retained and archived by Sheriff. Therefore, the system and its implementing policies, procedures, and technologies must comply with all requirements of a trusted system in accordance with California Government Code Section 12168.7, California Code of Regulations Title 2 Sections 22620.1-8, and Riverside County Board of Supervisors Policies A-68 and A-43.

Following a comprehensive evaluation, the ISO Assessment Team determined REDS to be fully compliant. During the evaluation, it was noted that REDS maintains at least two (2) separate official electronic records that are considered to be true and accurate copies of the original physical records. Therefore, it is recommended that the Riverside County Board of Supervisors (BOS) acknowledges REDS as a trusted system to be used by Sheriff as intended.

2 Scope and Limitations

The records management life cycle begins at the moment a record is created or received. First instances of records may be paper or electronic. In any case, the requirements of a trusted system, by California law, begin when the electronic version is created or received, or, in the case of a paper document, at the scanner where a paper document will be converted to an electronic duplicate or surrogate of the hard copy record. For this reason, the ISO assessment process begins by evaluating the ingest procedures for paper or electronic records. Other processes may take place within the workflow prior to this step and may further ensure the authenticity of a record. However, these recommended records management steps fall outside of the scope of Policy A-68, and therefore, fall outside of the scope of the ISO assessment.

3 Records Management Policy

Sheriff maintains a BOS-approved Departmental Records Retention Schedule (DRRS) that covers the records to be retained electronically by the system and requires deletion of records after an approved period of time. The system is designed to implement such disposition with the appropriate authorizations in order to comply with Board of Supervisors Policy A-43.

Sheriff has also written a Department Directive to implement REDS and requires that staff having access to or responsibilities for REDS read the policy and acknowledge their understanding of it.

Sheriff processes require the use of PDF/A for image format.

Sheriff processes indicate the appropriate use of approved compression techniques.

REDS job function responsibilities are identified within department processes and are mirrored in the access controls within the system.

4 Processes and Procedures

Departmental processes and procedures, as detailed in the REDS User Guide, System Configuration, Technical Specifications, and Scanner Settings, meet the definition of a trusted system. These documents and any revisions to them will be maintained as long as the records to which they pertain is retained.

Documentation pertaining to departmental procedures exist, are followed, and maintained:

- to check and validate complete scanning and indexing process;
- to examine documents prior to the scanning process to confirm their suitability for scanning;
- for documents that may cause scanning difficulties;
- for managing physical attachments, such as stick-on notes, or other notes or annotations;
- when scanning multi-page documents bound together with staples or clips;
- to determine size and content of batches;
- when source documents must be photocopied prior to scanning;
- to document variations to procedures due to type of document being scanned will be maintained for as long as the records to which they pertain;
- to document decisions made in relation to use of duplex or simplex scanning; black and white or color scanning;
- to ensure that the number of pages/sides in a batch is compared to the number of pages scanned;
- to ensure departmental procedures are followed to ensure that the scanner is functioning properly at the beginning of each day or batch. (Use of a test target or sample batch to establish a control.);
- to evaluate the image quality on a day-to-basis;
- to ensure results of quality tests are documented in a quality control log and maintained for the life of the system and/or records;
- when rescanning of a batch or page(s) is necessary and that ensure the original image is replaced and batch numbering and audit trail procedures are not compromised;
- for all image processing techniques;
- to provide evidence that the use of de-speckling has been disabled;
- to ensure complete and correct indexing of every record;
- to ensure results of accuracy checking are maintained;
- when data (and associated metadata) is received from another compliant system;
- to provide evidence of departmental indexing rules (manual and/or automated);
- to ensure system specific training is being provided to ensure that departmental indexing requirements are followed;
- to check and amend inaccurate index data and ensure audit trails are maintained;
- to retain source documents when scanning fails to capture all relevant data;
- to ensure quality control when source is not scanned, but information is collected through data entry/capture;
- to delete/purge records at the end of the retention period including appropriate authorization(s) and sign-off(s);
- when system and/or software is upgraded or changed;
- to ensure that digitally-born records are captured, indexed and verified; and,
- to check and validate complete indexing process and the amendment of indexing data if necessary.

5 Technical Controls and Audit Trails

The following technology observations have been made which confirm the system is fully compliant:

- The system complies with all requirements set forth by the Riverside County Information Security Standards and Specifications in accordance with the Riverside County Enterprise Information Security Policy (Board of Supervisors Policy A-58.)
- Departmental system recovery procedures exist and will be maintained and secured in a manner that supports authenticity of original data.
- System audit trails are maintained for all backup activity, including any problems incurred during the procedure.
- Departmental procedures exist and are followed for checking that the file integrity has not be compromised following a restore.
- Departmental procedures exist and are followed to ensure backup media is tested at regular intervals.
- Departmental procedures exist and are followed when performing regular system maintenance, including a detailed maintenance log stating the preventative and corrective maintenance procedures completed.
- Documentation of version control procedures (manual or automated) is maintained including departmental procedures to ensure that superseded versions are kept for the same length of time as the relevant information.
- Departmental procedures exist and are followed to ensure that all policy and procedural documentation is maintained, updated as appropriate and accessible.
- Documentation of system facilities are in place that ensure the integrity of stored information, including during transfer to and from storage media.
- Quantitative documentation of compression techniques including the algorithm used exist and are maintained.
- Documentation including a description of how the system's hardware and media will be protected from adverse environmental influences.
- Audit trail records of system historical activities or events that may need to be reconstructed in the future exist and are maintained.
- Audit trail records contain sufficient data points to ensure evidence of integrity and authenticity.
- Documentation of how audit trails will be accessed and interpreted and by whom exist and are maintained.
- The system prevents modification or deletion of record throughout its approved retention period.
- The system accurately reproduces the original record in all details.
- The system supports authorized versioning by creating a new record reflecting each modification (or single point in time modifications) without altering the original.
- The imaging/intake process uses industry standard image file formats to include JPEG, JBIG, JPEG2000, or PDF/A.
- PDF/A is used and compliant with ISO Standard 19005-1:2005 Part 1.
- Imaging compression that supports ITU Group 4, LZW, JPEG, JPEG 2000, or JBIG is employed.
- Minimum image scanning resolution is 300 dpi.
- Storage management/monitoring is implemented to ensure that ECMS has sufficient capacity for accurate reproduction of the records.

- The system employs an architecture that will allow data import/export to allow for migration to new platforms when EOL/S is reached.
- The system employs granular access control lists (ACLs) and/or other security controls to prevent unauthorized access.
- The system is backed up on a regular basis.
- The system is capable of deleting records on a specified schedule.
- The system is capable of suspending deletion schedules in the event of a legal hold or CPRA request.
- The system is capable of permanently deleting records in accordance with court-ordered legal purges.
- The system requires human (manual) intervention for the deletion of records that have met or exceeded their minimum retention period.
- The system supports the principles of least privilege and separation of duties via ACL(s), role-based access controls (RBAC), and/or other methods.
- Changes to the system are subject to formal, documented change control and patch management processes, and all resultant modifications/changes are reviewed and documented.
- The system produces and secures two copies of all records, which are stored in physically separate locations.
- The system enforces auditing and logging of logical access attempts (successful and failed), and all additions, modifications, and deletions of records.
- A Business Continuity Plan (Disaster Recovery Plan) is maintained for the system.

6 ISO Attestation

By signing below, I hereby acknowledge and certify that my office has determined REDS to meet all of the conditions of a trusted system and that official electronic records maintained in REDS are considered to be true and accurate copies of the original information received.

Name: Sebron K. Partridge

Position/Title: Chief Information Security Officer

Signature: Date 2/9/15