

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

454



FROM: Assessor-County Clerk-Recorder / Records Management and Archives Program

SUBMITTAL DATE:
July 11, 2011

SUBJECT: Addition of Board Policy A-68 "Trustworthy Official Electronic Records Preservation"

RECOMMENDED MOTION: That the Board of Supervisors approve the addition of Policy A-68 "Trustworthy Official Electronic Records Preservation" to the Board of Supervisors Policy Manual.

BACKGROUND: As a government agency of the State of California, the County must take steps to ensure that its official electronic records are stored in a "trusted system" as defined by Government Code Section 12168.7, which reads in part, "a '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." The Secretary of State has the responsibility to establish uniform statewide standards for trustworthy electronic documents. It is anticipated that the Secretary will adopt regulations to more clearly define the trusted system requirements of Section 12168.7 of the Government Code and which will incorporate portions of the Association of Information and Image Management's Recommended Practice on "Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)" (hereafter "AIIM ARP1-2009").

continued

Larry W. Ward, Assessor/County Clerk/Recorder

FINANCIAL DATA	Current F.Y. Total Cost:	\$ 0	In Current Year Budget:	NA
	Current F.Y. Net County Cost:	\$ 0	Budget Adjustment:	NA
	Annual Net County Cost:	\$ 0	For Fiscal Year:	NA

SOURCE OF FUNDS: NA	Positions To Be Deleted Per A-30	<input type="checkbox"/>
	Requires 4/5 Vote	<input checked="" type="checkbox"/>

C.E.O. RECOMMENDATION: APPROVE

BY: Karen L. Johnson

County Executive Office Signature

MINUTES OF THE BOARD OF SUPERVISORS

On motion of Supervisor Buster, seconded by Supervisor Benoit and duly carried, IT WAS ORDERED that the above matter is approved as recommended.

Ayes: Buster, Stone, Benoit and Ashley
 Nays: None
 Absent: Tavaglione
 Date: July 26, 2011
 xc: All Dept's., COB

Kecia Harper-Ihem
 Clerk of the Board
 By: Deputy

Prev. Agn. Ref.: | **District:** all | **Agenda Number:** 3.12

FISCAL PROCEDURES APPROVED
 PAUL ANGIULO, CPA, AUDITOR-CONTROLLER
 BY: RUSSELL S. DOMINSKI 7-13-11
 Nathany Coleby, CID 7/13/11
 Departmental Concurrence
 FORM APPROVED COUNTY COUNSEL
 BY: 7/13/2011
 DATE
 Dawn V. Lieu
 Policy Consent
 Policy Consent
 Dep't Recomm.: Per Exec. Ofc.:

**SUBJECT: Addition of Board Policy A-68
Trustworthy Official Electronic
Records Preservation**

PAGE: 2

The County of Riverside has chosen a proactive approach toward trusted systems and formed a committee to develop a recommended policy for the trustworthy storage of electronic records. The Committee utilized documents provided by the Secretary of State (including AllM ARP1-2009 and the text of the proposed regulations), other relevant state codes and established Board policies to create a concise document that, if followed, will reasonably assure the creation and maintenance of a trusted system by each County department, agency or district.

Compliance with this policy will be monitored by the Auditor-Controller's Internal Audit Team, the Riverside County Information Technology Department and the Records Management and Archives Program.

Purpose	3
Authority	3
Applicability	3
Policy	3
A. Responsibility of Department Heads.....	3
B. Prohibited Destruction of Certain Official Records.....	3
C. Official Record Storage Using Electronic Technologies	4
1. Electronic Content Management System (ECMS).....	4
2. Existing Departmental ECMS.....	4
3. Implementation of New ECMS	4
D. Departmental Compliance	4
1. Trusted System Requirements.....	4
2. Additional Requirements Pursuant to Other Applicable Law	5
E. Procedural Standards for Official Electronic Records.....	5
1. Business Practices Procedures.....	5
2. Quality Control for Scanning and Indexing.....	5
3. Departmental Records Retention Schedule Requirement	6
4. Accessibility of Official Electronic Records.....	6
5. Suspending Deletion of Official Electronic Records.....	6
F. Technology Standards for Official Electronic Records.....	6
1. Two Separate Official Electronic Records.....	6
2. Image File Formats for Converted Official Records	7
3. Document Image Compression.....	7
4. Image Quality Requirement.....	7
5. Sufficient Data Storage Capacity	7
6. Data Migration	7
7. Vendor Written Certification.....	8
G. Administrative Standards for Official Electronic Records	8
1. Cost / Benefit Analysis.....	8
2. ECMS Technology Procurement.....	8
3. Standard Forms	8
4. Departmental Cooperation with RMAP	8
5. Departmental Records Personnel	8
6. Custodian of Official Electronic Records	8
7. Training on Trusted System	9
8. Audits.....	9
H. Assessment Team	9

1. Evaluation of Departmental ECMS.....	9
2. Assessment Report on Trusted System.....	9
I. Conditions for Destruction of Official Records.....	10
1. Destruction Is Not Prohibited by Law	10
2. Assessment Report on Trusted System.....	10
3. Department Head Ensures Compliance.....	10
4. Board Approval and Resolution.....	10
5. Updated Departmental Records Retention Schedule	10
J. Requirements for Submittals to the Board of Supervisors	11
1. Departmental Submittal for Board Approval and Resolution.....	11
2. Departmental Notice to RMAP with Documentations.....	11
3. RMAP Submittal of Updated Departmental Records Retention Schedule.....	11
4. Concurrent Submittals to the Board of Supervisors	11
K. Definitions.....	11
1. AIIM	11
2. AIIM ARP1-2009.....	11
3. Board Policy A-43.....	11
4. ECMS	11
5. Electronically originated documents.....	12
6. Electronic documents	12
7. ISO.....	12
8. Official records.....	12
9. Official electronic records	12
10. PDF/A	12
11. RCIT	
12. RMAP	12
13. Trusted system requirements.....	12
Attachment A – Template Resolution.....	14

Purpose

The Board of Supervisors recognizes the need to establish uniform countywide standards to ensure that official records of the County of Riverside, when maintained electronically, complies with the trusted system requirements, are true and accurate representations of the original information, and remain accessible for the duration of the records' applicable retention period.

Authority

This policy is adopted in consideration of the provisions of Government Code sections 26205 and 26205.1; Government Code section 12168.7 pertaining to standards for recording permanent and nonpermanent documents in electronic media and trusted system; and Board Policy A-43 pertaining to County Records Management and Archives Policy, including Section C.7 (standards on electronic format).

Government Code sections 26205 and 26205.1 allows the Board of Supervisors, at the request of a County officer, to authorize the destruction of any official record that is not expressly required to be filed and preserved if the official record is electronically recorded on a trusted system that does not permit additions, deletions, or changes to the original record images, is produced in compliance with Government Code section 12168.7, accurately reproduces the original record, and is conveniently accessible.

Applicability

This policy regarding trustworthy official electronic record preservation applies to County departments that:

1. Create or store electronic documents as the official records of the County;
2. Intend on destroying the original hardcopy and maintaining the electronic documents as the official records of the County; or
3. Maintain electronically originated documents as the official records of the County.

Such departments shall comply with this policy and implement or exceed the minimum standards established herein.

Policy

A. Responsibility of Department Heads

It is the responsibility of department heads to ensure their departmental ECMS is a trusted system and departmental compliance with the trusted system requirements, this policy and the associated departmental procedures on trusted system, and Board Policy A-43.

For purpose of this policy, "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 and is further defined in Section 5.3.3 of AllIM ARP1-2009.

B. Prohibited Destruction of Certain Official Records

Departments shall not destroy: (i) official records that are expressly required by law to be filed and preserved; and/or (ii) official records that are required by law to be retained in hardcopy format. This policy shall not be construed to allow a department to maintain such official records electronically in place of the original hardcopy.

C. Official Record Storage Using Electronic Technologies

1. Electronic Content Management System

Electronic Content Management System ("ECMS") means any electronic technology implemented by the department to create, store, manage and/or reproduce official electronic records, and includes, without limitations, the electronic technologies identified in Section K.4 of this policy.

2. Existing Departmental ECMS

A department that has an existing Electronic Content Management System in place prior to the effective date of this policy must:

- a. Ensure its ECMS is evaluated by the Assessment Team to the greatest extent technologically and procedurally possible in order to ensure that official electronic records are stored in a trusted system;
- b. Comply with this policy as soon as practicable;
- c. Secure, as soon as practicable, the Board of Supervisors' approval on trusted system.

3. Implementation of New ECMS

A department that implements a new Electronic Content Management System on or after the effective date of this policy must:

- a. Ensure its ECMS is designed in accordance with Section 6.2 of AIRM ARP1-2009;
- b. Comply with this policy.
- c. Secure the Board of Supervisor's approval on trusted system.

D. Departmental Compliance

1. Trusted System Requirements

A department that maintains official electronic records in its departmental ECMS must:

- a. Ensure the ECMS is a trusted system that does not permit additions, deletions, or changes to the original official records.
- b. Produce the official electronic records in compliance with the trusted system requirements, as defined in Section K.13 of this policy.
- c. Use ECMS technology that accurately reproduces the original official records in all details and does not permit additions, deletions, or changes to the original official record images.
- d. Ensure that the official electronic records in the ECMS is conveniently accessible and ensure provision is made for preserving, examining and using such records for the duration of the records' applicable retention period.
- e. Separately maintain a duplicate copy of the official electronic records contained in the ECMS that does not permit additions, deletions, or changes to the original record images.

2. Additional Requirements Pursuant to Other Applicable Law

If the official records and/or official electronic records of the department are subject to additional requirements pursuant to other applicable law, department must ensure compliance with such additional requirements.

E. Procedural Standards for Official Electronic Records

1. Business Practices Procedures

- a. Department must develop and implement departmental procedures documenting its business practices on the creation, management and storage of official electronic records in a trusted system that are consistent with this policy and in conformance with Section 6.17 of AIIM ARP1-2009.
- b. Before implementing its ECMS, department must prepare its business practices procedures on trusted system. Such business practices procedures shall include the following information:
 - (i) Description of how original hardcopy of official records will be scanned, indexed, and verified;
 - (ii) Description of how the ECMS will be secured from unauthorized access;
 - (iii) Description of how official electronic records will be secured from unauthorized modification or alteration;
 - (iv) Description of how authorized modification of official electronic records will be managed, including audit trail information and ability to retrieve any previous version required to be maintained.
 - (v) Description of how notes and annotations (if any) will be stored and managed, if they are part of the official electronic records;
 - (vi) Description of how this policy and the departmental procedures on trusted system will be followed;
 - (vii) Description of how the ECMS will adhere to Board Policy A-43, County General Records Retention Schedule and Board-approved Departmental Records Retention Schedule.
 - (viii) Description of how functional roles of departmental personnel are separated to ensure error checking.
- c. Department must update its departmental procedures on trusted system to reflect any modifications of its ECMS. Such departmental procedures, when updated, must clearly state when the modifications took effect and what areas were affected.
- d. Department shall require all personnel using departmental ECMS to follow this policy and its departmental procedures on trusted system.

2. Quality Control for Scanning and Indexing

To ensure quality control for scanning and indexing official records, department shall require all personnel performing scanning and indexing to:

- a. Check and validate the complete scanning and indexing process;
- b. Facilitate the re-scanning and indexing process;

- c. Verify readability of each page or each document;
- d. Verify proper indexing of each document;
- e. Verify accurate page counts for each document; and
- f. Verify accurate security for each document.

3. Departmental Records Retention Schedule Requirement

Department must evaluate its current recordkeeping as follows:

- a. Conduct an inventory of the official records of each division and section;
- b. Identify all disposable official records pursuant to the applicable records retention schedules;
- c. Identify all official records to be retained pursuant to the applicable records retention schedules; and
- d. Destroy any backlog of outdated non-records.

Unless all official records of the department are subject to County General Records Retention Schedule, the department must secure the Board of Supervisor's approval of its Departmental Records Retention Schedule in accordance with Board Policy A-43.

4. Accessibility of Official Electronic Records

- a. Official electronic records are subject to the records' applicable retention periods as provided in the County General Records Retention Schedule and/or the Board-approved Departmental Records Retention Schedule.
- b. Department must ensure that official electronic records maintained in its departmental ECMS remain conveniently accessible during the records' applicable retention period.

5. Suspending Deletion of Official Electronic Records

Official electronic records that are scheduled to be deleted pursuant to the records' retention period shall be suspended by the department if:

- a. The department receives notice of pending litigation, reasonably anticipated litigation, an audit, or records request prior to the expiration of such records' retention period; and
- b. Such official electronic records are relevant to the litigation, audit or records request.

The deletion of such official electronic records will be suspended until the final resolution of the litigation, audit and/or records request.

F. Technology Standards for Official Electronic Records

1. Two Separate Official Electronic Records

Department must ensure at least two (2) separate official electronic records are created in the departmental ECMS that meets all of the conditions of a trusted system as identified in Section 5.3.3 of AIIIM ARP1-2009, including:

- a. *Prevent Unauthorized Modification.* The ECMS must utilize both hardware and media storage methodologies to prevent unauthorized additions, modifications or deletions during the official electronic record's retention period.
- b. *Verifiable Through Independent Audit.* The ECMS must be verifiable through independent audit processes ensuring that there is no plausible way for the official electronic record to be modified, altered, or deleted during such record's retention period.

- c. *Stored in a Safe and Separate Location.* The ECMS must write at least one copy of the official electronic record into electronic media that does not permit unauthorized additions, deletions, or changes to the original and that is to be stored and maintained in a safe and separate location.

Department must ensure every official electronic record maintained in the departmental ECMS is considered to be a true and accurate copy of the original information received.

2. Image File Formats for Converted Official Records

- a. Department must use industry standard (non-proprietary) image file formats for all official records that are scanned or otherwise converted into electronic format. Industry standard image file formats include JPEG, JBIG, JPEG 2000, or PDF-A.
- b. If PDF/A is chosen as the image file format for long-term storage of official electronic records, department must follow ISO Standard 19005-1:2005 Part 1.
- c. The use of any other image file format not specified herein is prohibited, unless the department obtains the vendor's certification or RCIT's verification pursuant to Section F.7 of this policy that such image file format is industry standard (non-proprietary) and complies with Section 5.4.1.4 of AIIIM ARP1-2009.

3. Document Image Compression

Department must use image compression/decompression that supports ITU Group 4, LZW, JPEG, JPEG 2000, or JBIG. The use of any other image compression technology not specified herein is prohibited, unless the department obtains the vendor's certification or RCIT's verification pursuant to Section F.7 of this policy that such technology:

- a. Supports output format standards with no proprietary alterations of the algorithms;
- b. Does not include extraneous information unsupported by relevant industry standards; and
- c. Complies with Section 5.4.2.4 of AIIIM ARP1-2009.

4. Image Quality Requirement

Department must use minimum scanning resolution of 300 dots per inch (dpi) to ensure image quality for official electronic records.

5. Sufficient Data Storage Capacity

Department must ensure the data storage capacity of its ECMS is sufficient for accurate reproduction of the official electronic records.

6. Data Migration

- a. Department must make every effort to ensure its ECMS employs an open systems (industry standard or non-proprietary) architecture that will allow County to migrate official electronic records to new platforms as ECMS technology advances.
- b. Prior to the implementation of data migration, department must create a specific migration plan to integrate official electronic records from older to newer hardware and software platforms to ensure proper integration without adversely affecting the official electronic records managed by the older ECMS technology.

7. Vendor Certification or RCIT Verification

Department must obtain the vendor's written certification that its ECMS technology is in compliance with the applicable technology standards of Section F of this policy. However, a department with an existing ECMS prior to the effective date of this policy may obtain RCIT's written verification in lieu of the vendor's written certification.

G. Administrative Standards for Official Electronic Records

1. Cost/Benefits Analysis

Prior to investing in new ECMS technology, the department must conduct a cost/benefits analysis to ensure that such ECMS will reduce records personnel and storage costs and allow official records to be managed more productively.

2. ECMS Technology Procurements

Prior to selecting an ECMS technology vendor, department must develop a request for proposal document that:

- a. Requires vendors to certify in writing their technology is in compliance with the applicable technology standards of Section F of this policy; and
- b. Contains sufficient information regarding specific requirements of the ECMS technology and departmental expectations to enable vendors to clearly understand the business and technical goals and operational requirements of the department and to ensure the ECMS technology achieves anticipated results.

3. Standard Forms

- a. RMAP, in consultation with Executive Office and County Counsel, shall develop, as appropriate, standard forms to facilitate the implementation of this policy, including vendor's certification and RCIT's verification. RMAP shall further consult RCIT regarding any standard forms that relate to the technology standards of this policy.
- b. Departments shall utilize standard forms that are developed by RMAP pursuant to this Section G.3. RMAP shall make such standard forms available to departments upon request.

4. Departmental Cooperation with RMAP

Departments shall cooperate with RMAP to meet the intent of this policy.

5. Departmental Records Personnel

Department head shall designate records personnel to enforce and monitor compliance with this policy and the departmental procedures on trusted system.

6. Custodian of Official Electronic Records

- a. To ensure County official electronic records are admissible evidence, department head shall designate a custodian of official electronic records to authenticate the official electronic records that are maintained in the departmental ECMS.
- b. The custodian of official electronic records shall be sufficiently knowledgeable about the departmental ECMS (including how official electronic records are collected and assembled), trusted system, this policy and the associated departmental procedures on trusted system.

7. Training on Trusted System

Records personnel, with the following responsibilities, must attend training conducted by the Office of Secretary of State or a seminar sponsored by AIIM or the State of California on trusted system:

- a. Designing departmental ECMS;
- b. Enforcing this policy or the departmental procedures on trusted system; and
- c. Designated as the departmental custodian of official electronic records.

8. Audits

Within two (2) years after the most recent prior audit or evaluation of the departmental ECMS as a trusted system, department head shall ensure the departmental ECMS is audited by the Internal Audit Division of the County Auditor-Controller's Office and RCIT to verify there is no plausible way for the official electronic records to be modified, altered, or deleted during such records' retention period. Such audit must also be conducted whenever significant modifications are made to the departmental ECMS.

The Internal Audits Division of the County Auditor-Controller's Office will make determinations relevant to the department's trusted systems documentation and procedures with regard to the departmental ECMS. RCIT will make determinations relevant to the technology employed to ensure that there is no technological means of unauthorized modification to an official record stored within the ECMS.

If the result of the audit is a finding indicating a deficiency in the departmental ECMS that would place in doubt the integrity of the official electronic records stored, then the department must suspend the destruction of the official records in hard copy format until a positive finding is released.

If a department is not audited on its two-year cycle for any reason, the department may choose to secure an audit from an agency outside of the County. If so, a copy of the audit must be provided to the ACO Internal Audit Division, RCIT and RMAP.

H. Assessment Team

1. Evaluation of Departmental ECMS

Assessment Team means an external auditing entity retained by a department to evaluate its departmental ECMS to the greatest extent technologically and procedurally possible in order to ensure that official electronic records are stored in a trusted system. The Assessment Team must be sufficiently knowledgeable about the trusted system requirements.

The Assessment Team will evaluate departmental ECMS for compliance with the trusted system requirements, this policy and the departmental procedures on trusted system.

2. Assessment Report on Trusted System

The Assessment Team shall prepare an Assessment Report on its evaluation of the departmental ECMS as a trusted system. The Assessment Report shall include:

- a. Findings on departmental compliance and/or deficiency with respect to the trusted system requirements, this policy and the departmental procedures on trusted system.
- b. Where appropriate, recommendations of improvements in departmental procedural and administrative practices.
- c. Where appropriate, recommendations of improvements in technical implementations.

- d. Where applicable, findings on departmental corrections of any deficiencies and/or implementations of recommended improvements.
- e. Determinations on whether two (2) separate official electronic records are created in the departmental ECMS that meets all of the conditions of a trusted system as identified in Section 5.3.3 of AIRM ARP1-2009 and Section F.1 of this policy.
- f. Determinations on whether the official electronic records maintained in the departmental ECMS are considered to be true and accurate copy of the original information received.

I. Conditions for Destruction of Official Records

Department head with custody of departmental official records may cause the original hardcopy of such official records to be destroyed and maintain such official records electronically in its departmental ECMS only if all of the following conditions are satisfied:

1. Destruction Is Not Prohibited by Law

The official records are not expressly required by law to be file and preserved, and/or required by law to be retained in hardcopy format.

2. Assessment Report on Trusted System

The Assessment Team determined in its Assessment Report that:

- a. At least two (2) separate official electronic records are created in the departmental ECMS meeting all of the conditions of a trusted system; and
- b. The official electronic records maintained in the departmental ECMS are considered to be true and accurate copies of the original information received.

3. Department Head Ensures Compliance

Department head ensures departmental ECMS is a trusted system, and departmental compliance with the trusted system requirements, this policy and the departmental procedures on trusted system, and Board Policy A-43.

4. Board Approval and Resolution

Department head secured the Board of Supervisors' approval of departmental ECMS as a trusted system, and a resolution adopted by the Board of Supervisors pursuant to Government Code section 26205.1(a) authorizing the department head to destroy the original hardcopy and maintain the official records electronically in the departmental ECMS.

5. Updated Departmental Records Retention Schedule

The Departmental Records Retention Schedule is updated by RMAP in accordance with the Board of Supervisors' resolution described in Paragraph 4 above, and approved by the Board of Supervisors.

The conditions set forth in Paragraphs 1 through 3 above must first be satisfied before the department head may secure the necessary approval and resolution from the Board of Supervisors pursuant to Paragraph 4. Submittals to the Board of Supervisors under Paragraphs 4 and 5 must be concurrent.

J. Requirements for Submittals to the Board of Supervisors

1. Departmental Submittal for Board Approval and Resolution

To secure Board approval and resolution pursuant to Section I.4, department head must submit to the Board of Supervisors a fully executed Form 11 in conjunction with the following documents:

- a. The Assessment Report on trusted system as described in Section I.2.
- b. Proposed resolution that satisfies all conditions set forth in Section I and substantially conforms with Attachment A, Template Resolution.

2. Departmental Notice to RMAP with Documentations

Departments intending to secure Board approval and resolution pursuant to Section I.5 shall notify RMAP utilizing a notification form developed by RMAP and provide RMAP with a copy of the Assessment Report on trusted system and departmental proposed resolution.

3. RMAP Submittal of Updated Departmental Records Retention Schedule

Pursuant to Section D.9 of Board Policy A-43, all proposed and updated department records retention schedule shall be submitted on behalf of the departments by RMAP to the Board of Supervisors for approval.

RMAP may, as it determines appropriate, update the departmental records retention schedule in accordance with the departmental proposed resolution, or alternatively, confer with the department to resolve any issues.

4. Concurrent Submittals to the Board of Supervisors

Department shall coordinate with RMAP to ensure that the departmental submittal for Board approval and resolution under Section J.2 is concurrent with the updated departmental records retention schedule submitted by RMAP on behalf of the department under Section J.4.

K. Definitions

As used in this Policy, the following definitions shall apply:

1. "AIIM" means the Association for Information and Image Management.
2. "AIIM ARP1-2009" refers to the AIIM ARP1-2009 Analysis, Selection, and Implementation of Electronic Document Management Systems approved on June 5, 2009. AIIM ARP1-2009 may be downloaded directly from AIIM at www.aiim.org/standards, or from the California Secretary of State at www.sos.ca.gov/archives/local-gov-program.
3. "Board Policy A-43" means Board of Supervisors' Policy A-43 entitled Records Management and Archives Policy.
4. ECMS, includes, but is not limited to, the following electronic technologies:
 - a. Document imaging technologies that are used to convert hardcopy into electronic format;
 - b. Document or library services technologies that are used to manage electronically originated documents;

Subject:

TRUSTWORTHY OFFICIAL ELECTRONIC RECORDS PRESERVATION

Policy No.
A-68

Page
12 of 17

- c. Business process management or workflow technologies that are used to automate work processes including the creation, routing, tracking, and management of information being processed;
 - d. Enterprise report management technologies that are used to store electronic formatted reports;
 - e. Forms processing technologies that are used to incorporate interactive forms and manage related forms data;
 - f. Optical character recognition or intelligent character recognition technologies; and
 - g. Various applications also considered as add-ons such as records management applications, legacy systems and integration tools.
5. "Electronically originated documents" includes any document or record created without first having originated in hardcopy format. It includes all documents or records generated through electronic submissions.
 6. "Electronic documents" means electronically originated documents or hardcopy documents or records that have been scanned or otherwise converted into electronic format.
 7. "ISO" means the International Organization for Standardization. ISO documents referred to in this policy may be purchased from AIIM at www.aiim.org/standards.
 8. "Official records" shall include official documents or official records that are: (i) defined as such in applicable statutes and in the business practices of County departments that are responsible for retaining said documents or records; (ii) identified in County General Records Retention Schedule; or (iii) identified in the Board of Supervisors' approved departmental records retention schedules.
 9. "Official electronic records" are electronic documents that are created or stored by County departments as the official records of the County.
 10. "PDF/A" means Portable Document Format/Archive, which is an electronic file format whereby documents are self-contained allowing them to be reproduced with all of the document coding embedded within the file.
 11. "RCIT" means Riverside County Information Technology.
 12. "RMAP" means Riverside County Records Management and Archives Program.
 13. "Trusted system requirements" means the following requirements:
 - a. Government Code sections 26205 and 26205.1.
 - b. Government Code section 12168.7, including but not limited to the minimum standards or guidelines, or both, as recommended by the American National Standards Institute or AIIM for recording of permanent records or nonpermanent records.
 - c. The following sections of AIIM ARP1-2009:
 - (i) Section 5.3.3 – Trusted system and legal considerations;
 - (ii) Section 5.4.1.4 – Image formats;
 - (iii) Section 5.4.2.4 – Document image compression;
 - (iv) Section 6.2 – Recommended project steps; and
 - (v) Section 6.17 – Business practices documentation.

- d. The concepts contained in ISO 15801 on Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability.
- e. The concepts contained in ISO 15489, Part 1 governing Information and documentation – Records management.
- f. ISO 19005-1:2005, Part 1 governing Use of PDF 1.4 (PDF/A-1), only if PDF/A is chosen as the image file format for long-term storage.

**ATTACHMENT A
TEMPLATE RESOLUTION**

Board of Supervisors

County of Riverside

RESOLUTION NO. _____

**APPROVING [DEPARTMENT NAME]'S ELECTRONIC CONTENT MANAGEMENT SYSTEM AND
AUTHORIZING [DEPARTMENT HEAD] TO DESTROY HARDCOPY OF OFFICIAL RECORDS AND
TO MAINTAIN SUCH OFFICIAL RECORDS ELECTRONICALLY**

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; and

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 the record is electronically recorded on a trusted system, does not permit additions, deletions, or changes to the original document images, is produced in compliance with Government Code section 12168.7, accurately reproduces the original record in all details, and is conveniently accessible, and if a duplicate copy of the electronic record contained in the trusted system that does not permit additions, deletions or changes to the original document images is also separately maintained; and

WHEREAS, in accordance with Government Code section 26205.1, the County officer having custody of County records that are not expressly required by law to be filed and preserved may cause to be destroyed such records if 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), the County officer who destroys any record maintains such record electronically in a trusted system that does not permit additions, deletions, or changes to the original record or other duplicate of the record and is produced in compliance with Government Code section 12168.7; and

WHEREAS, the Board of Supervisors has established Board Policy A-68, entitled Trustworthy Official Electronic Records Preservation, and [department name] has developed and implemented its associated departmental procedures on trusted system; and

WHEREAS, [department name] has a Board-approved departmental records retention schedule; and

WHEREAS, [department head] has custody of the following departmental official records series (hereafter "Official Records"):

Code	Title	Description	Official Record Retention

WHEREAS, the Official Records are not expressly required by law to be filed and preserved; and

(Insert either: [WHEREAS, the Official Records are not required by law to be retained in hardcopy format; and]

or: [WHEREAS, pursuant to [insert applicable law], the Official Records are required by law to be retained in hardcopy format for [insert hardcopy retention period]; and])

WHEREAS, the Official Records are maintained electronically in the Electronic Content Management System of [department name] (hereafter "ECMS"); and

WHEREAS, the ECMS has been evaluated by an Assessment Team, [company name], to the greatest extent technologically and procedurally possible in order to ensure that the Official Records are electronically stored in a trusted system. The Assessment Team concluded in its Assessment Report that: (i) at least two (2) separate official electronic records are created in the ECMS meeting all of the conditions of a trusted system; and (ii) the official electronic records maintained in the ECMS are considered to be true and accurate copies of the original information received; and

WHEREAS, [department head] has ensured that: (i) the ECMS is a trusted system, is produced in compliance with Section 12168.7 of the Government Code, and does not permit additions, deletions,

or changes to the original record or other duplicate of the record; (ii) the official electronic records maintained in the ECMS shall remain conveniently accessible for the duration of the records' applicable retention period; and (iii) a duplicate copy of the official electronic records contained in the ECMS that does not permit additions, deletions, or changes to the original document images is also separately maintained; and

WHEREAS, [department head] has further ensured departmental compliance with the trusted system requirements, Board Policy A-68 and the associated departmental procedures on trusted system, and Board Policy A-43; and

(Insert if applicable: WHEREAS, pursuant to *[insert applicable law]* the Official Records and/or official electronic records in the ECMS are subject to the following additional requirements: *[insert additional requirements]*. [Department head] has ensured compliance with these additional requirements; and)

WHEREAS, *[insert additional information if necessary]*; and

WHEREAS, Board Policy A-68 requires the department head to secure the Board of Supervisors' approval of the 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 destroy the original hardcopy of the Official Records that are maintained electronically in the ECMS; and

WHEREAS, Board Policy A-68 further requires the departmental records retention schedule be updated by County Records Management and Archives Program (hereafter "RMAP") on behalf of the department in accordance with this resolution.

NOW THEREFORE, BE IT RESOLVED AND ORDERED that the Board of Supervisors of the County of Riverside hereby approves the ECMS as a trusted system.

(Insert either: [BE IT FURTHER RESOLVED AND ORDERED that pursuant to California Government Code section 26205.1, subdivision (a), the Board of Supervisors of the County of Riverside hereby grants [department head] continuing authority to destroy the original hardcopy of the

Official Records and maintain such Official Records electronically in the ECMS for the records' applicable retention period.]

or: **[BE IT FURTHER RESOLVED AND ORDERED** that pursuant to California Government Code section 26205.1, subdivision (a), the Board of Supervisors of the County of Riverside hereby grants [department head] continuing authority to destroy the original hardcopy of the Official Records and maintain such Official Records electronically as follows:

1. As required by law, the original hardcopy of the Official Records shall be retained in hardcopy format for [*insert hardcopy retention period*]; and
2. After the expiration of the above stated retention period, the original hardcopy of the Official Records may be destroyed and maintained electronically in the ECMS for the remainder of such records' applicable retention period.]

BE IT FURTHER RESOLVED AND ORDERED that the Board of Supervisors of the County of Riverside hereby approves the updated departmental records retention schedule of [department name], which is concurrently but separately submitted by RMAP on behalf of [department name].

BE IT FURTHER RESOLVED AND ORDERED that if notice of litigation, reasonably anticipated litigation, audit or records request is received by [department name] 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 the ECMS shall be suspended by [department head] or his/her designee until the final resolution of the litigation, audit and/or records request.

BE IT FURTHER RESOLVED AND ORDERED that [*insert additional conditions if necessary*].