163

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

FROM: Riverside County Information Security Office

SUBMITTAL DATE:
December 5, 2013

SUBJECT: Revised Board Policy No. A-68 pertaining to Trustworthy Official Electronic Records Preservation

RECOMMENDED MOTION: That the Board of Supervisors:

1. Approve the revised Board Policy A-68 as set forth in Exhibit A; and,
2. Require the Information Security Office to provide an assessment status report to the Executive Office on an annual basis.

BACKGROUND:

Summary

On July 26, 2011, the Board adopted Policy A-68 to ensure that when departments elect to maintain official records in electronic format that they do so in accordance with the provisions of Government Code § 12168.7, including following the guidelines established by the Association of Information and Image Management, "AIIM ARP1-2009 Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)." (Continued on page 2)

Larry W. Ward
Assessor-County Clerk-Recorder

Sebron K. Partridge
Chief Information Security Officer

Kevin Crawford
Chief Information Officer

FINANCIAL DATA	Current Fiscal Year:	Next Fiscal Year:	Total Cost:	Ongoing Cost:	POLICY/CONSENT (per Exec. Office)
COST	$ NA	$ NA	$ NA	$ NA	Consent ☐ Policy ☑
NET COUNTY COST	$ NA	$ NA	$ NA	$ NA	

SOURCE OF FUNDS: NA

Budget Adjustment: NA

For Fiscal Year: NA

C.E.O. RECOMMENDATION: APPROVE

BY: Jennifer L. Sargent

County Executive Office Signature

MINUTES OF THE BOARD OF SUPERVISORS

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

Ayes: Jeffries, Stone, Benoit and Ashley
Nays: None
Absent: Tavaglione
Date: December 17, 2013
xc: ISO, ACR, RCIT, EO

Kecia Harper-Ihem
Clerk of the Board
By: Deputy

Prev. Agn. Ref.: 3.12 July 26, 2011 | **District:** ALL | **Agenda Number:** 3-31

Departmental Concurrence

FORM APPROVED COUNTY COUNSEL
BY: TAMMY D. LIEU DATE 12/5/13

☐ Positions Added ☐ Change Order
☐ A-30 ☒ 4/5 Vote

BACKGROUND:
Summary (continued)

Since the adoption of Board Policy A-68, the Secretary of State has adopted regulations to more clearly define the trusted system requirements of Government Code § 12168.7. These regulations necessitate revisions to Board Policy A-68. Specifically, the proposed revisions require compliance with California Code of Regulations Title 2, Division 7, Chapter 15 "Trustworthy Electronic Document or Records Preservation," Sections 22620.1 through 22620.8. The policy has been further revised to allow departments to utilize the Tagged Image File Format (TIFF) if certain conditions are satisfied and evaluated by the Information Security Office (ISO) for trusted system compliance.

In accordance with Board of Supervisors Policy A-43 § C.7, the Records Management and Archives Program (RMAP) participated in the initial development of and this revision to the policy in order to ensure that appropriate standards are maintained. Subject to the Board's approval, the ISO, the Riverside County Information Technology (RCIT) department, and RMAP mutually agree to transfer the responsibility of implementing and monitoring compliance with this policy to the ISO. Therefore, all electronic records systems shall be evaluated by the ISO for compliance with the trusted system requirements.

As this policy authorizes destruction of official county records when certain conditions have been met, a 4/5 vote by the Board of Supervisors is required pursuant to Government Code § 26202.

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 6
3. Quality Control for Electronically Originated Official Records 6
4. Departmental Records Retention Schedule Requirement 6
5. Accessibility of Official Electronic Records 6
6. Suspending Deletion of Official Electronic Records 7
F. Technology Standards for Official Electronic Records 7
1. Two Separate Official Electronic Records 7
2. Image File Formats for Converted Official Records 7
3. Document Image Compression 8
4. Image Quality Requirement 8
5. Sufficient Data Storage Capacity 8
6. Data Migration 8
7. Vendor Written Certification 9
G. Administrative Standards for Official Electronic Records 9
1. Cost / Benefit Analysis 9
2. ECMS Technology Procurement 9
3. Standard Forms 9
4. Departmental Cooperation with ISO 9
5. Departmental Records Personnel 9
6. Custodian of Official Electronic Records 9
7. Training on Trusted System 10
H. Assessment 10
1. Evaluation of Departmental ECMS 10
2. Assessment Report on Trusted Systems 10

3. Ongoing Compliance 10

I. Conditions for Destruction of Official Records 11

1. Destruction Is Not Prohibited by Law 11
2. Assessment Report on Trusted System 11
3. Department Head Ensures Compliance 11
4. Departmental Records Retention Schedule 11
5. Board Approval and Resolution 11

J. Requirements for Submittals to the Board of Supervisors 12

K. Definitions 12

1. AIIM 12
2. AIIM ARP1-2009 12
3. ANSI 12
4. Board Policy A-43 12
5. CCR 12
6. ECMS 12
7. Electronically originated documents 12
8. Electronic documents 12
9. ISO 13
10. Official records 13
11. Official electronic records 13
12. PDF/A 13
13. RMAP 13
14. TIFF 13
15. Trusted System 13
16. Trusted system requirements 13

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; California Code of Regulations Title 2, Division 7, Chapter 15 "Trustworthy Electronic Document or Records Preservation" Sections 22620.1 through 22620.8; 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 and 2 CCR 22620.1-22620.8, 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 AIIM 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.6 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 of the 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 AIIM ARP1-2009;

b. Comply with this policy.

c. Secure the Board of Supervisor's approval of the 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.16 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, 2 CCR 22620.5 Business Practice Documentation, 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) If applicable, description of how electronically originated official records will be captured, indexed and verified;

      (iii) Description of how the ECMS will be secured with appropriate access and from unauthorized access;

      (iv) Description of how official electronic records will be secured from unauthorized modification or alteration;

      (v) 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.

      (vi) Description of how notes and annotations (if any) will be stored and managed, if they are part of the official electronic records;

      (vii) Description of how this policy and the departmental procedures on trusted system will be followed;

      (viii) Description of how the ECMS will adhere to Board Policy A-43, County General Records Retention Schedule and Board-approved Departmental Records Retention Schedule.

      (ix) 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; and

e. Verify accurate page counts for each document.

3. Quality Control for Electronically Originated Official Records

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

a. Check and validate the complete indexing process;

b. Facilitate the re-indexing process;

c. Verify the proper indexing (accuracy) of each record; and

d. Verify search and access success for each batch.

4. 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.

5. 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.

6. 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 required by 2 CCR 22620.7 Trusted Storage of Official Electronic Documents or Records and as identified in Section 5.3.3 of AIIM 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 comply with 2 CCR 22620.8 Electronic File Format for Preservation of Converted Official Documents or Records, and 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, PDF-A or TIFF, under certain conditions detailed in subsection c. below.

b. If PDF/A is chosen as the image file format for long-term storage of official electronic records, department should follow "ANSI/AIIM/CGATS/ISO 19005-1:2005, Document Management – Electronic Document File Format for Long-Term Preservation - Part 1 Use of PDF 1.4 (PDF/A-1)," approved as ANSI Standards on June 15, 2008.

c. The use of TIFF is only permissible within existing ECMS, as defined in Section C.2 of this policy. Departments with existing ECMS that use TIFF image file format must comply with all of the following conditions:
   (i) Exercise caution when using TIFF and resolve all risks and problems associated with TIFF, including those identified in Section 5.4.1.4 of AIIM ARP1-2009 and specific to its ECMS.

(ii) Ensure compensating controls are in place to maintain a trusted system, and fully document:

- The structures, color maps and compensation methods to ensure the TIFF file created is accurate; and
- All compensating controls that secure the TIFF file from unauthorized modification or deletion.

(iii) Maintain and not destroy the County's original hardcopy until such time as the existing ECMS passes its two-year assessment as described in Section H.3. If the assessment findings support the trustworthiness of the TIFF images stored, then the County's original hardcopy may be destroyed in accordance with Board resolution and Board of Supervisors Policy A-43 § D.11. Destruction may only take place following successful completion of the trusted system assessment as described in Section H.3.

The Assessment Team must independently verify departmental compliance with all of the above conditions.

New ECMS, as defined in Section C.3 of this policy, must also be evaluated on a case-by-case basis to determine the business need for TIFF.

d. The use of any other image file format not specified herein is prohibited, unless the department obtains the vendor's certification 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 AIIM ARP1-2009.

3. Document Image Compression

Department must comply with 2 CCR 22620.6 Electronic File Compression, and 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 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 AIIM ARP1-2009.

4. Image Quality Requirement

Department must use at least the 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

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. A copy of this certification must be provided to the Assessment Team as part of the assessment process.

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.

4. Standard Forms

a. The ISO, in consultation with the Executive Office and County Counsel, shall develop, as appropriate, standard forms to facilitate the implementation of this policy, including template resolution and vendor's certification.

b. Departments shall utilize standard forms developed by the ISO pursuant to this Section G.4. ISO shall make such standard forms available to departments upon request.

4. Departmental Cooperation with ISO

Departments shall cooperate with the ISO 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 Information Security Office and/or other program approved by the ISO:

a. Designing departmental ECMS;

b. Enforcing this policy or the departmental procedures on trusted system;

c. Designated as the departmental custodian of official electronic records; or

d. Authorized users of the departmental ECMS.

H. Assessment

1. Evaluation of Departmental ECMS

The ISO has been designated as the Assessment Team, which means an independent auditing team that evaluates a department's 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 and this policy. 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 required by 2 CCR 22620.7 and identified in Section 5.3.3 of AIIM 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.

3. Ongoing Compliance

Within two (2) years after the most recent prior assessment of the departmental ECMS as a trusted system, department head shall ensure the departmental ECMS is re-evaluated by the ISO to verify there is no plausible way for the official electronic records to be modified, altered, or deleted during

such records' retention period. Such assessment must also be conducted whenever significant modifications are made to the departmental ECMS.

If the result of the assessment is a finding indicating any deficiencies 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 hardcopy format and implement a system wide hold against the deletion of official electronic records pursuant to the records' retention period until a subsequent finding is released that such deficiencies have been corrected by the department.

4. ISO's ECMS

No department may assess itself in fulfillment of this section. With respect to ISO's ECMS, ISO may, therefore, secure an assessment from an independent auditing agency or entity outside of the County ("Assessment Entity") to determine trusted system compliance. A copy of the assessment report shall be submitted to the Executive Office.

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 or, in the case of ISO's ECMS, the Assessment Entity 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. Departmental Records Retention Schedule

   Department head shall cooperate with RMAP to ensure that the Departmental Records Retention Schedule is current and approved by the Board of Supervisors.

5. 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.

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

J. Requirements for Submittals to the Board of Supervisors

To secure Board approval and resolution pursuant to Section I.5, department head must submit to the Board of Supervisors a fully executed Form 11 in conjunction with the following documents:

1. The Assessment Report on trusted system as described in Section I.2.

2. Proposed resolution that satisfies all conditions set forth in Section I that complies with this policy and substantially conforms to the template resolution provided by ISO.

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 http://www.aiim.org/standards/, or from the California Secretary of State at http://www.sos.ca.gov/archives/local-gov-program/.

3. "ANSI" means the American National Standards Institute

4. "Board Policy A-43" means Board of Supervisors' Policy A-43 entitled Records Management and Archives Policy.

5. "CCR" means California Code of Regulations.

6. "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;

   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.

7. "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.

8. "Electronic documents" means electronically originated documents or hardcopy documents or records that have been scanned or otherwise converted into electronic format.

9. "ISO" means Riverside County Information Security Office.

10. "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.

11. "Official electronic records" are electronic documents that are created or stored by County departments as the official records of the County.

12. "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.

13. "RMAP" means Riverside County Records Management and Archives Program.

14. "TIFF" means Tagged Image File Format.

15. "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 AIIM ARP1-2009.

16. "Trusted system requirements" means the following requirements:

    a. Government Code sections 25105, 26205, 26205.1, 26205.5, 26907, 27001, and 27322.2 and Welfare & Institutions Code section 10851, as applicable.

    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. State of California Title 2, Division 7, Chapter 15 Sections 22620.1 through 22620.8 "Trustworthy Electronic Document or Record Preservation."

    d. 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.

    e. The concepts contained in International Organization for Standardization 15801 on Electronic Imaging – Information stored electronically – Recommendations for trustworthiness and reliability.

    f. The concepts contained in International Organization for Standardization 15489, Part 1 governing Information and documentation – Records management.