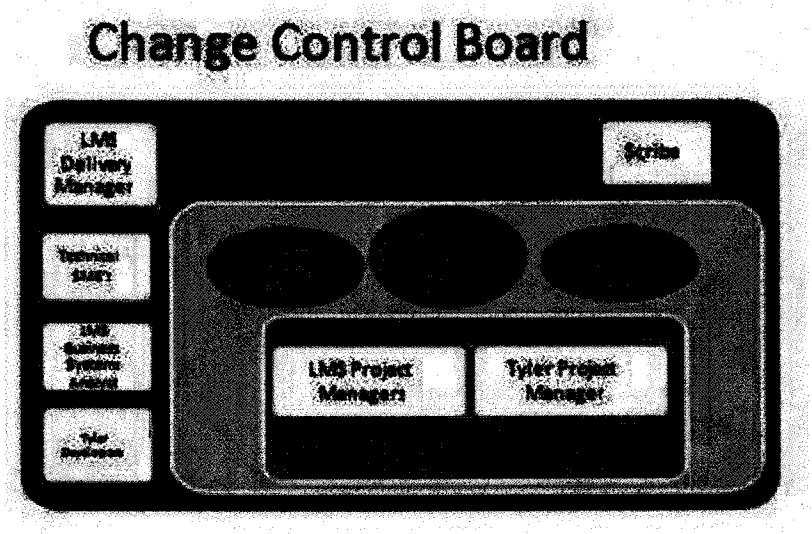
### 3.16.3 Change Control Board Participants, Roles and Responsibilities

The Change Control Board is depicted in the diagram below:



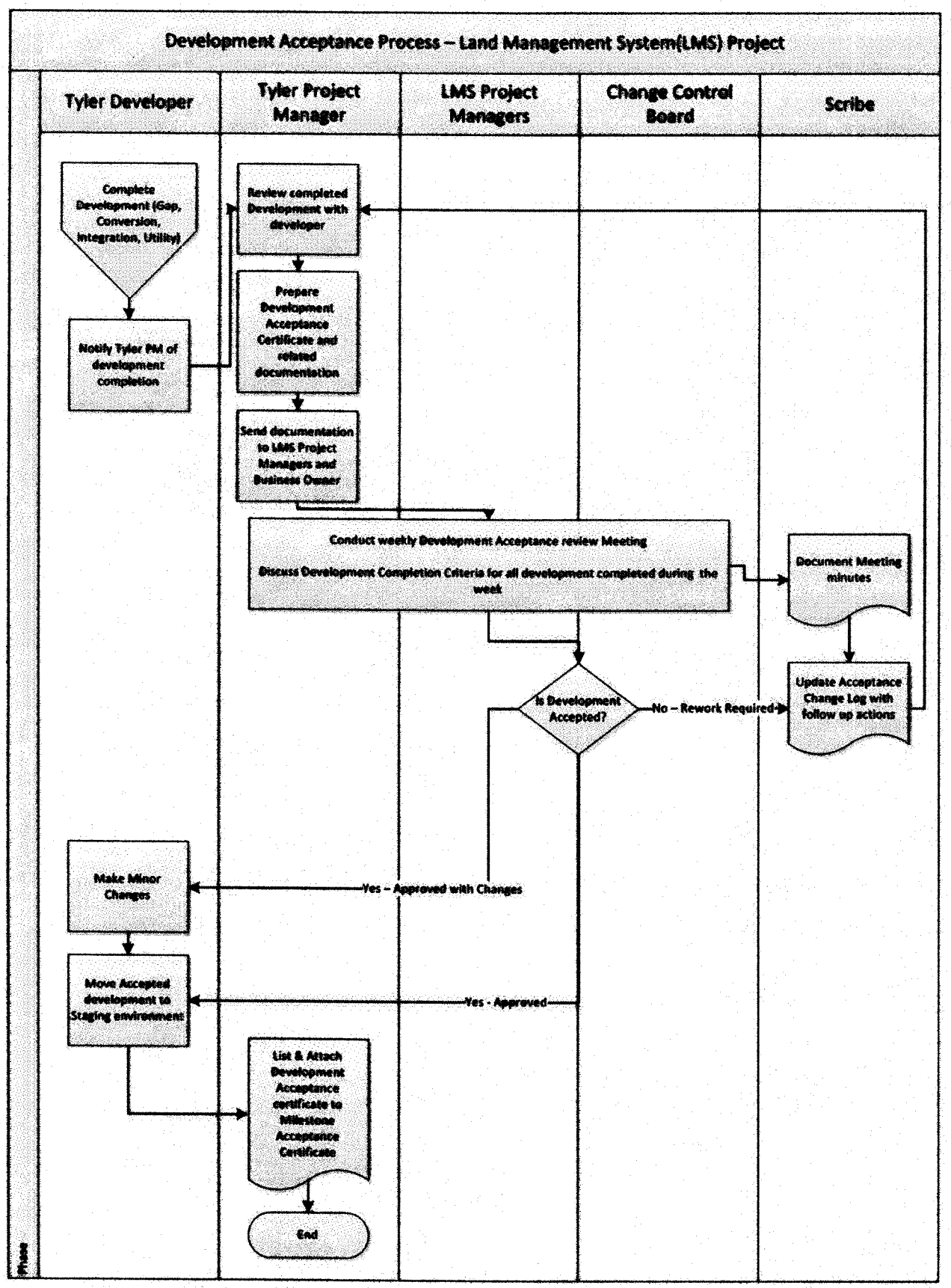

## Roles and Responsibilities

| Role | Responsibility |
|---|---|
| Project Managers | Refer to Attachment ROL - Roles and Responsibilities |
| TLMA Project Sponsor | Refer to Attachment ROL - Roles and Responsibilities |
| TLMA Business Owners | Refer to Attachment ROL - Roles and Responsibilities |
| Project Administrator – Scribe | Refer to Attachment ROL - Roles and Responsibilities |
| TLMA Business Systems Analyst | Refer to Attachment ROL - Roles and Responsibilities |
| TLMA SME Teams | Refer to Attachment ROL - Roles and Responsibilities |
| Tyler Developers | Refer to Attachment ROL - Roles and Responsibilities |

### 3.16.4 Development Acceptance Process

The Development Acceptance Process is pictured below.

*This space intentionally* left blank


Development Acceptance Process – Land Management System(LMS) Project
Tyler Developer
Tyler Project Manager
LMS Project Managers
Change Control Board
Scribe
Complete Development (Gap, Conversion, Integration, Utility)
Review completed Development with developer
Prepare Development Acceptance Certificate and related documentation
Notify Tyler PM of development completion
Send documentation to LMS Project Managers and Business Owner
Conduct weekly Development Acceptance review Meeting
Discuss Development Completion Criteria for all development completed during the week
Document Meeting minutes
Update Acceptance Change Log with follow up actions
Is Development Accepted?
No – Rework Required
Make Minor Changes
Yes – Approved with Changes
Move Accepted development to Staging environment
Yes - Approved
List & Attach Development Acceptance certificate to Milestone Acceptance Certificate
End
Phase

### 3.16.5 Status

The meeting participants will recommend one of the following status' at the Development Acceptance Meeting.

***Approved Status***:

The development is approved "as is" by the Change Control Board (CCB).

***Approved with Changes Status***:

The recommended changes / or actions are minor and can easily and quickly be addressed. The changes are understood by the business owners, business systems analysts, and the Project Managers. All parties agree that no further reviews are needed. The developer will make the changes and resolve the open actions. The business owner and business systems analyst will review the changes and confirm completion.

***Rework Required Status***:

If recommended changes and / or actions are required that significantly alter the development, the development will enter rework status, on terms and conditions to be mutually agreed to by the parties according to Attachment CHG. The entire Development Acceptance process will be repeated when the rework has been completed until the development has reached Approved Status.

### 3.16.6 Exit Criteria for Review

In order to closely manage the process for any Gap/Custom Enhancements identified in accordance with Attachment DEL, the exit process must be clearly defined. The exit criteria for the Development Acceptance process include:

- Items logged on the log of recommended changes and actions form has been verified by Project Managers as complete.
- The development is placed in the staging / test environment
- Completed log of recommended changes and actions is saved in the project shared directory for archival and audit purposes.

### 3.16.7 Milestone Acceptance Process

Goals of the Milestone Acceptance Process

The primary goals of the Milestone Acceptance Process will be the following:

- Ensure completeness, consistency, and accuracy of the deliverables within a specific project phase
- Provide reviewers with a common understanding of Acceptance Criteria and the scope of the Deliverable
- To trigger a Milestone payment for the accepted project phase

### 3.16.8 Change Control Board Participants, Roles and Responsibilities

The Milestone Process Review Team is depicted in the diagram below

**Roles and Responsibilities**

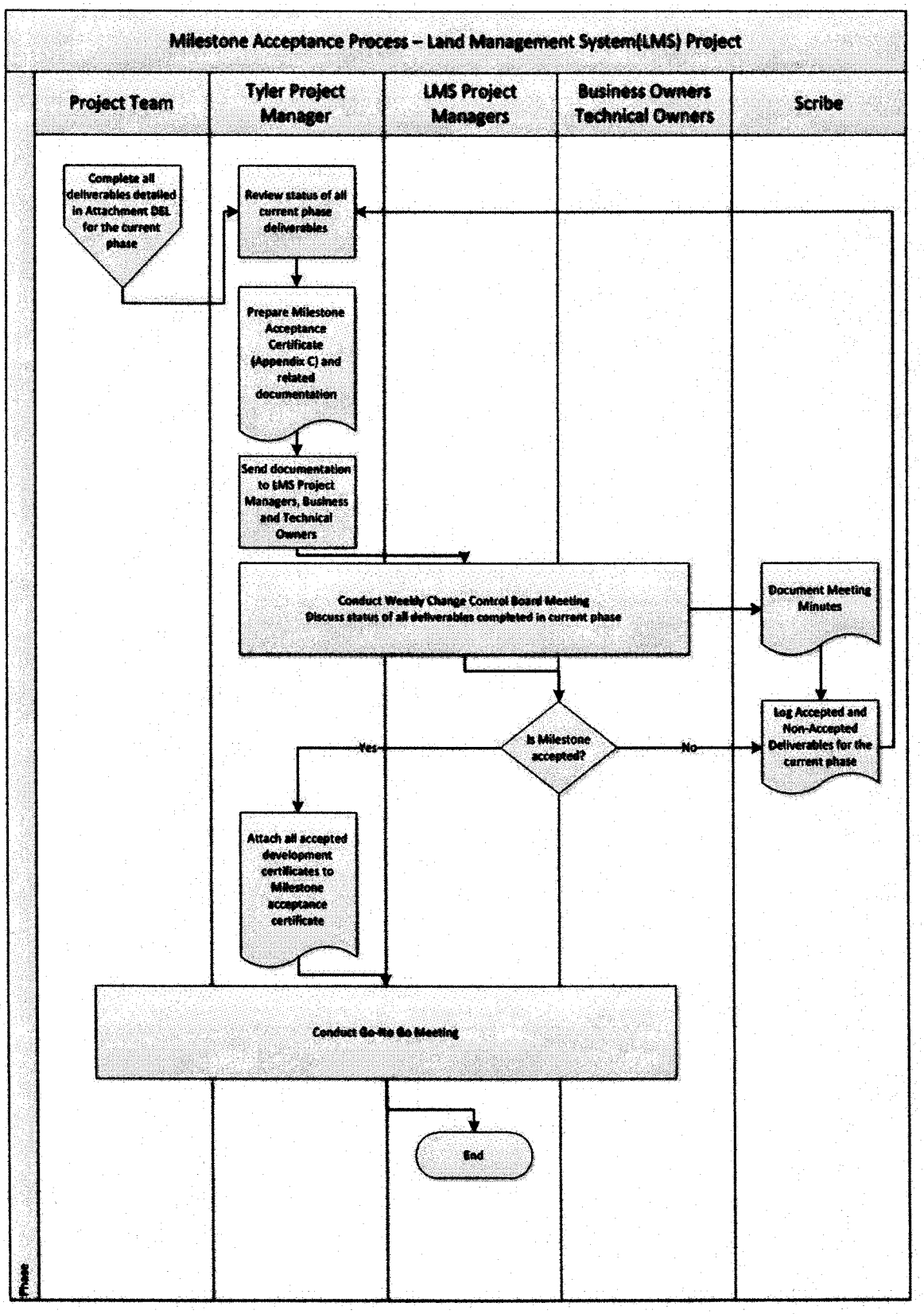
| Role | Responsibility |
|---|---|
| Project Managers | Refer to *Attachment ROL* Roles and Responsibilities |
| Project Sponsor | Refer to *Attachment ROL* Roles and Responsibilities |
| Business Owners | Refer to *Attachment ROL* Roles and Responsibilities |
| Project Administrator - Scribe | Refer to *Attachment ROL* Roles and Responsibilities |
| Business Systems Analyst | Refer to *Attachment ROL* Roles and Responsibilities |
| SME Teams | Refer to *Attachment ROL* Roles and Responsibilities |

### 3.16.9 Milestone Acceptance Process

The Milestone Acceptance Process is pictured below.

For the avoidance of doubt, the "Conduct Go No-Go Meeting" step is an internal County process only, and does not control acceptance of a Milestone or a corresponding payment obligation.

*This space intentionally* left blank


Milestone Acceptance Process – Land Management System(LMS) Project
Project Team
Tyler Project Manager
LMS Project Managers
Business Owners Technical Owners
Scribe
Complete all deliverables detailed in Attachment DEL for the current phase
Review status of all current phase deliverables
Prepare Milestone Acceptance Certificate (Appendix C) and related documentation
Send documentation to LMS Project Managers, Business and Technical Owners
Conduct Weekly Change Control Board Meeting
Discuss status of all deliverables completed in current phase
Document Meeting Minutes
Is Milestone accepted?
Yes
No
Log Accepted and Non-Accepted Deliverables for the current phase
Attach all accepted development certificates to Milestone acceptance certificate
Conduct Go-No Go Meeting
End
Phase

### 3.16.10 Acceptance Criteria for Milestones

Acceptance Criteria are listed in Attachment DEL.

The following sample appendices shall be used to document Acceptance Criteria within each Milestone.

**Appendix A Acceptance Action / Changes Log**

**Appendix B Development Acceptance Certificate**

**Appendix C Milestone Acceptance Certificate**

END OF ATTACHMENT ACC

## 3.17 Attachment LCP - Tyler Life Cycle Policy

### Tyler Release Life-Cycle Policy

**The Tyler Release Life-Cycle Policy is designed to balance our clients' need for flexibility and stability while meeting the demands for strategic product enhancements. Clients will benefit to adhering to this policy by receiving quality improvements from development and technical support. The Release Life-Cycle Stages are:**


**1. Release Planning**

**In this stage, product release features and content from the prioritized backlog of all open requests, internal and external, are reviewed and scheduled into the release. Custom feature enhancements and modifications are considered billable.**

**2. Early Adoption (Beta)**

**This represents a stage before General Availability in which a select few clients participate in testing the upcoming release with Tyler. This allows Tyler to deliver the highest quality, customer-tested product.**

**3. General Availability (Gold)**

**In this stage the new release is made available for client sites. All clients on a current maintenance plan during this time will receive full support as well as critical and non-critical updates.**

**4. Limited Support**

**This represents a stage in which the given release has matured through the Early Adoption and General Availability phases and minimal development efforts need to be placed on the product for the remainder of its life. Clients who are current on maintenance will still receive full software support during this stage but development will be limited. Clients are encouraged to upgrade to a more current release as some software corrections could require it.**

**5. Version Retirement**

**This represents a stage that receives only minimal support services and no development activity. Clients are *strongly* encouraged to upgrade to the newest available release. *End of year or legislatively mandated updates will not be performed in this stage.***

**Release Stage Schedule**

| EnerGov Version | Release Planning | Early Adoption | General Availability | Limited Support | Version Retirement |
|---|---|---|---|---|---|
| 9.3 | 10/2011 | 01/2012 | 04/2012 | 04/2013 | 04/2014 |
| 9.4 | 01/2012 | 07/2012 | 10/2012 | 10/2013 | 10/2014 |
| 9.5 | 09/2012 | 01/2013 | 05/2013 | 05/2014 | 05/2015 |
| 9.6.0 | 02/2013 | 09/2013 | 11/2013 | 11/2014 | 11/2015 |

## 3.18 Attachment SLA- Disaster Recovery; Support/Maintenance

### 3.18.1

Tyler shall provide Maintenance and Support Services for the Software in accordance with the terms of this Attachment SLA.

This section sets forth the ongoing metrics, policies and requirements for the provision of Maintenance and Support Services for so long as TLMA has timely paid its Maintenance and Support Services fees. These Maintenance and Support Services will include Defect Correction, troubleshooting, technical analysis, problem diagnosis, procedural assistance, and escalation.

Maintenance and Support Services will be provided for the Software itemized in Attachment PRC.

TLMA acknowledges and agrees that Maintenance and Support Services do not include:

- Initial project installation/implementation,
- Onsite support (unless Tyler cannot remotely correct a Defect in the Software)
- Application design
- Consulting services
- Support of an operating system or hardware
- Support of any integrations/interfaces, except as requested by TLMA pursuant to Attachment CHG and provided by Tyler on a time and materials basis

TLMA has the option to purchase Disaster Recovery Services, as set forth in Attachment PRC. To the extent TLMA exercises that option, the terms set forth herein will govern the scope and delivery of those Disaster Recovery Services.

### 3.18.2 Cost of Maintenance and Support Services

TLMA shall pay Tyler for Maintenance and Support Services following the agreed upon payment schedule set forth in Attachment PRC.

### 3.18.3 Term of Agreement

Maintenance and Support Services shall be initiated upon the earlier of (i) Milestone 3, Phase 3 (System Acceptance/UAT), as set forth in Attachment DEL; or (ii) one (1) year from the commencement of Milestone 1, Phase 1 (Kick-Off Meeting).

Thereafter, Maintenance and Support Services shall automatically renew in one (1) year increments for an additional nine (9) years unless TLMA provides written notice to Tyler of its intent not to renew at least sixty (60) days prior to the expiration of the then-current yearly increment. Tyler commits to making Maintenance and Support Services for the Software available during this entire period.

### 3.18.4 General Terms & Conditions

#### 3.18.4.1 Initiation of Support

Maintenance and Support Services shall begin as provided in Section 3.18.3 above.

### 3.18.4.2 Payment Terms; Invoicing

Maintenance and Support Services fees shall be due and payable annually in advance pursuant to Attachment PRC.

Tyler shall invoice TLMA for the forthcoming year's Maintenance and Support Services fees approximately sixty (60) days in advance of the renewal date. The invoice is due and payable on or before the start of the new Maintenance and Support Services year, or thirty (30) days upon receipt of Tyler's invoice, whichever is later.

Tyler reserves the right to suspend Maintenance and Support Services if TLMA fails to pay undisputed Maintenance and Support Services fees within sixty (60) days of the due date or sixty (60) days upon receipt of Tyler's invoice, whichever is later. Tyler will reinstate Maintenance and Support Services upon TLMA's payment of the overdue Maintenance and Support Services fees.

Pursuant to this Agreement, Tyler shall provide TLMA with all generally available releases of the Software that makes available to customers receiving Maintenance and Support Services, according to the timeframe set forth in Tyler's release lifecycle policy and without additional charge to TLMA, so long as TLMA has timely paid its Maintenance and Support Services fees.

If requested and authorized by TLMA, installation and training services related to new releases of the Software will be provided at the negotiated Professional Services rates, on the terms set forth in Attachment PRC and Attachment CHG. TLMA acknowledges and agrees that a new release of the Software is for implementation without any customization/modification performed by TLMA without Tyler's knowledge or consent. Notwithstanding the foregoing, all customizations/modifications which have been incorporated in the Software as Custom Enhancements performed by Tyler on TLMA's behalf will be incorporated in future releases, and future releases will provide compatibility for all integrated Third Party Products which are necessary for the Software to function properly and for all Custom Enhancements developed by Tyler for TLMA.

### 3.18.5 Software Maintenance and Support Terms

During the term of this Agreement, Tyler shall provide Maintenance and Support Services for the Software during the hours described in the 'Support Hours' section in this Attachment.

Tyler shall maintain trained staff capable of rendering the Maintenance and Support Services set forth herein.

Tyler shall in a professional, good and workmanlike manner perform Defect Correction using the then current 'Problem Correction Procedure', provided, that any future revision of the Problem Correction Procedure shall not reduce the levels of service received by TLMA hereunder. Following completion of the Defect Correction, Tyler shall deliver the Defect Correction through a thoroughly tested "fix" consisting of sufficient programming to implement the Defect Correction as soon as possible.

Tyler shall not be responsible to provide Defect Correction or warranty support for the Software to the extent that any Defect or warranty claim arises as a result of modifications made by TLMA to the Software without Tyler's consent.

Tyler shall support prior releases of the Software in accordance with Tyler's then-current release life cycle policy. Tyler's current release life cycle policy is attached as Attachment LCP.

### 3.18.6 Support Hours

Tyler's Software support team will be available Monday to Friday, 4:00 AM to 5:00 PM PST during all TLMA work days. Certain customers, those with Platinum Support, have access to Tyler's Help Desk 24/7. TLMA will also be eligible to receive Maintenance and Support Services from 5:00 PM – 6:00 PM PST from a co-divisional Help Desk, accessible at 800-646-2633. That Help Desk will provide front-line Software support only.

Tyler's Software support team shall provide, by mutual agreement, after-hours on-call support with prior notice (on a time and materials basis subject to the rates set forth in Attachment PRC) for the following:

- Monday to Friday, 6:00 PM to 6:00 AM PST
- Weekends (Saturdays and Sundays 24 hours support)
- County Holidays (24 Hours Support)

TLMA will not be responsible for paying time and materials rates for any time spent by Tyler's support team outside of normal support hours to resolve a Defect in accordance with the priority resolution periods set forth in Section 3.18.11 unless requested by TLMA. Notwithstanding the foregoing, in the event Tyler provides Maintenance and Support Services to resolve an issue that is not caused by a Defect, TLMA agrees that Tyler may invoice TLMA for those services on a time and materials basis, as set forth in Attachment PRC.

### 3.18.7 Support Access

Tyler's support will be accessible by calling their toll free number (888-355-1093) or by emailing a support request to energovsupport@tylertech.com.

As of the Effective Date, Tyler's team consists of an Account Manager and Help Desk staff. The Account Manager is responsible for the day-to-day operations of the team and ensures Tyler provides exceptional technical support to clients. The Help Desk staff are responsible for assisting the team with clients' issues, providing on-going team training and diagnosing and resolving client issues in a timely and courteous manner.

### 3.18.8 Paging

There may be times when TLMA is experiencing a priority 1 critical issue and all technicians for the requested team are on the line assisting clients. In this circumstance, it is appropriate to press 0 to be redirected to the operator. The operator will page the appropriate team. Tyler asks that TLMA reserves this function for those times when the system is down, or a mission critical process is unable to be completed and TLMA is not able to reach a technician immediately via standard methods.

### 3.18.8.1 Tyler Responsibilities

Tyler will maintain an online support reporting system that allows TLMA to log and track support tickets.

### 3.18.8.2 TLMA Responsibilities

Tyler will provide VPN tools to access TLMA's network remotely. Tyler currently utilizes "Go To Assist" as a secure commercial PC to PC remote connectivity tool to provide remote maintenance Services. TLMA shall maintain for the duration of the Agreement a high-speed Internet connection capable of connecting to TLMA's PC's and server. As a secondary connectivity tool to the Tyler Servers, Tyler will install a third party secure unattended remote connectivity program, which is currently Bomgar, as approved under County security policies. TLMA will need to provide Tyler a login account with local administrative privileges to the Tyler Servers. Tyler requires that TLMA also maintain an alternate remote connectivity method (including VPN, if necessary) for backup connectivity purposes. Tyler, at its option, will use the connections to assist with problem diagnosis and resolution.

Tyler and TLMA shall develop mutually agreed upon policies and procedures regarding any remote access provided to Tyler hereunder.

TLMA shall provide, at no charge to Tyler, full and free access to the Software ; working space; adequate facilities within a reasonable distance from the equipment; and use of machines, attachments, features, or other equipment necessary to provide Maintenance and Support Services set forth herein.

### 3.18.9 Backup and Restoration

TLMA is responsible for maintaining current backups of all data and images according to the backup plan recommended by Tyler during implementation. This plan includes a backup schedule, tape rotation requirements, verification of successful backups and off-site storage provisions. Tyler will provide reasonable application support to TLMA in their backup and restoration activities when needed.

### 3.18.10 High Availability

Tyler will support TLMA in TLMA's development of a High Availability design for both the database and application Software. TLMA will implement and maintain the High Availability environment for the database. TLMA, with Tyler's support, will implement and maintain the configurations related to High Availability within the Software.

### 3.18.11 Problem Correction Procedure

Tyler will use its best efforts to respond to and resolve all support calls in the most commercially expedient, efficient manner, and commits to the response and resolution goals set forth below

### 3.18.11.1 Help Desk Call Priorities

Each call logged is given a priority (1, 2, 3, and 4) according to TLMA's needs/deadlines. The goal of this structure is to clearly understand the importance of the issue and assign the priority for response/resolution. TLMA is responsible for setting the priority of the call, and through an ongoing collaborative process, the initial priority may be refined and updated.

Response is confirmation that the problem report has been received and logged into the support system. This begins the troubleshooting process and starts the clock for further time specific escalation procedures.

Resolution is a mutually agreed upon condition where a) the problem has been satisfactorily resolved; or b) a satisfactory work-around procedure has been identified and implemented.

TLMA shall utilize the prioritization and response matrix outlined below for organizing and submitting Software support incidents.

| Priority | Description | Response Goal*** | Resolution Goal |
|---|---|---|---|
| 1 | **Emergency**<br><br>Production/system is down and work cannot continue until problem is fixed. Or system is executing but not usable* output is generated. | **ASAP, with status reports daily if not fixed within 24 hours.** | **All parties to work continuously until problem is resolved.** |
| 2 | **Significant**<br><br>Inaccurate or loss of business data. The output is not being saved correctly or the defect prevents the nominal** solution from being generated. Problem is occurring in a business critical module, and there is no work-around. | **72 hours, with status reports every two days, if not fixed within 72 hours.** | **Work should continue on a normal workday basis until a permanent solution is in place.** |
| 3 | **Normal**<br><br>Issue is not critical to the business or there is a workaround to an otherwise priority 1 or 2 issue. | **72 hours, with status reports every two days, if not fixed within 72 hours.** | **Resolution is worked into a planned project repair and development schedule.** |

* Not usable is defined as TLMA being unable to use the Software in the live production environment to fulfill a critical business need, for which the Software was intended.

** Nominal is defined as the output normally generated when no anomalies are occurring.

*** The 24-hour goal is in clock hours for all Priority 1 problems. The 72-hour goal is clock hours for Platinum & Premium customer problems, and 3 business days (Monday through Friday, excluding holidays) for Standard customer problems. TLMA is enrolled in the Standard support package as of the Effective Date.

### 3.18.11.2 Development Issue Priorities

Incidents requiring development or escalated to development are given a priority codes to represent the following resolution goals.

**Priority 1: High Priority Changes – Hot Patch**: These changes are due to a severe Defect or issue in the Software, are highly visible to TLMA and typically have a negative impact on TLMA, support or implementation members. These changes are required to be performed as soon as practical to help ensure continued availability, integrity, operation, stability or security across

internal and/or external technologies. Hot Patches do not follow normal development procedures and are intended for quick response to high priority issues.

**Priority 2: Medium Priority Changes – Scheduled Patch**: These changes are due to moderate Defects and are visible to TLMA and typically cause mild TLMA inconveniences; these changes can be planned and scheduled for a patch at a time deemed convenient by support, development and the customer. Scheduled Patches occur on a bi-weekly basis.

**Priority 3: Scheduled Release:** These are changes and development requests that have been accepted for the next release. New releases include revised and new functionality and minor bug fixes.

**Priority 4: Future Release**: These are changes and development requests that have been accepted for a future but undetermined release. These requests are reprioritized prior to the beginning of each release. Changes prioritized for a future release typically are not guaranteed to be developed; each change request is reviewed prior to the beginning of a new release, and retained/prioritized for development; dropped from the development roadmap; or moved to a future release.

#### 3.18.11.3 Follow up on Open Calls

Some issues will not be resolved during the initial call to the Help Desk. If the call remains open, Tyler's technician will give TLMA an open call number to reference, and will confirm the priority of the incident.

TLMA can follow up on an open issue by calling the appropriate support team and referencing the call number to the technician who answers or leave this information in a message. Referencing the open call number allows anyone in support to quickly follow up on the issue. TLMA can also update the incident through TCP on Tyler's Web site (www.tylertech.com) and add a note requesting follow-up.

### 3.18.12 Support Escalation

If Tyler is unable to deliver a resolution within the timeframe defined in 'Problem Correction Procedures' section of this Attachment or if TLMA is not satisfied with the quality of the resolution provided by Tyler, TLMA shall seek assistance, as necessary, from Tyler's management.

- Technical Support Managers and Leads
- Energov Support Team Lead
- Director Product Support – Energov
- VP of Client Services
- Energov Product Manager

### 3.18.13 Enhancement Requests

Post implementation, and upon request from TLMA, Tyler shall evaluate and provide TLMA a quote for development of Custom Enhancements, as described in the Professional Services section of Attachment PRC. Gap Enhancements will be covered under Attachment CHG. Tyler shall not charge TLMA for the development of quotes.

### 3.18.14 System Management

#### 3.18.14.1 Tyler Software Patch Management

Tyler shall provide TLMA written documentation detailing their patch management plan. The patch management plan shall include, but is not limited to, the following elements:

- Configuration
- Testing
- Roles and responsibilities
- Third party components (including Microsoft release and patch management and mobile operating system management)
- This plan requires input from TLMA.
- Tyler shall remediate any TLMA reported Software or Third Party Software vulnerabilities within the timeframes set forth in *Attachment A58*.
- Tyler shall provide notification of patches and updates affecting security within the timeframes set forth in *Attachment A58* throughout the Software lifecycle.
- Tyler shall test and validate the appropriate patches and updates and/or workarounds internally on a standard test version of the application prior to making the same available to TLMA. TLMA shall test the appropriate patches and updates and/or workarounds in its testing environment before use in live production.
- Tyler shall be responsible to apply the patches remotely. Tyler shall monitor and confirm the stabilization of the system after applying the patches/updates.
- Tyler shall update all Documentation that pertains to the patch or update.
- Tyler Software Release Management
- Tyler will provide release notes, including all enhancements, bug fixes, etc. to TLMA as those notes are made generally available to Tyler's Maintenance and Support Services customers for the Software.
- TLMA may reasonably inquire and communicate with Tyler regarding new release features and functionality, including questions regarding release notes associated with new releases. If the release requires setup or a day of training, Tyler will advise TLMA of such requirement.
- Tyler shall test, and validate the new releases internally on a standard test version of the Software prior to making such new release available to TLMA. TLMA shall test the new release in its testing environment prior to use in live production.
- Tyler shall be responsible to deploy new releases. Tyler shall monitor and confirm the stabilization of the system after deployment of the new release.
- Tyler shall update all documentation that pertains to the new release.

#### 3.18.14.2 Software Roadmap and Strategy

Upon request, Tyler will discuss with TLMA future release plans or planned functionality.

TLMA will share upcoming initiatives and strategic direction.

#### 3.18.14.3 Support Roles and Responsibilities

The parties shall refer to Attachment ROL for support roles and responsibilities.

#### 3.18.14.4 Compliance Requests

For as long as this Attachment SLA is in effect, Tyler will modify the Software to remain compliant with all state and federal laws, regulations and mandates, including changes in

privacy protection, data security, forms and reporting requirements, for no additional cost beyond the annual Maintenance and Support Services fees. Tyler shall deliver any patch or release necessary for TLMA to be compliant with regulatory changes (i) within sixty (60) days of written notice of such changes with respect to minor revisions to forms, deadlines or processes, or as otherwise agreed by the parties; or (ii) with respect to major regulatory changes that impact Software design and functionality, in a reasonable time period after notification. Tyler will further make a reasonable effort to provide TLMA with the opportunity to test any changes prior to putting them into production.

#### 3.18.14.5 Software Version

TLMA understands, acknowledges and agrees that the technology upon which the Software is based changes rapidly. TLMA further acknowledges that Tyler will continue to improve the functionality and features of the Software to improve legal compliance, accuracy, functionality and usability. As a result, Tyler does not represent or warrant that the Software will function for an indefinite period of time.

For any new release or version, including a major release, of the Software that requires a significant change in the Hardware and/or operating system, Tyler will support the then-current release in accordance with the applicable life cycle release policy.

For any new release or version of the Software that does not require a significant change in the Hardware and/or operating system, Tyler and TLMA may jointly analyze the functionality of the Software in response to changes to determine whether TLMA must upgrade.

Tyler agrees that the Software shall be designed to remain functional on the Hardware designated in this Agreement for a period of no less than three (3) years following the Warranty Period.

#### 3.18.14.6 User Community

Tyler provides a user community forum to allow Tyler clients to connect with other users and Tyler staff to share information, collaborate, access support and receive training. In this interactive environment, individual knowledge is amplified exponentially across the community.

### 3.18.15 Disaster Recovery

On the terms set forth in Attachment PRC, TLMA has the option to purchase Disaster Recovery Services. In the event TLMA exercises that option, the terms and conditions set forth below will govern the scope and deployment of those services.

#### 3.18.15.1.1 Disaster Recovery Plan

The Disaster Recovery Plan is a mutually drafted document which details, in addition to this Section 3.18.14.11, the Disaster Recovery Services Tyler shall provide to TLMA. The parties' responsibilities with respect to the Disaster Recovery Plan are further defined below.

For purposes of this Section, a "Disaster" is defined as an unplanned event that prevents the Software from performing critical processes, as mutually agreed to by the parties, and that cannot be resolved in 24 hours. Examples of a Disaster include fire, hazardous materials incident, flood, hurricane, tornado, winter storm, earthquake, radiological accident, civil

disturbance or explosion. A Disaster is not a hardware or network failure covered by a third-party service agreement, or a support incident subject to this Attachment SLA.

TLMA may declare a Disaster whenever Tyler support staff is available under the terms of the support call process document provided herein.

Tyler's Responsibilities:

- Coordinate activities associated with transfer of data to Tyler's data center.
- Document Disaster Recovery Services strategy for Critical Processes.
- Review the Disaster Recovery Plan with TLMA.
- Provide reasonable guidance for Disaster Recovery Services policies and procedures.
- Identify modules, databases, applications, and files required for Disaster Recovery Services.
- Provide an alternate processing site for a period of ninety days (90) business days if required.
- Maintain and keep in their possession, a copy of the Disaster Recovery Plan, policies, and procedures in the event TLMA's copy is lost or destroyed.
- Tyler will maintain a disaster recovery policy to protect and restore Tyler development environments deployed on Tyler's property, within two (2) calendar days of the occurrence of any event that would disable or otherwise impact those environments.

TLMA's Responsibilities:

- Provide remote access to TLMA's Tyler database server for analysis and configuration of data transfer.
- Provide network support if required to enable transfer of data from TLMA's server to the Tyler data center.
- Provide PCs and high-speed modems for access from TLMA's alternate processing location, if required.
- Provide technical resources to configure remote access PCs, including the Software, if reasonably required to receive Disaster Recovery Services pursuant this Attachment SLA.
- Provide a chain of command document for communication during a disaster.
- Maintain the Disaster Recovery Plan and integrate the Disaster Recovery Plan made with Tyler with TLMA's comprehensive disaster recovery plan.
- Note: Tyler is only responsible for getting Tyler Software operational. Any software, including without limitation operating systems or databases, not directly related to the Tyler Software is TLMA's responsibility.

Shared Responsibilities:

- Identify critical users for Disaster Recovery Services.
- Identify critical processes for Disaster Recovery services.
- Identify RTO.

- Draft initial Disaster Recovery Plan within ninety (90) days of commencement of Initial Term.
- Define recovery processes for post Disaster operations (mandatory for Odyssey CM TLMAs, optional for all others).

#### 3.18.15.1.2 Data Transfer

The electronic transfer solution provides nightly (between the hours of 8 PM and 6 AM) transfer and archiving of TLMA's Tyler data and is subject to the following conditions:

- Initial data transfer may require portable disk.
- Data transferred shall include only items essential to provision of service.
- Those modules of the Software necessary to perform Critical Processes will be included in the Disaster Recovery Services. Software modules which do not perform Critical Processes shall not be included in data transfer or the Disaster Recovery Services.
- Only production databases are backed up.
- Data from the last seven (7) successful data transfers are retained by Tyler.
- Total data storage is limited to 1 terabyte. Storage limit may be increased in 200 GB increments by mutual agreement and at additional cost.
- Data transferred to Tyler as part of Disaster Recovery Services is not available for TLMA's data retrieval or restoration not associated with the Disaster Recovery Services provided by Tyler. Tyler may provide data transferred by TLMA on an exception basis, upon request.
- Tyler is not responsible for the integrity of the data provided by TLMA to Tyler. Tyler will use the most current viable data to restore TLMA's critical processes.
- Tyler may use select information from the TLMA database for research and analysis purposes.
- To the extent the database contains Confidential Information, Tyler shall keep confidential such information in accordance with the confidentiality provisions of the Agreement(s) by which TLMA licenses the Software from Tyler.
- Tyler Disaster Recovery Services staff will monitor status of data transfers on business days.
- In the event of two (2) consecutive data transfer failures, Tyler will timely provide notice to TLMA in order to commence troubleshooting.
- Tyler shall have no liability for failure of data transfers not solely caused by Tyler.
- Tyler will provide transfer report related to TLMA data transfer upon request.
- TLMA shall provide to Tyler any required encryption key (or other comparable device), including the right to back-up such key (or device), required to access the transferred data.

#### 3.18.15.1.3 Disaster Recovery Services During Disaster

A. Upon declaration of a Disaster, Tyler shall provide Disaster Recovery Services from one of its hosting facilities for the duration of the Disaster, not to exceed ninety (90) consecutive business days. Use of Tyler's data center in excess of such period shall require the parties to execute a change order detailing the duration of the extension and the additional cost associated therewith.
B. Hosting Services During a Disaster.
    i. Hosting Services during a Disaster will be provided in accord with Tyler's then-current standard availability guarantees from its Service Level Agreement for

SaaS clients. Any credits issued to TLMA will be based on the total Disaster Recovery Services fee paid for the then-current term.

ii. Tyler will include interfaces for the Software covered under this Attachment SLA.

iii. Hosting Services shall not include interfaces or interconnects with third party products unless specifically agreed in the Disaster Recovery Plan.

C. During a Disaster, TLMA will receive priority access to Software support.

#### 3.18.15.1.4 Annual Disaster Recovery Test

The parties may review and test the Disaster Recovery service.

- Scheduled by parties at least thirty (30) days in advance
- TLMA must provide a list of users who will partake in the test,
- Test shall not exceed 2 weeks,
- Retest within same year available if initial test not agreed by both parties to be successful

#### 3.18.15.1.5 Estimated Schedule

The Disaster Recovery Services provided pursuant this Attachment SLA will be performed consistent with the estimated schedule mutually agreed to by Tyler and TLMA. Tyler and TLMA agree to promptly perform their respective responsibilities according to such schedule.

#### 3.18.15.1.6 Tyler's Other Responsibilities

Project management services are provided as part of the Disaster Recovery Services. Tyler will designate a Project Manager who will be Tyler's contact for all communications with TLMA and will have the authority to act on Tyler's behalf in matters regarding this Statement of Work. Tyler's project manager will perform the following tasks:

- Review Statement of Work with TLMA's project manager.
- Review current project status.
- Recommend changes or additions to the project as appropriate.
- Administer the change control procedure.
- Review and evaluate the progress of the project with TLMA's project manager to resolve any necessary changes.

#### 3.18.15.1.7 TLMA's Other Responsibilities

Tyler's performance is predicated upon the following responsibilities being fulfilled by TLMA:

Prior to the start of the Statement of Work, TLMA will designate, in writing, a person who will be TLMA's Project Manager who will be TLMA's contact for all communications with Tyler and who has the authority to act on behalf of TLMA in all aspects of the Statement of Work. The Project Manager will perform the following activities:

- Interface between Tyler's Project Manager and TLMA's organization.
- Administer project change control with Tyler's project manager.
- Arrange reasonable access to TLMA's data for project personnel, as reasonably required.
- Conduct any communication through Tyler's Project Manager.

- Help resolve and escalate project issues within TLMA's organization as required.
- Obtain and provide project requirements, data, decisions and approvals within five (5) business days of request. If such requirements, data, decisions or approvals are delayed beyond the time specified, TLMA agrees to relieve Tyler of its responsibility for the affected Service until TLMA performs that obligation.
- Accept responsibility for the data files, selection and implementation of controls for TLMA's location, and security of the stored data.

TLMA acknowledge that it is TLMA's responsibility to identify and make the interpretation of any applicable federal, state and local laws, regulations and statutes.

#### 3.18.15.1.8 Project Change Control Procedure

When Tyler and TLMA agree to a change in the Disaster Recovery Plan, Tyler will prepare a written description of the agreed change which both Tyler and TLMA must sign. The Change Order will describe the change, the rationale for the change, and specify any change in the charges, estimated schedule, or other terms. When charges are necessary in order for Tyler to analyze a change, Tyler will give TLMA a written estimate and begin the analysis only after TLMA's written authorization.

END OF ATTACHMENT SLA

## 3.19 Attachment SCH- Project Schedule

Below is high level schedule estimating the duration of Milestones and deliverables for the LMS Project, as shown in Attachment PRC and referenced in Attachment DEL. It is intended that Milestone 1, Phase 1 will commence within thirty (30) to ninety (90) days following the Effective Date. Once finalized and approved by authorized representatives of both parties, that final schedule shall become part of this Attachment, as if fully set forth herein.

Project Schedule, Estimated as of the Effective Date

Milestone 1: 4 months

Milestone 2: 6 months

Milestone 3: 2 months

Milestone 4: 2 months

Milestone 5: 1 month

Milestone 6: 1 month

Milestone 7: 3 months

END OF ATTACHMENT SCH

## 3.20 ATTACHMENT LSF - Laserfiche Repository and Integration

### 3.20.1 Project Scope

Tyler will coordinate the integration of the Software with TLMA's Laserfiche repository through ECS Imaging, Inc, a Laserfiche VAR selected by County. Tyler will require that ECS adhere to a consistent naming schema to extract associated data/files from the Laserfiche repository.

ECS will provide the following services:

- From an update/insert function within the Software, automatically export associated Tyler data files **to** a Laserfiche RIO repository(s) for storage in a file format, as defined in Attachment DEL.
- Retrieve associated stored data files **from** a Laserfiche RIO repository as well as render that data within the Software as needed, and in a format and design, as defined in Attachment DEL.
- Develop any custom solutions, including scripting within the scope of the integration between the Software and Laserfiche RIO.
- Design, configure, and test the Software-Laserfiche RIO "integration".
- Provide technical architecture recommendations to support the EnerGov application and other future applications as well.

### 3.20.2 ECS Project Scope

ECS scope of services includes developing an integration that:

- Allows users to export documents from the Software and send to Laserfiche
- Allows users to retrieve documents in Laserfiche from the Software
- Functions as a server level integration (Client workstations will not need to be modified in order to operate)

ECS shall satisfy the project scope by completing the following requirements:

- *Design an export/import integration that:*
  - Exports documents from the Software to a local path on the server
  - Exports document index information from the Software to a local path on the server
  - Imports documents to Laserfiche from a local path on the server
  - Imports document index information to Laserfiche from a local path on the server
  - Imports documents to Laserfiche specific folders based on document index information
  - Import document to Laserfiche with specific document naming based on document index information
- *Design a retrieval integration that:*
  - Embeds a search URL in the Software based on a unique index value identifier to display related documents stored in Laserfiche, in a browser window
- *Design a workflow/integration for newly scanned documents in Laserfiche that:*

- Pushes index value information for newly scanned documents to the Software database

**ECS Out of Scope Activities**

ECS out of scope activities are defined as follows:

- Any major activity that is not defined as a aforementioned primary requirements
- Any secondary activity that does not relate to the aforementioned primary requirements
- Activities that require services that do not meet the technical requirements stated below.

NOTE: ECS will provide its services according to its proposed work plan for a total cost of $24,000, which Tyler will absorb and for which County will not be responsible. Notwithstanding the foregoing, to the extent County requests, or ECS requires, additional ECS services or days beyond the scope outlined herein, the parties will confer, according to the process set forth in Attachment CHG, to evaluate a mutually agreeable reallocation of payment obligations for the ECS services and any project impacts that may arise given an expanded ECS scope.

**ECS Technical Requirements**

ECS requires that the following be provided by either Contractor or TLMA:

- Contractor to provide the Laserfiche API built on .NET Framework at least 1 month prior to project kick off (project kick off, defined as official start date of detailed Laserfiche requirements gathering by Tyler, TLMA, and ECS).
- Contractor to provide Laserfiche API documentation at the conclusion of the development cycle for Software release 9.7.3.
- Laserfiche API to have built in functionality to assign buttons with appropriate triggers to send documents to Laserfiche from the Software
- Laserfiche API to have built in functionality to embed URLs with appropriate triggers to launch documents in Laserfiche WebLink from the Software
- TLMA to provide an independent test environment for development and testing purposes to ensure the final product meets all appropriate requirements of the project
- Contractor to provide timely adjustments to the Laserfiche API if the API does not allow ECS to meet the requirements in the project scope
    - Contractor must make any adjustments to the API in 1 calendar month or less
    - TLMA must accept project delays in 1 calendar month intervals if any adjustments to the Laserfiche API are required
- TLMA to provide VPN or remote access for ease of development and testing

**ECS Professional Services Estimate**

- 2 Days – Requirements Gathering, Project Planning, Solution Design, Project Documentation
- 16 Days – Development
    - 10 Days – Programming and Solution Development, Deployment to Test Environment, Testing and Validation of Primary Requirements Completion

    - 1 Day – Minor Revisions (Round 1)
    - 1 Day – Minor Revisions (Round 2, if necessary)
    - 1 Day – Minor Revisions (Round 3, if necessary)
    - 3 Days – Deployment to Production, Testing and Validation of All Requirements
- 1 Day – Training for Staff – How to use the integration
- 1 Day – Post Implementation Troubleshooting, Project Closing Documentation

**Total: 20 Days/160 hours of ECS Professional Services**

**ECS Development Project Duration Estimate**

The ECS development cycle will take approximately 2 calendar months to complete from the project kick off (project kick off, defined as official start date of detailed Laserfiche requirements gathering by Tyler, TLMA, and ECS). This includes all professional services indicated above.

NOTE: The ECS development cycle of 2 calendar months can be extended based on several factors defined herein, including:

- Technical requirement factors that are not met
- Added activities that are determined to be out of scope

### 3.20.3 Project Assumptions

Laserfiche directories will be created by TLMA as destination points which correspond to Tyler data file categories. Tyler will provide a Laserfiche API, and ECS will develop a custom solution(s) to export and retrieve documents from the Laserfiche repository on demand. Tyler will also ensure that the ECS naming schema has been reviewed and approved by TLMA.

- The data file type from the Software must be discussed and defined in advance to ensure compatibility with the Laserfiche RIO system.
- Development and/or testing environments will be established
- Production architecture of the Laserfiche repository will be defined
- All migrations / document conversions are handled via the Laserfiche API and the ECS interface

### 3.20.4 Out of Scope Activities

Any activities not listed above including, but not limited to the following:

- Upgrade of any existing Laserfiche installation
- Laserfiche RIO user training, except as allocated above
- Load testing or performance benchmarking relative to the Laserfiche RIO solution
- Any application or host system access that encompasses coding, scripting, application analysis, system performance, and/or troubleshooting beyond the integration of the Software and Laserfiche RIO.
- Any operating system or non-Laserfiche or non-Tyler application or Hardware tuning, troubleshooting or maintenance steps including patches, upgrades and/or installations/re-installations.

### 3.20.5 Deliverables

See Attachment DEL

### 3.20.6 Acceptance Criteria

See Attachment DEL

### 3.20.7 Assumptions

See Attachment ROL

### 3.20.8 Analysis & Design

TLMA will decide to create a new Laserfiche RIO repository for the LMS Project or utilize the existing repository(ies). This decision can be based on various factors that include but are not limited to: Business Decisions, Technical Decisions / Constraints, Best Practices, Performance, etc. TLMA will provide a change order, if needed, in case a new repository is to be created, according to the terms of Attachment CHG.

The Laserfiche RIO repository will include following:

#### 3.20.8.1 Folder Taxonomy

TLMA will design and implement folder taxonomy to store content created via the Tyler API and ECS interface. The purpose of folder taxonomy would be to allow the Software to export files to designated repository directories, AND to allow end users to directly navigate content using the Laserfiche RIO interface if needed.

#### 3.20.8.2 Object Types

TLMA and Tyler will discuss designs and implement Laserfiche and Tyler-supported custom object types (document types / folder types) for this project if needed. Custom object types may be needed to capture attribute / case information on documents / folders that are not provided out-of-the-box in the Laserfiche RIO object model.

#### 3.20.8.3 Security/Access Control

If needed, TLMA will work with its enterprise document management vendor, Tyler and ECS to define application and/or user Access Control Lists (also known as ACLs, Permission Sets), Users Accounts and Groups.

It is assumed that User Accounts will be either synchronized using an existing Active Directory or will be created by TLMA as needed.

It is also assumed that users will not be directly added to the ACLs, rather users would be added to Groups, and then Groups are added to Access Control Lists.

#### 3.20.8.4 Auditing

See Attachment DEL.

### 3.20.8.5 Retention Policy Services

See Attachment DEL.

### 3.20.8.6 LMS Integration Design Support

Design discussions involving the Tyler API and ECS interface to the Laserfiche RIO repository, exporting and retrieving content from the existing server, or other sundry activities. will be defined according to Attachment DEL.

### 3.20.8.7 Testing

See Attachment SOW

END OF ATTACHMENT LSF

## 3.21 Attachment A-43 Riverside County Records and Archives Policy

See attached Board Policy A-43

**COUNTY OF RIVERSIDE, CALIFORNIA**
**BOARD OF SUPERVISORS POLICY**

| Subject: | Policy Number | Page |
|---|---|---|
| **COUNTY RECORDS MANAGEMENT AND ARCHIVES POLICY** | **A-43** | **1 of 16** |

## Part A. General

### Section A.1. Title

This policy shall be known as "The County Records Management and Archives Policy."

### Section A.2. Findings

The Board of Supervisors finds that in order to safeguard rights and ensure accountability it is in the best interest of the county and the citizens thereof, and essential for the administration of county government, to create, receive, maintain, and make available accurate and reliable county records; and that the most effective way to ensure this is to apply consistent standards of responsible recordkeeping across all county departments.

### Section A.3. Authority

This policy is adopted in consideration of the provisions of Government Code §6250 et seq. pertaining to the availability and accessibility of public records; Government Code §§26201-26202.6 and §§26205-26205.8 pertaining to the Board of Supervisors' responsibilities regarding the retention and destruction of County records; in accordance with Government Code §12168 et seq. pertaining to establishing standards; in accordance with Government Code §34090.7 pertaining to prescribing procedures for destruction of duplicate records; and pursuant to County of Riverside Resolution 2004-044 pertaining to the retention and destruction of county records.

### Section A.4. Purpose and intent

It is the purpose and intent of this policy to establish a uniform program of responsible recordkeeping applicable to all county departments in accordance with applicable law. By doing so, it is the Board of Supervisors' goal to:

a. **SAVE SPACE** by removing from offices records not required for the day-to-day operations; by removing from storage areas records that no longer have significant value; and by maintaining a consistent flow of records from office space to off-site storage to destruction.
b. **SAVE MONEY** by better utilization of office space and imaging technology for active records; by restricting the use of leased space for storage of inactive records; by controlling the purchase of equipment and supplies to file inactive records; by providing cost effective storage facilities for inactive records; and by encouraging the use of automated micrographic systems for very active, long term and archival records.
c. **SAVE TIME AND LABOR** in locating records by removing inactive records from office files; by centrally locating inactive records in an off-site facility; by maintaining a computerized records management system which provides for

retrieval and accounting of off-site records and utilizing imaging technology and automation for active records retrieval.

d. **PRESERVE AND PROTECT** documents of historical significance and/or archival value.

**Section A.5. Applicability**

This policy and the standards for responsible recordkeeping developed under its authority apply to all county departments.

**Part B. Program responsibilities**

**Section B.1. Responsibilities – records management and archives program**

The County Assessor-Clerk-Recorder's office shall manage and operate the County Records Management Program and the County Archives (to be known collectively as RMAP) on behalf of the County Board of Supervisors. RMAP shall develop and maintain a multi-year business plan to make available archival, records and reformatting services to all county departments. This plan shall include establishing fees adequate to recover the full costs of such services.

RMAP shall periodically survey departmental records management practices, and where appropriate recommend improvements in those practices. This shall include assessing use of space, equipment, systems and supplies necessary and appropriate to create, receive, maintain, store, archive and make available records.

**Section B.2. Responsibilities – County Records Center**

To make available cost effective storage, access, and disposal for county records of temporary value, RMAP shall manage and operate the official County Records Center following generally accepted records management standards.

Preferably, county records with limited retention periods that are not immediately required to support day-to-day business should, as appropriate, be stored at the County Records Center for the remainder of their retention period.

Any alternative records storage facilities used by departments to store county records, such as leased facilities or third party vendors, shall meet appropriate guidelines for secure records storage developed by RMAP based on generally accepted best practices. County records shall only be stored in facilities with fire warning and suppression systems, and with adequate security to prevent unauthorized access to, or interference with, the records.

**Section B.3. Responsibilities – County Archives**

The official County Archives shall identify, collect, preserve, and make available the county's documentary heritage of records of permanent value. The County Archives shall follow generally accepted standards of archival practice.

In order to ensure preservation of records most cost effectively, departments which choose to transfer county records of permanent value to the County Archives should do so as soon as practicable. County departments should work with the County Archives as applicable to develop procedures that balance the need to preserve records of permanent value with continuing department business need for access to them.

**Section B.4. Responsibilities – custody, control of, and access to records**

The rights of custody and control of records that departments choose to store in the County Records Center remain with the departments, which are responsible for granting access to county employees or members of the public in accordance with all applicable statutes, regulations, policies, and procedures. Any and all legal restrictions regarding access to records shall remain in effect while stored at the County Records Center on behalf of departments.

When departments choose to have records accessioned into the County Archives, rights of custody and control of those records transfer to the County Archives. This shall be known as archival custody. The County Archives shall be responsible for providing access to records in archival custody to county employees or members of the public in accordance with all applicable statutes, regulations, policies, and procedures. Any and all legal restrictions regarding access shall remain in effect for records under archival custody.

Any county officer or employee having custody or control of any county records shall, at the expiration of their term of office, appointment, or employment, deliver custody and control of all records kept or received by them to their successors or supervisors, or to RMAP if appropriate and as directed.

All records in the possession of any county department shall, upon termination of activities of such department, be transferred to any successor department or to RMAP as appropriate, provided that such transfer of custody and control is consistent with the formal provisions of such termination.

**Section B.5. Responsibilities – departmental cooperation**

County departments shall, as appropriate, cooperate with RMAP to meet the intent of this policy, follow the guidelines for responsible recordkeeping established under this policy, and develop department policies and procedures in accordance with those guidelines.

Each county department shall designate an individual, or individuals, to assist with and be directly responsible for implementing this policy. RMAP shall offer regular training to assist and support those departmental personnel.

**Section B.6. Responsibilities – requests for space allocation**

Departments shall include a description of their records management plan with any request for additional space and relevant capital improvements, and in that description shall include any work with RMAP to most efficiently and cost effectively address the space demands of records in their current location.

**Section B.7. Responsibilities – records & micrographic equipment, software & systems**

Regarding purchases, upgrading, or rental of records and/or micrographic equipment, software and systems the purchasing agent shall consult with RMAP to ensure efficient and cost-effective use of existing resources and to meet established standards for responsible recordkeeping.

**Section B.8. Responsibilities – annual report**

Within 90 days following the end of each fiscal year, RMAP shall make an annual report to the Board of Supervisors summarizing the activities of the program, and conformance to generally accepted responsible recordkeeping standards. The annual report shall include a listing of all extensions to retention periods requested by and granted to departments through the course of the year, and brief summaries of the justifications given.

The annual report shall include a summary of the financial activities of the program in the previous year compared with budgeted appropriations and estimated revenues. The annual report shall also include the program's long-range financial plan over a period of not less than five years into the future. The annual report shall also include an executive summary of the program's business plan, including, but not limited to, an assessment of service needs and market opportunities, strategic planning, and capital planning.

**Part C. Standards**

**Section C.1. Standards – establishing**

With the approval of the County Executive Officer and County Counsel, RMAP shall establish standards for responsible recordkeeping in conformity with applicable statutes, regulations and recognized best practices, and shall upon request provide training, advice, and assistance to all county departments in conforming with those standards.

As necessary and appropriate, the director of RMAP shall organize one or more committees to assist in establishing standards for responsible recordkeeping. He or she, or his or her representative, shall chair any such committee, which shall include representatives of concerned departments.

**Section C.2. Standards – establishing – records retention and destruction**

RMAP shall develop standards, forms and procedures to assist departments in preparing departmental records retention schedules that adequately provide for the indefinite retention of records of permanent value, and for the prompt and orderly disposition of records of temporary value.

**Section C.3. Standards – copy of record**

Where any county record, as defined in this policy, is created or received and maintained in more than one copy, the department concerned shall clearly designate a copy of record, and shall assign responsibility for maintaining that copy of record in accordance with the applicable records retention schedule.

**Section C.4. Standards – eye-readable formats**

Records with a mandatory retention of five years or longer shall be maintained in an eye-readable format in addition to any electronic format used for access or business process support. Records vital to business continuity, whatever their mandatory retention, shall be maintained in eye-readable format in addition to any electronic format used for access or business process support.

**Section C.5. Standards – reformatting**

To ensure cost-effective production of copies, whether analog or digital, of county records that meet required standards for surrogates, RMAP shall manage and operate an official county reformatting program following generally accepted industry standards. RMAP shall maintain a reference library of such applicable national and international reformatting standards for the use of all county departments and other clients.

Reformatting of county records by any department other than RMAP, or by any outside contractor, shall meet or exceed the same standards applied by the county reformatting program. All departments performing their own reformatting or contracting for reformatting shall work with RMAP to establish appropriate procedures to confirm adherence to those standards.

**Section C.6. Standards – microfilm**

All film used in the microphotography process shall meet or exceed minimum standards of quality approved by the United States Bureau of Standards and the American National Standards Institute, or other generally recognized standard setting

organizations as applicable and relevant. A true copy of the microfilm shall be kept in a safe and separate place for security purposes.

**Section C.7. Standards – electronic format**

In accordance with Government Code §12168 et seq., the Board of Supervisors recognizes the need to adopt uniform countywide standards for the purpose of storing and recording both permanent and temporary records in electronic media. In order to ensure that uniform countywide standards remain current and relevant, RMAP, in consultation with the County Executive Officer and County Counsel, shall adopt appropriate standards established by the American National Standards Institute, the Association for Information and Image Management, or other generally recognized standard setting organizations as applicable and relevant. These standards shall include a requirement that a trusted system be utilized.

In order to implement standards as expeditiously as possible, and until such time as specific countywide standards are adopted, RMAP shall make readily available to departments copies of standards and/or guidelines recommended by the American National Standards Institute, the Association for Information and Image Management, or other generally recognized standard setting organizations, as applicable and relevant, for recording permanent and/or nonpermanent records. County officers shall ensure microfilming, electronic data imaging, and photographic reproduction meet or exceed these minimum standards.

**Section C.8. Standards – electronic filing**

When not inconsistent with other provisions of law, RMAP may, in consultation with the County Executive Officer, County Counsel, and other interested parties, propose to the Board of Supervisors adoption of policies and procedures to authorize electronic filing in lieu of filing or recording documents presented in paper format, including filing by facsimile, of any document required to be filed with the county under any act administered by the county.

The rules and regulations may set forth standards for the acceptance of a signature in a form other than the proper handwriting of the person filing a document that requires his or her signature. A signature on a document electronically filed, or filed by facsimile, in accordance with those rules and regulations is prima facie evidence for all purposes that the document actually was signed by the person whose signature appears on the electronically filed document or facsimile.

The filing or recording shall constitute a unique computerized informational record. The record need not be retained in the form in which it is received, if the technology used to retain the record results in a permanent record that does not permit additions, deletions,

or changes to the original document, and from which an accurate image may be created during the period for which the record is required to be retained. The filing officer may employ a system of microphotography, optical disk, or reproduction by other techniques that do not permit additions, deletions, or changes to the original document. A true copy of the microfilm, optical disk, or other storage medium shall be kept in a safe and separate place for security purposes.

**Part D. Records retention**

**Section D.1. Records retention schedules – general**

In order to most efficiently and effectively implement the various provisions of the Government Code pertaining to Board of Supervisors approval of records retention and destruction, the county shall use Board approved general and departmental records retention schedules that specify various record series, their retention periods, and any particular restrictions or specifications regarding their retention, disposition and destruction.

**Section D.2. Records retention schedules – responsibilities**

RMAP shall coordinate preparation of records retention schedules and records destruction activities generally, and shall act as liaison between departments, risk management, the County Auditor-Controller, County Counsel and the County Executive Office in matters dealing with records retention.

County departments shall develop and maintain their own records retention schedules and records destruction activities in accordance with the established guidelines pursuant to Section D.9, below. This includes coordinating statutorily required Board approval of each departmental schedule, and periodic updates as necessary to remain current.

**Section D.3. Records retention schedules – responsibilities – master file**

RMAP shall maintain a master file of all records retention schedules approved by the Board of Supervisors with a copy of the Board minute order of approval attached to each. RMAP shall make readily available to county officials, employees, and the public reference copies of approved records retention schedules.

**Section D.4. Records retention schedules – standard – copy of record**

Records retention schedules shall apply to the copy of record, unless explicitly stated otherwise.

**Section D.5. Records retention schedules – standard – retention periods**

The retention periods on Board approved records retention schedules are mandatory, and records shall be disposed of in accordance with those approved retention periods. Records not required for active or likely litigation, and which have been subjected to any and all applicable audits, must be disposed of at the end of their scheduled retention period, unless a department head certifies a specified business need to extend their retention period. RMAP shall keep a register of such certified extensions, and report a summary of extensions in their annual report.

In some departments, records of a series listed on the county's general records retention schedule may need to be retained longer than the general schedule period, due to specific audit or contract requirements applicable to that department's programs. Departments should treat such cases separately when developing and revising their specific records retention schedules.

As an interim measure until all departments have specific records retention schedules, department heads or their designees shall certify a business need to extend the retention period required by the general schedule for such records, citing the specific audit or contract provisions concerned. Such records shall be disposed of on authority of the general schedule when this certified extension has passed.

No duplicates or other copies of any record shall be retained longer than the mandatory retention period for the copy of record. When records are disposed of by schedule, departments shall ensure they retain no duplicates or other copies.

**Section D.6. Records retention schedules – approval**

Pursuant to Government Code §26205.1, to be in effect records retention schedules require approval by the Board of Supervisors. Records retention schedules submitted by RMAP to the County Executive Office for Board approval shall require prior sign off by the County Archives manager, Risk Management, County Auditor-Controller, County Counsel, and the director of RMAP.

RMAP sign-off of any proposed records retention schedule shall include certification the schedule was reviewed by a professional archivist and/or historian to ensure the need to maintain the county's documentary heritage is adequately considered in establishing the retention periods.

**Section D.7. Records retention schedules – list of approved schedules**

All records retention schedules approved by the Board of Supervisors shall be listed below in this section by title, schedule number, approval date, and agenda number.

The list in this section shall constitute the only valid list of authorized records retention schedules to be used by county departments and RMAP.

Subsequent to the adoption of this policy, a motion for the Board of Supervisors to approve a records retention schedule shall be taken as a motion to amend this policy to add the title and approval date of the schedule to this section.

Listing a records retention schedule in this section shall be taken as inclusion by reference of the entire approved retention schedule in the text of this policy.
When revising a records retention schedule, a motion for the Board of Supervisors to approve a revised retention schedule shall be taken as a motion to amend this section of this policy to add the title of the revised schedule and approval date to this section, and to delete the title and approval date of the previous version of that schedule from this section.

Board approved records retention schedules are listed in **Attachment A**.

**Section D.8. Records retention schedules – general schedule**

A general records retention schedule for the county shall be developed and maintained under the supervision of the director of RMAP, or designee, in consultation with other county departments as necessary and appropriate.

The completed or updated proposed general records retention schedule shall be accompanied by a signature page signed by the county archives manager, Risk Management, County Auditor-Controller, County Counsel, and the director of RMAP, or their respective designees. The general records retention schedule and its accompanying signature page shall be submitted under cover of a fully executed Form 11 by RMAP to the County Executive Office pursuant to Board Policy A-5 for review and submittal to the Board of Supervisors for approval.
A Board approved general records retention schedule shall only provide authority for the disposition of 'housekeeping' records commonly found in most county departments. The general records retention schedule shall not cover the specific programmatic records produced by departments. Retention requirements of programmatic records shall be defined and documented by departments in their own specific records retention schedules.

Pursuant to Government Code §26205.1, no general records retention schedule shall be effective unless and until approved by the Board of Supervisors.

**Section D.9. Records retention schedules – departmental schedules**

Specific records retention schedules shall be developed and maintained by each county department. RMAP shall provide forms and procedures for inventorying records and developing retention schedules, and shall provide guidance and assistance to department personnel in their use upon request.

All proposed or updated department records retention schedules and their accompanying signature pages shall be submitted on behalf of departments by RMAP under cover of a fully executed Form 11 to the County Executive Office pursuant to Board Policy A-5 for review and submittal to the Board of Supervisors for approval. All records retention schedules submitted to the Board of Supervisors shall be accompanied by a signature page signed by the head of the department, Risk Management, County Auditor-Controller, County Counsel, the county archives manager, and the director of RMAP, or their respective designees.

Pursuant to Government Code §26205.1, no departmental records retention schedule shall be effective unless or until approved by the Board of Supervisors.

**Section D.10. Records retention – records destruction**

Pursuant to Government Code §§26201-26202.6 and §§26205-26205.8, County records, as defined in this policy, shall only be destroyed: (1) in accordance with an approved records retention schedule listed in this policy; or (2) after reformatting to required standards; or (3) with specific permission of the Board of Supervisors.

Reformatting means to copy the content, structure, and context of records to another medium in such a way the copy may act as a satisfactory surrogate for the original. In order to conserve space and resources, original records reformatted to required standards may be destroyed before their approved retention period has expired, since from the time the originals are destroyed the reformatted copies are deemed to be original records, and subject to the same requirements and restrictions of the retention schedules applicable to the originals.
Records shall be destroyed in accordance with standards and procedures developed by RMAP. These procedures shall include a form approving the destruction signed by the head of the department, or designee, and the director of RMAP, or designee. All approvals of the destruction of records shall include: (1) a citation to the specific records retention schedule and the specific item on that schedule providing authority for the destruction; or, (2) certification that the records were reformatted to required standards, and the reformatted copies are intended to serve as the copy of record; or (3) an attached copy of the board minute order authorizing destruction.

Records required in relation to active or likely litigation shall be maintained, and may not be destroyed by authority of an approved schedule, until all litigation matters are finally

resolved and both risk management and County Counsel approve disposition. Records required for audit purposes shall not be destroyed by authority of an approved schedule until all applicable audits are complete and audit exceptions resolved. All approvals of the destruction of records shall include certification by the head of the department, or their designee, that the records are not required in relation to active or likely litigation or for audit purposes.

A representative of RMAP or the department shall supervise the destruction of records, and shall attest in writing that destruction is carried out according to required procedures.

**Section D.11. Records retention – non-records destruction**

Pursuant to Government Code §34090.7 and other provisions of the state statutes, non-records, as defined in this policy, may be destroyed at any time. Departments may dispose of non-records when they are no longer needed to support business processes.

**Glossary**

As used in this policy, the following terms shall have the following meanings:

"Accession" means the process whereby the County Archives accepts transfer from a county department of records of permanent value which the department selects for preservation and which are brought within the County Archives' systems of physical and intellectual control.

"Archival custody" means the state of records once accessioned by the County Archives, and in which the County Archives accepts responsibility for appropriately maintaining those records, which includes planning and budgeting for their preservation, and for providing access in accordance with all applicable statutes, regulations, policies and procedures.

"Copy of record" means the copy of a record designated as the official copy.

"County Archives" means a facility for the collection, preservation, and use of records of permanent value transferred by departments to the County Archives, and which is managed and operated to generally accepted standards of archival practice. Departments transfer legal custody of records that they choose to transfer to the County Archives, although legal, regulatory and procedural restrictions regarding access to those records remain in effect.

"County Records Center" means a facility for the cost-effective storage and disposition of records of temporary value managed and operated to generally accepted records

management standards. Departments retain legal custody of the records they choose to house in the County Records Center.

"Department" means every county office, department, group of departments, division, bureau, board, and commission that is not a separate public entity of the county.

"Duplicate" means any accurate and unabridged copy of a record or series of records.

"Eye-readable" means that records are in a format that can be directly interpreted by the human eye with or without magnification, and with no need for mediating interpretation such as software applications. Examples of eye-readable formats are paper, microfilm, and microfiche.

"Non-records" means duplicates or other copies of records made solely for convenience or reference; working papers such as rough notes, calculations or drafts assembled or created and used in the preparation or analysis of other documents; appointment logs; stocks of blank forms or publications; or library or museum material intended solely for reference or exhibit.

"Permanent value" as applied to records means there is no termination or end point to the value of maintaining the records, and that they or their appropriate surrogate are intended to be available indefinitely.

"Records" means all papers, maps, plans, photographic films and prints, microfilm or other microformats, electronic data, audio and visual materials, and other documents, regardless of physical form or characteristics, which are produced, received, owned, used, or retained by a department in the regular course of transacting official county business.

"Reformatting" means to copy the content, structure, and context of records to another medium, whether analog or digital, in such a way that the copy may act as a satisfactory surrogate for the original. This requires meeting accepted national standards for particular processes and media.

"Responsible recordkeeping" is a generally accepted term that means creating, receiving, maintaining, and making available records in an efficient and cost-effective manner which conforms to all applicable statutes and regulations, supports business processes, and meets the responsibilities placed on public agencies to safeguard rights and ensure accountability.

"Retention period" means the length of time a record must be retained to fulfill its administrative, fiscal and/or legal function.
"Retention schedule" means a list of all categories of records produced or maintained by a department or agency, and the required and approved actions to be taken with regard to those records, including establishing their retention period.
"Temporary value" as applied to records means there is a termination or end point to the value of maintaining the records, and that they are intended to be disposed of at that point.

"Trusted system" means a combination of techniques, policies, and procedures within which there is no plausible scenario in which a document retrieved from or reproduced by that system could differ substantially from the document as originally stored.

**Reference:**
Minute Order 3.12 of 04/16/1991
Minute Order 3.4 of 01/28/2003
Minute Order 3.36 of 01/13/2004
Minute Order 3.8 of 06/8/2004
Minute Order 3.5 of 1/23/2007
Minute Order 3.8 of 2/5/2008
Minute Order 3.12 of 12/16/2008
Minute Order 3.6 of 7/21/2009
Minute Order 3.11 of 12/01/2009
Minute Order 3.19 of 4/20/2010
Minute Order 3.4 of 12/17/2010
Minute Order 3.2 of 11/08/2011
Minute Order 3.10 of 12/12/2011
Minute Order 3.10 of 1/10/2012
Minute Order 3.20 of 08/28/2012
Minute Order 3.2 of 11/27/2012
Minute Order 3-18 of 02/26/2013
Minute Order 3-12 of 07/14/2013
Minute Order 3-18 of 08/20/2013
Minute Order 3-15 of 11/05/2013
Minute Order 3-9 of 12/10/2013

## Attachment A

### Section D.7. Records retention schedules – list of approved schedules

Board approved records retention schedules are listed below as follows:

| *Schedule Title* | *Schedule No.* | *Date* | *Agenda No.* |
|---|---|---|---|
| General Records Retention Schedule | GRRS_2013_Rev08 | 12/10/2013 | 3-9 |
| | | | |
| Agricultural Commissioner's Office | DRRS_AGC_2013_Rev01 | 12/10/2013 | 3-9 |
| Animal Services | DRRS_CHA-AS_2011_Rev01 | 7/12/2011 | 3.10 |
| ACR – Assessor | DRRS_ACR-A_2011_Rev02 | 7/12/2011 | 3.10 |
| ACR – County Clerk | DRRS_ACR-C_2011_Rev02 | 7/12/2011 | 3.10 |
| ACR – Recorder | DRRS_ACR-R_2013_Rev03 | 11/05/2013 | 3-15 |
| ACR – Records Management and Archives Program | DRRS_ACR_RMAP_2013_Rev01 | 2/26/2013 | 3-18 |
| Child Support Services | DRRS_CSS_2010_Rev01 | 12/7/2010 | 3.4 |
| County Counsel | DRRS_COCO_2008_Rev01 | 12/16/2008 | 3.12 |
| County Executive Office | DRRS_CEO_2013_Rev03 | 7/16/2013 | 3-12 |
| County Human Resources | DRRS_CHR_2011_Rev02 | 1/10/2012 | 3.10 |
| Department of Public Social Services | DRRS_DPSS_2011_Rev01 | 1/10/2012 | 3.10 |
| District Attorney's Office | DRRS_DAO_2013_Rev01 | 12/10/2013 | 3-9 |
| EDA – Real Estate | DRRS_EDA-RE_2011_Rev01 | 11/08/2011 | 3.2 |
| EDA/RDA – Project Management Office (Projects) | DRRS_EDA/RDA-PMO_2011_Rev01 | 11/08/2011 | 3.2 |
| EDA – Workforce Development Department | DRRS_WDD_2013_Rev01 | 12/10/2013 | 3-9 |
| Environmental Health – District Environmental Services | DRRS_CHA-DES_2011_Rev02 | 7/12/2011 | 3.10 |
| Environmental Health – Environmental Protection and Oversight Division | DRRS_CHA-EPO_2010_Rev02 | 12/7/2010 | 3.4 |
| Flood Control | 950-01 | 12/18/1990 | 7.7 |
| Mental Health | DRRS_MH_2013_Rev01 | 8/20/2013 | 3-18 |
| Office on Aging | DRRS_OoA_2012_Rev01 | 11/27/2012 | 3.2 |
| Probation | DRRS_PROB_2013_Rev01 | 11/05/2013 | 3-15 |
| Public Defender | DRRS_PD_2013_Rev01 | 11/05/2013 | 3-15 |
| Public Health – Children's Medical Services | DRRS_PH-CMS_2011_Rev02 | 11/08/2011 | 3.2 |
| Public Health – Clinic Management | DRRS_CHA-CM_2011_Rev02 | 11/08/2011 | 3.2 |
| Public Health – Community Outreach | DRRS_PH-CO_2013_Rev03 | 7/16/2013 | 3-12 |
| Public Health – Disease Control / Administration | DRRS_PH-DC-A_2011_Rev02 | 11/08/2011 | 3.2 |

| | | | |
|---|---|---|---|
| Public Health – Disease Control / Communicable Diseases | | 1/23/2007 | 3.5 |
| Public Health – Disease Control / Healthy Children's Connection | | 1/23/2007 | 3.5 |
| Public Health – Disease Control / Sexually Transmitted Diseases | DRRS_PH-STD_2013_Rev02 | 11/05/2013 | 3-15 |
| Public Health – Disease Control / Tuberculosis | DRRS_PH-DC-TB_2011_Rev02 | 11/08/2011 | 3.2 |
| Public Health –Epidemiology & Program Evaluation | | 1/23/2007 | 3.5 |
| Public Health – Fiscal | DRRS_PH-FCL_2013_Rev01 | 12/10/2013 | 3-9 |
| Public Health –HIV / AIDS | DRRS_PH-HIV_2013_Rev03 | 11/05/2013 | 3-15 |
| Public Health –Immunization | DRRS_PH-IM_2011_Rev02 | 7/12/2011 | 3.10 |
| Public Health – Laboratory | DRRS_PH-LAB_2012_Rev01 | 11/27/2012 | 3.2 |
| Public Health – Maternal, Child and Adolescent Health (MCAH) | DRRS_PH_MCAH_2012_Rev02 | 8/28/2012 | 3.20 |
| Public Health – Nursing | DRRS_CHA_PHN_2010_Rev01 | 12/7/2010 | 3.4 |
| Public Health - Nutrition Services / Women, Infants, Children (WIC) | DRRS_PH-NS_2010_Rev02 | 12/7/2010 | 3.4 |
| Public Health – Special Services Division / Office of Industrial Hygiene | DRRS_PH-IH_2011_Rev02 | 1/10/2012 | 3.10 |
| Riverside County Information Technology (RCIT) | DRRS_RCIT_2011_Rev01 | 7/12/2011 | 3.10 |
| Riverside County Regional Medical Center (RCRMC) | DRRS_RCRMC_2013_Rev01 | 11/05/2013 | 3-15 |
| Sheriff-Coroner-Public Administrator | DRRS_SHF_2013_Rev01 | 2/26/2013 | 3-18 |
| TLMA – Code Enforcement | DRRS_TLMA_CODE_2012_Rev01 | 2/26/2013 | 3-18 |
| TLMA – Transportation | DRRS_TRANS_2013_Rev02 | 7/16/2013 | 3-12 |
| Treasurer-Tax Collector | DRRS_TTC_2012_Rev01 | 8/28/2012 | 3.20 |
| Veterans' Services | DRRS_VET_2012_Rev02 | 8/28/2012 | 3.20 |

## 3.22 Attachment A58- Riverside County Enterprise Security Policy

See Attached Board Policy A-58

| **Subject:** | **Number:** | **Page** |
|---|---|---|
| Information Security Policy | A-58 | 1 of 1 |

It is the policy of Riverside County to protect Riverside County information in accordance with all applicable laws, governmental regulations and accepted best practices to minimize

information security risk; ensuring the right information is available to the right people at the right time.

To achieve this goal, the Riverside County Board of Supervisors authorizes the Riverside County Chief Information Security Officer (CISO) to develop and maintain the Riverside County Information Security Program and requires all Riverside County Departments to comply.

The Information Security Program consists of the Program Framework, the Information Security Risk Management Methodology and Information Security Standards:

- The Program Framework defines the program's Vision, Mission and Roles & Responsibilities.

- The Information Security Risk Management Methodology defines the processes for assessing, accepting and mitigating information security risk.

- The Information Security Standards define the specific controls and processes required to mitigate information security risks. The Information Security Office (ISO) will develop Information Security Standards as necessary.

The Riverside County Chief Information Security Officer is further authorized to assist the state and federal governments in drafting security and privacy legislation to ensure that the best interests of the constituents of Riverside County are represented.

**Reference:**

Minute Order 3.39 of O712912003

Minute Order 3.7 of 11/0712006

Minute Order 3.33 of 04/07/2009

# RIVERSIDE COUNTY

## INFORMATION SECURITY

## PROGRAM FRAMEWORK

## PURPOSE

The purpose of the Riverside County Information Security Program Framework is to define the Vision, Mission and Roles & Responsibilities for Information Security Program.

## VISION

The vision of the Information Security Program is that through appropriate information security risk management, Riverside County will reduce the chances of having an information security incident impact the delivery of service to its constituents.

## MISSION

The mission of the Information Security Program is to ensure the right information is available to the right people at the right time.

## SCOPE

The scope of the Information Security Program includes all Riverside County information assets.

## AUDIENCE

The audience for this document includes all Riverside County personnel with roles listed herein.

## TERMINOLOGY

Information Security Incident - The unauthorized modification of, denial of access to or disclosure of an information asset.

Information Asset - Information in any form, created or collected to support Riverside County operations.

Information Security Risk - The combination of the probability of an information security incident occurring and its impact to county finances or constituent confidence.

Information security Risk Management - The assessment, acceptance and mitigation of information security risk.

Riverside county Department - Any clearly defined functional body governed by the Riverside County Board of Supervisors. This includes but is not limited to Departments, Agencies and Commissions.

## ROLES AND RESPONSIBILITIES

**BOARD OF SUPERVISORS**

The Board of supervisors is responsible for reviewing and ratifying the Information Security Policy (A-58).

**COUNTY EXECUTTVE OFFTCER (CEO)**

The County Executive Officer acts as an agent of the Board of Supervisors to ensure that administrative policies and programs are carried out by departments.

**CHIEF INFORMATTON SECURTTY OFFICER (CISO)**

The chief Information security officer is responsible for managing the Information Security Program.

**RIVERSIDE COUNTY DEPARTMENT HEAD**

Department Heads are responsible for ensuring Departmental participation in the Information Security Program and designating a Department Information Security Officer.

**DEPARTMENT INFORMATION SECURITY OFFTCER (DISO)**

Department Information Security Officers are responsible for ensuring that processes and standards developed by the Information Security Program are communicated and implemented within their Department. The Department Information Security Officer must report directly to either the Department Head or a Deputy Department Head. This title is a designation not a human resources classification.

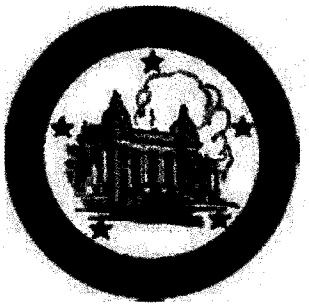
**AUDITOR CONTROLLER**

The Auditor Controller is responsible for including information security as a component of their audit plan. The Auditor Controller will collaborate with the Information Security

Office on Issues related to compliance with the Information Security Program.

## REVISION HISTORY

| Change Date | Changed by (Name) | Revision | Description of Changes | Approved By | Approval Date |
|---|---|---|---|---|---|
| 03/16/09 | Sebron | 1.0 | Published Document | Jack B. Miller | 03/17/09 |



# RIVERSIDE COUNTY

## INFORMATION SECURITY RISK MANAGEMENT METHODOLOGY

## PURPOSE

The Riverside County Information Security Risk Management Methodology supports the Riverside County Information Security Program by defining processes for managing information security risk. This methodology defines how information security risks are assessed, accepted and/or mitigated.

## SCOPE

The scope of the Information Security Risk Management Methodology includes all Riverside County Information assets.

## AUDIENCE

The audience for this document includes all Riverside County personnel with roles listed herein.

## TERMINOLOGY

Information Security Risk - The combination of the probability of an information security incident occurring and its impact to county finances or constituent confidence.

Information Asset - Information in any form, created or collected to support Riverside County operations.

Information Security Incident - The unauthorized modification of, denial of access to ordisclosure of an information asset.

Gap Analysis - A gap analysis is a differential comparison between the required information security processes and standards and the actual implementation of controls. The gap analysis includes remediation plans for all identified gaps.

Vulnerability - An exposure that could result in an information security incident.

Threat - The intent and ability to cause an information security incident.

Mitigating control - other controls that reduce the ISIP associated with this particular gap.

Previously Accepted Risk - other accepted risks that may increase the overall risk associated with this particular gap.

Potential scenarios - Situations resulting from an information security incident arising from this particular gap.

Information Security Incident Probability (ISIP) - The likelihood of the occurrence of an information security incident. The ISIP is a combination of vulnerability and threat and is classified based on the following parameters.

| | High | Probable | Low |
|---|---|---|---|
| Probability | Highly Likely | Probable | Not Likely |

Operational State - The operating state of the County when an incident occurs. For purposes ofquantifying business impact the ISO has defined the following two categories:

- Business As Usual - standard day to day operating paradigm .
- Regional Disaster - circumstance where a significant number of business processes are impacted due to a regional event

Business Impact - The repercussions to the County's finances and/or constituent confidence if an information security incident occurs.

Business Impact Rating (BIR) - Logical grouping of business impacts based on the following parameters.

| **Constituent Confidence** | | |
|---|---|---|
| **Severe** | **Moderate** | **Minor** |
| Extensive Dissatisfaction | Moderate Dissatisfaction | Limited Dissatisfaction |

| **County Finances** | | |
|---|---|---|
| **Severe** | **Moderate** | **Minor** |
| Monetary Loss<br><br>Greater than $5,000,000 | Monetary Loss between<br><br>$1,000,000 and $5,000,000 | Monetary Loss<br><br>Less than $1,000,000 |

## ROLES AND RESPONSIBILITIES

### COUNTY EXECUTIVE OFFICER (CEO)

The County Executive Officer will escalate Information Security Risks to the Board of Supervisors as necessary.

### CHIEF INFORMATION SECURTTY OFFICER (CISO)

All risk assessments must be submitted to the Chief Information Security Officer for validation and approval. CISO signatory approval is required for acceptance of all critical, high and medium level information security risks.

### INFORMATION SECURITY OFFICE (ISO)

The Information Security Office will develop Information Security Standards to ensure Riverside County's Information Security Risk is appropriately mitigated and assists departments with implementing the Riverside County Risk Management Methodology.

### DEPARTMENT HEAD

Department Heads are responsible for ensuring their departments comply with Riverside County's Information Security Risk Management Methodology. Requests to the CISO foracceptance of critical, high and medium information security risks must be submitted by theDepartment Head.

### DEPARTMENT INFORMATTON SECURITY OFFICER (DISO)

The Department Information Security Officer is responsible for ensuring that a gap analysis is completed within 90 days of the release of new Information Security Standards. While the ISO is the only organization authorized to document formal information security risk assessments,the DISO is responsible for ensuring Risk Assessments are com

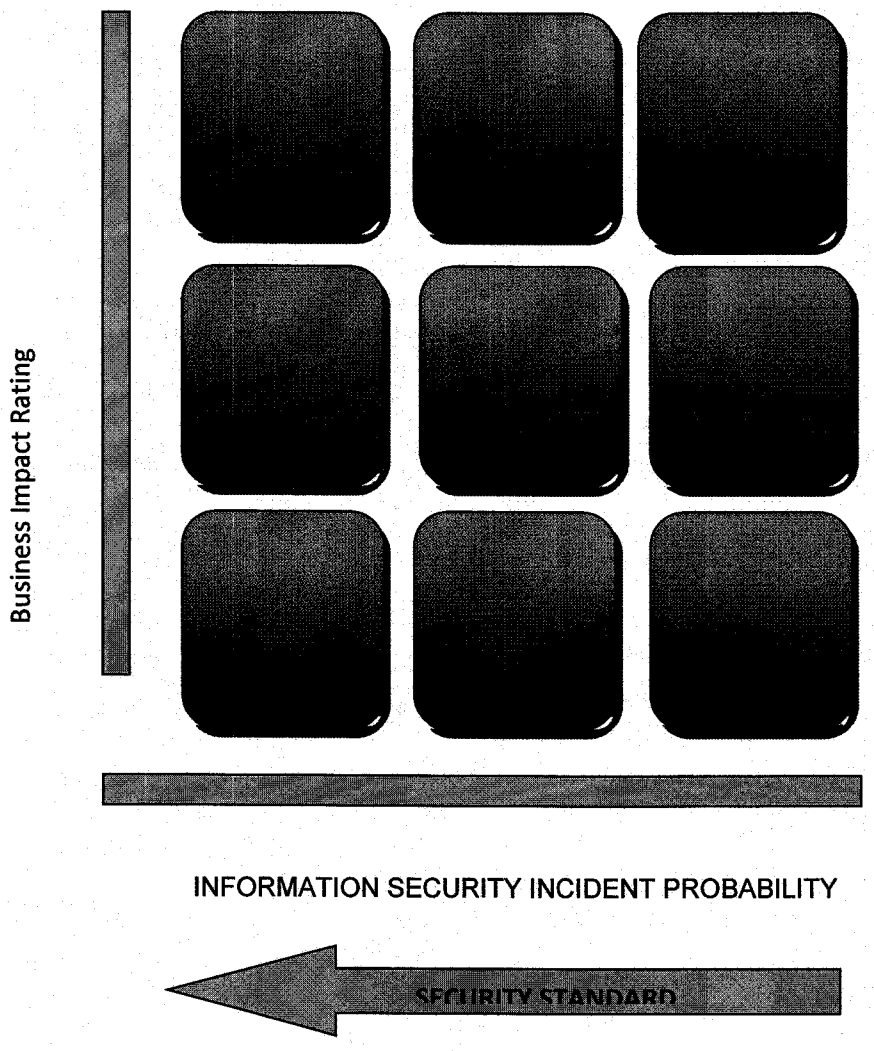
## PROCESSES

RISK MITIGATION

Process Overview

The Risk Mitigation Process reduces Riverside County's information security risk to low through the development and implementation of Information Security Standards. Information Security Standards establish the minimum set of controls necessary to reduce the Information Security Incident Probability (ISIP) thereby reducing information security risk. If the controls required by an Information Security Standard will not be implemented, the Risk Assessment Process must be followed to accurately classify the level of risk and the Risk Acceptance Process must be followed to appropriately accept the risk.

RISK CLASSIFICATION MATRIX

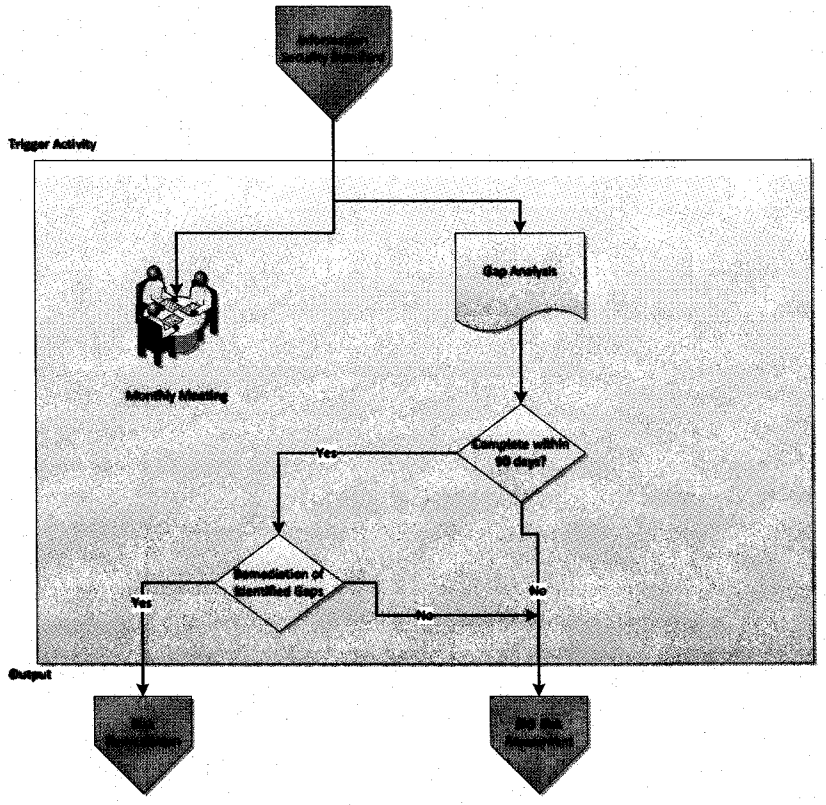


**Process Activity**

1. ISO will develop Information Security Standards based on information security best practices and regulatory requirements
2. Departments must complete a gap analysis within 90 days of the release of an Information Security Standard
3. ISO will provide Departments with gap analysis templates
4. Departments will provide the ISO with monthly status updates
5. Copies of the completed gap analysis must be provided to the ISO
6. Departments must engage the ISO to complete the Risk Assessment and Acceptance Processes for all identified gaps that will not be remediated
7. Departments must immediately contact the ISO if they determine that they will not be able to complete the gap analysis within the required 90 day timeframe
8. The Risk Assessment and Acceptance Processes must be followed if the gap analysis is going to exceed the 90 day timeframe

**Process Flow**

Risk Mitigation Process



## RISK ASSESSMENT

Process Overview

The Risk Assessment Process provides a consistent, systematic process to identify, analyze and classify risk. This systematic process must provide comparable and reproducible results. This process is triggered by the identification of a gap or the annual re-evaluation of accepted risk. The output of this process is classified risk. If classified risk will not be mitigated, the Risk Acceptance Process must be followed to ensure the risk is appropriately accepted. Only the ISO is authorized to document formal information security risk assessments.

Process Activity

1. Identify information assets
2. Identify vulnerabilities associated with the area of non-conformance
3. Identify threats that could exploit identified vulnerabilities
4. Identify mitigating controls
5. Identify previously accepted risks

- Review all currently accepted risks for the identified information assets in order to understand what, if any, relationship this risk may have with any accepted risks.

6. Identify Information Security Incident Probability (ISIP)

- ISIP will be classified using the following criteria:

| | **High** | **Medium** | **Low** |
|---|---|---|---|
| Probability | Highly Likely | Probable | Not Likely |

- The ISIP is based on a combination of the following factors:
    - Frequency of attempt - How often is this attack attempted?
    - Ease of exploit - How sophisticated is the attack?
    - Do likely attackers have the skills to execute the attacks?
    - Strength of controls - How vulnerable is the information asset? To what extent do the existing controls mitigate the risk?
    - Are there any currently accepted risks that:
        - Increase the frequency of attempt?
        - Increase the ease of exploit?
        - Reduce the strength of existing controls?
    - Would accepting this risk:
        - Increase the overall level of risk to the department or county?
        - Increase the risk of another currently accepted risk?
        - Increase the reliance on a specific control or set of controls?

7. Identify operational state
   - Business as usual
   - Regional disaster
8. Identify potential scenario
9. Quantify business impact
   - Financial
   - Constituent confidence
10. Identify Business Impact Rating (BIR)
   - Identify the BIR of an incident. The highest level of identified business impacts must be used for this assessment. BIR is classified based on the following parameters.

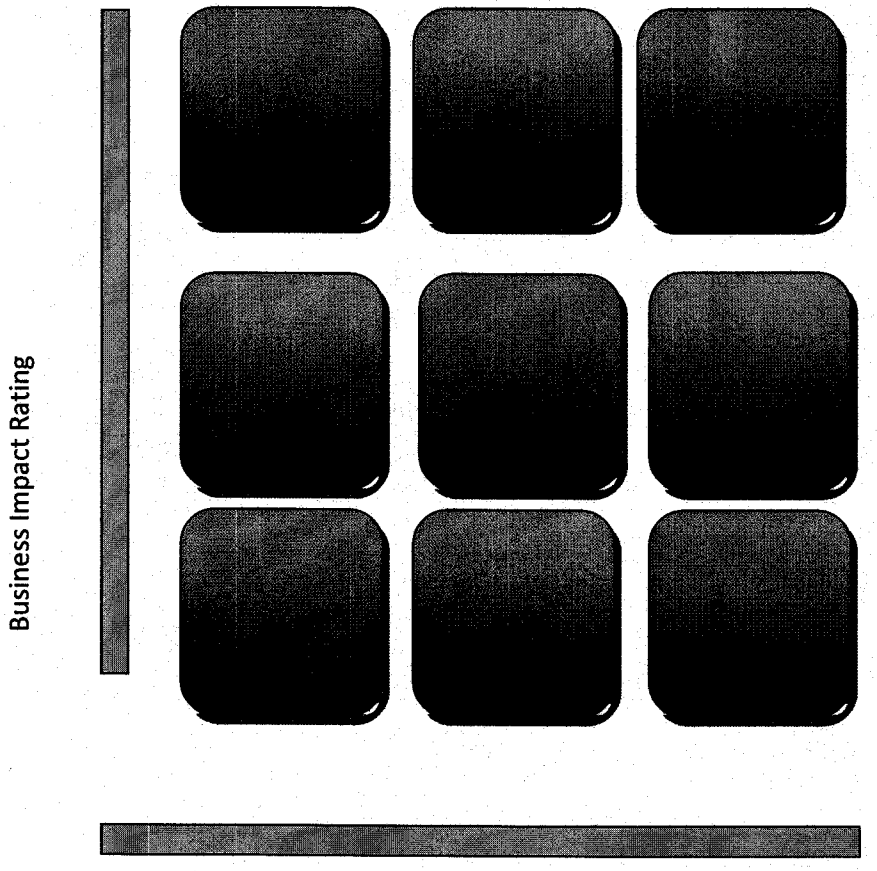
| **Constituent Confidence** | | |
|---|---|---|
| **Severe** | **Moderate** | **Minor** |
| Extensive Dissatisfaction | Moderate Dissatisfaction | Limited Dissatisfaction |

| **County Finances** | | |
|---|---|---|
| **Severe** | **Moderate** | **Minor** |
| Monetary Loss<br>Greater than $5,000,000 | Monetary Loss between<br>$1,000,000 and $5,000,000 | Monetary Loss<br>Less than $1,000,000 |

11. Classify the risk according to the Risk Classification matrix.

****continues on next page****

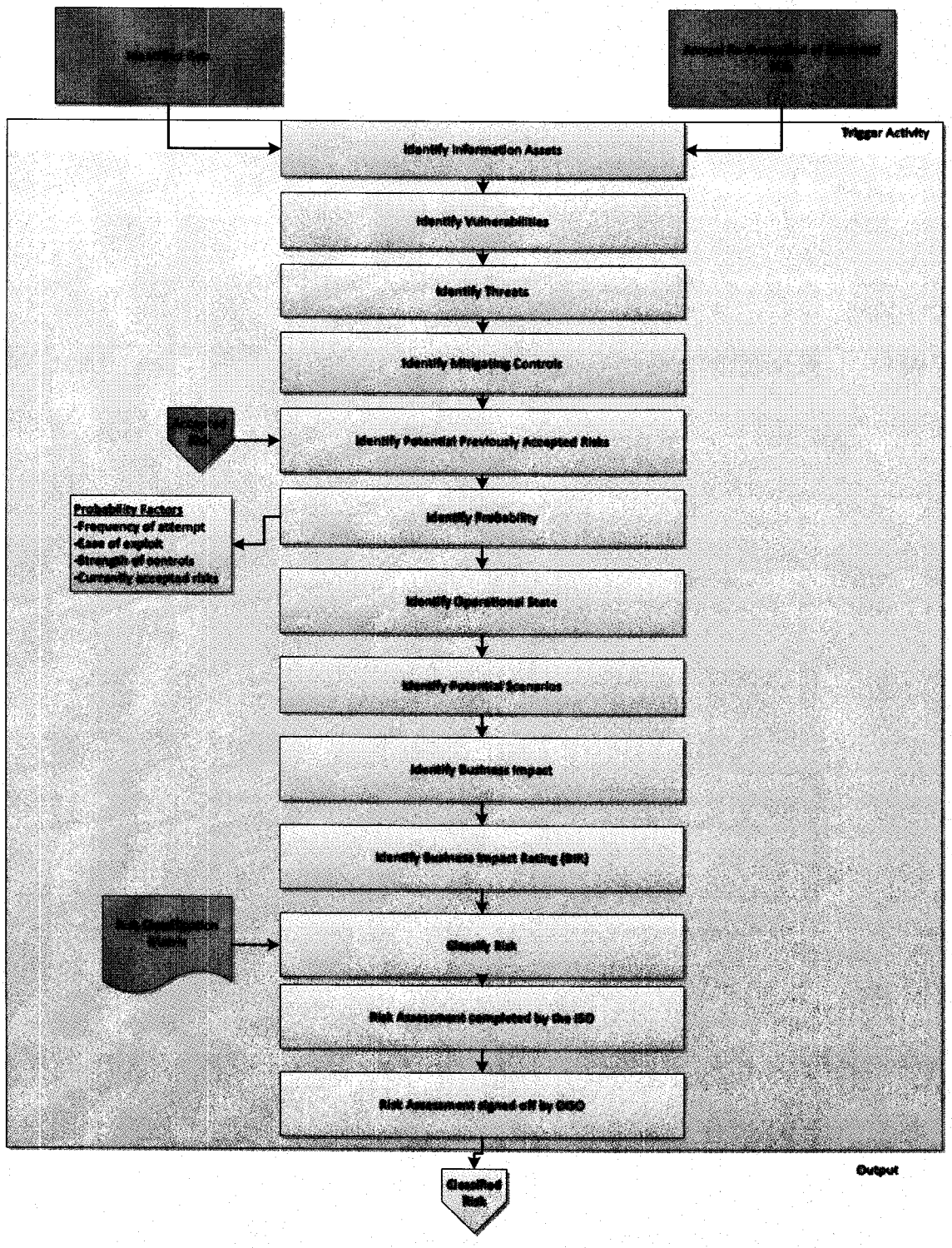
RISK CLASSIFICATION MATRIX



12. Risk Assessment completed by Departmental ISO Representative, and reviewed with DISO and submitted to the CISO for signoff.

13. Risk assessment signoff to be completed by the Chief Information Security Officer

Risk Assessment Process



## RISK ACCEPTANCE

### Process Overview

The Risk Acceptance Process provides a consistent, structured process to objectively accept information security risk in accordance with Riverside County's risk acceptance criteria. If the Chief Information Security Officer is unwilling to accept the classified risk, the Department will remediate the gap or implement other mitigating controls to reduce the risk to an acceptable level.

### Process Activity

1. Acceptance requests submitted to the CISO by the Department Head on the Risk Acceptance Form.

2. ISO to validate the business impact as appropriate (Executive Office, Public Information Officer, Risk Management, County Counsel etc.)

3. Risk accepted

   - CISO will generate and distribute an executive report to the informed parties as identified in the Operational Risk Acceptance Table
   - All risk acceptances for critical and high risks will expire, by default, on an annual basis
   - At time of expiration, each risk must be re-assessed and re-accepted.

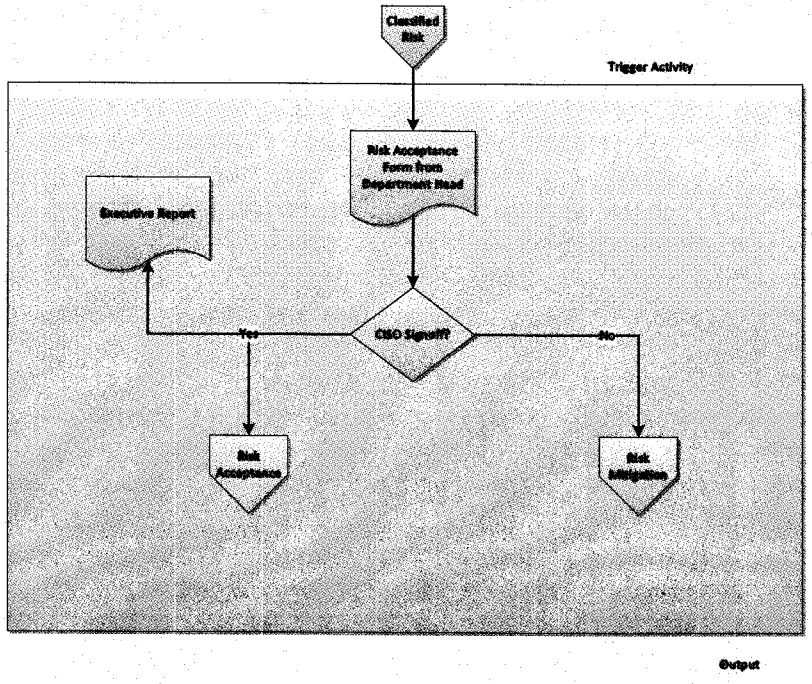
4. Risk not accepted

   - Department will remediate gap or implement other mitigating controls to reduce the risk to a level that Riverside County is willing to accept

### Operational Risk Acceptance Table

| Risk Classification | Authorized Acceptor(s) | Informed Parties |
|---|---|---|
| CRITICAL RISK | CISO | Executive Office |
| HIGH RISK | CISO | Executive Office |
| MEDIUM RISK | CISO | Executive Office |
| LOW RISK | DEFAULT ACCEPTANCE | Not Applicable |

## PROCESS FLOW




## REFERENCE SECTION

*N/A*

## REVISION HISTORY

| Change Date | Changed by (Name) | Revision | Description of Changes | Approved By | Approval Date |
|---|---|---|---|---|---|
| 03/16/09 | Sebron | 1.0 | Published Document | Jack B. Miller | 03/17/09 |

## 3.23 Attachment A-68- Riverside County Trusted System Policy

See attached Policy A-68 in PDF format.

**COUNTY OF RIVERSIDE, CALIFORNIA**
**BOARD OF SUPERVISORS POLICY**

| Subject: | Policy Number | Page |
|---|---|---|
| TRUSTWORTHY OFFICIAL ELECTRONIC RECORDS PRESERVATION | A-68 | 1 of 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; 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 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 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.

3. 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 the 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 www.aiim.org/standards, or from the California Secretary of State at 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.

**Reference:**
**Minute Order 3.12 of 07/26/2011**
**Minute Order 3-31 of 12/17/2013**

# 4 APPENDICES

# Appendix A – Acceptance Actions / Change Log

| Log # | Date | Specification / Milestone | Revision # | Action / Change Description | Current Owner | Status | Notes, Resolution, Decision | Target Close | Close Date | Approved By: |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | |
| 2 | | | | | | | | | | |
| 3 | | | | | | | | | | |
| 4 | | | | | | | | | | |
| 5 | | | | | | | | | | |
| 6 | | | | | | | | | | |
| 7 | | | | | | | | | | |
| 8 | | | | | | | | | | |
| 9 | | | | | | | | | | |
| 10 | | | | | | | | | | |
| 11 | | | | | | | | | | |
| 12 | | | | | | | | | | |
| 13 | | | | | | | | | | |
| 14 | | | | | | | | | | |
| 15 | | | | | | | | | | |
| 16 | | | | | | | | | | |
| 17 | | | | | | | | | | |
| 18 | | | | | | | | | | |
| 19 | | | | | | | | | | |
| 20 | | | | | | | | | | |

## Appendix B – Development Acceptance Certificate

### Development Acceptance Certificate

| Project Name | Land Management System | Reference Number | |
|---|---|---|---|
| Priority | | Date Requested | |
| Requestor | | Date Required | |

| Summary of Development Required |
|---|
| |
| |
| |

| Deliverables Control | Status |
|---|---|
| 1. Business Specification Completed Date: | |
| 2. Technical Specification Completed Date: | |
| 3. Development Completed (includes unit testing) Date: | |
| 4. User Acceptance Testing Completed Date: | |
| 5. Development Review Meeting Date: | |
| 6. Roll Back Plan Reviewed Date: | |

| Schedule Impact & Scope of Work | | | |
|---|---|---|---|
| | | Date Approved | Implementation |

| | | | |
|---|---|---|---|
| | | | Phase |
| Business Owner Name | | | |
| Business Owner Name | | | |
| Business Sponsor Name | | | |
| Comments: | | | |

| Decision | | | |
|---|---|---|---|
| | Approved | | Rework Required |
| | Approved with Changes | | Other |

By: Tyler Project Manager _____ Date: _____

By: TLMA Project Manager _____ Date: _____

By: TLMA Delivery Manager _____ Date: _____

# Appendix C – Milestone Acceptance Certificate

Milestone Acceptance Certificate

| | | | |
|---|---|---|---|
| Project Name | TLARC-371 | Reference Number | |
| Milestone/Phase # | | Date Requested | |
| Requestor | | Date Required | |

| |
|---|
| This certificate confirms acceptance of the following Milestones as defined in the Statement of Work executed as part of the LMS Contract <Date>. |
| <Milestone Description> |
| |
| |

| Approved deliverables included in this milestone | |
|---|---|
| Please list each deliverable | |
| 1. | 21. |
| 2. | 22. |
| 3. | 23. |
| 4. | 24. |
| 5. | 25. |
| 6. | 26. |
| 7. | 27. |
| 8. | 28. |
| 9. | 29. |
| 10 | 30. |

| | |
|---|---|
| 11. | 31. |
| 12. | 32. |
| 13. | 33. |
| 14. | 34. |
| 15. | 35. |
| 16. | 36. |
| 17. | 37. |
| 18. | 38. |
| 19. | 39. |
| 20. | 40. |

| Decision | | | |
|---|---|---|---|
| | Approved | | Not-Approved |

By: Tyler Project Manager _____ Date: _____

By: TLMA Project Manager _____ Date: _____

By: TLMA Delivery Manager _____ Date: _____

## Appendix D – Change Request Form

| | TLARC-371 LMS | | |
|---|---|---|---|
| | | | |
| | | | |

| Change Request Description |
|---|
| 1. |
| 2. |
| 3. |
| **Reason for Request** |
| |
| **Business Requirements** |
| 1. |
| 2. |
| 3. |
| |
| **Recommended Change** |
| 1. |
| 2. |
| 3. |
| **Impact Analysis (to be completed by Tyler)** |

| Estimated Cost: | Estimated Hours: | Deliverable Date: |
|---|---|---|
| Describe Impact to any other project deliverable: | | |
| **Decision** | | |
| Approved | Rejected | |
| Approved with modifications | Deferred | |
| **Approvals** | | |
| Business Owner: | TLMA Project Manager: | |
| Tyler Project Manager: | TLMA Project Manager: | |
| TLMA Project Manager: | TLMA Delivery Manager: | |

# Appendix G1 – Riverside County User Agreement

**Riverside County Enterprise**

**Information Systems Security Policy**

**User Agreement**

I have read, understand and am fully aware of the County of Riverside Enterprise Information Systems Security Policy; and I agree to comply with the terms of this policy.

I also agree to remain informed of and comply with future revisions to this policy.

As a user of the County's information systems, you will have access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all users actively support and fully comply with the measures described in the Enterprise Information Systems Security Policy. Failure to comply can place the entire County network at serious risk; and users who fail to comply will be subject to disciplinary action.

Users of the County's information systems shall at all times act in accordance with all applicable laws and County policies, rules or procedures. Users shall not use County information systems in an improper or unauthorized manner.

**User Name:** _____

**Signature:** _____

**Date:** _____

**Responsible Manager Approval Authority**

**Name and Title:** _____

**Signature:** _____

**Date:** _____

**This form shall be retained in department, district or agency files.**

# Appendix G2 – Riverside County Remote Access Agreement

**Riverside County Enterprise**

**Information Systems Security Policy**

**Remote Access Agreement**

I have read, understand and am fully aware of the terms of the County of Riverside Enterprise Information Systems Security Policy, especially as applied to remote users of the County's information systems; and I agree to comply with the terms of this policy. I also agree to remain informed of and comply with future revisions to this policy.

As a remote user of the County's information systems, you will have unique access to sensitive resources that are connected through the County network. To assure security throughout the entire County network, it is critical that all remote users actively support and fully comply with the measures described in the Enterprise Information Systems Security Policy. Failure to comply can place the entire County network at serious risk; and remote users who fail to comply will be subject to disciplinary action.

Remote users of the County's information systems shall at all times act in accordance with all applicable laws and County policies, rules or procedures. Remote users shall not use County information systems in an improper or unauthorized manner.

**Remote User Name:** _____

**Signature:** _____

**Date:** _____

**Responsible Manager Approval Authority**

**Name and Title:** _____

**Signature:** _____

**Date:** _____

**This form shall be retained in department, district or agency files.**

## Appendix H1 – Hardware Configuration Details Worksheet

(Tyler to review and recommend any changes required)

# Hardware Configuration Details –Proposed

| | Hardware Description | Model | Version | Quantity | Environment | Other Details |
|---|---|---|---|---|---|---|
| 1 | **Web Server**<br><br>Operating System Microsoft Windows 2012<br><br>Host Processor: Intel© Xeon© E5 -2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 8 GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS ), D = 100 (LMS Program, DB and Data Files, and Reserved disk space) | Virtual Machine | Current | 1 | Development | |
| 2 | **Application Server**<br><br>Operating System Microsoft Windows 2012<br><br>Host Processor: Intel© Xeon© E5 -2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 4GB RAM<br><br>1000mbps Ethernet N IC<br><br>SAN Drive Space: C = 60 GB (OS), D = 200 GB (LMS Program Files and Reserved disk space) | Virtual Machine | Current | 1 | Development | |

| | Hardware Description | Model | Version | Quantity | Environment | Other Details |
|---|---|---|---|---|---|---|
| 3 | **SQL Server**<br>Operating System Microsoft Windows 2012<br><br>Database Microsoft SQL Server 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 4GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 500 GB (LMS Program, DB and Data Files, and Reserved disk space) | Virtual Machine | Current | 1 | Development | |
| 4 | **Web Server**<br>Operating System Microsoft Windows 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 8GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 500 GB (LMS Program, DB and Data Files, and Reserved disk space) | Virtual Machine | Current | 1 | Test / Staging | |
| 5 | **Application Server**<br><br>Operating System Microsoft Windows 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB) | Virtual Machine | Current | 1 | Test / Staging | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Memory 4GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 200 (LMS Program Files and Reserved disk space) | | | | | |
| | **Hardware Description** | **Model** | **Version** | **Quantity** | **Environment** | **Other Details** |
| 6 | **SQL Server**<br><br>Operating System Microsoft Windows 2012<br><br>Database Microsoft SQL Server 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 16GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 500 GB (LMS Program, DB and Data Files, and Reserved disk space) | Virtual Machine | Current | 1 | Test / Staging | |
| 7 | **Web Server**<br>Operating System Microsoft Windows 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 32GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 200 GB (LMS Program, DB and Data Files, and Reserved disk space) | Virtual Machine | Current | 4 | Production | |
| 8 | **Application Server**<br>Operating System Microsoft Windows 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB) | Virtual Machine | Current | 1 | Production | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Memory 32GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 200 GB (LMS Program, DB and Data Files, and Reserved disk space) | | | | | |
| | **Hardware Description** | **Model** | **Version** | **Quantity** | **Environment** | **Other Details** |
| 9 | **SQL Server (Clustered)**<br>Operating System Microsoft Windows 2012<br><br>Database Microsoft SQL Server 2012 Enterprise<br><br>Host Processor: 2 Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB)<br><br>64GB PCL-10600R-9 (Low voltage DIMM) RAM<br><br>2Gb 331 FLR Ethernet Adapter 4 Ports<br><br>Local Disk Space: C = 60 GB (OS), D = 200 GB (LMS Program Files and Reserved disk space)<br><br>SAN Drive Space: LUN1 (RAID10) SQL DB Files<br><br>LUN2(RAID5) 20TB Data | Virtual Machine | Current | 4 | Production | |
| 10 | **Reporting Services Server**<br><br>Operating System Microsoft Windows 2012<br><br>Database Microsoft SQL Server 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 16GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 500 GB (LMS Program, DB and Data Files, and Reserved disk space) | Virtual Machine | Current | 1 | Development | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 11 | **Reporting Services Server**<br><br>Operating System Microsoft Windows 2012<br><br>Database Microsoft SQL Server 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 16GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 500 GB (LMS Program, DB and Data Files, and Reserved disk space) | Virtual Machine | Current | 1 | Test/Staging | |
| 12 | **Reporting Services Server**<br><br>Operating System Microsoft Windows 2012<br><br>Database Microsoft SQL Server 2012<br><br>Host Processor: Intel© Xeon© E5-2660 (8 core, 2.20 GHz, 20 MB)<br><br>Memory 16GB RAM<br><br>1000mbps Ethernet NIC<br><br>SAN Drive Space: C = 60 GB (OS), D = 500 GB (LMS Program, DB and Data Files, and Reserved disk space) | Virtual Machine | Current | 1 | Production | |

*** The remainder of this page has been left intentionally blank ***

# Appendix H2 – Software Configuration Details Worksheet

(Worksheet to be completed by Tyler)

| | Software Description | Vendor | Version | Qty | Environment | Other Details |
|---|---|---|---|---|---|---|
| 1 | **Operating System Microsoft Windows 2012** | Microsoft | Current | 15 | Development, Test/Staging, Production | |
| 2 | **Database Microsoft SQL Server 2012** | Microsoft | Current | 6 | Development, Test/Staging, Production | |
| 3 | **Microsoft IIS 7.0** | Microsoft | Current | 6 | Development, Test/Staging, Production | |
| 4 | **ArcGIS** | ESRI | 10 or Greater | 1 | Development, Test/Staging, Production | |
| 5 | **Bluebeam** | Bluebeam | Current | TBD | Production | |
| 6 | **Laserfiche** | TBD | Current | TBD | Production | |

# Appendix H3 – Peripherals Configuration Details Worksheet

## (Tyler to review and recommend any changes needed)

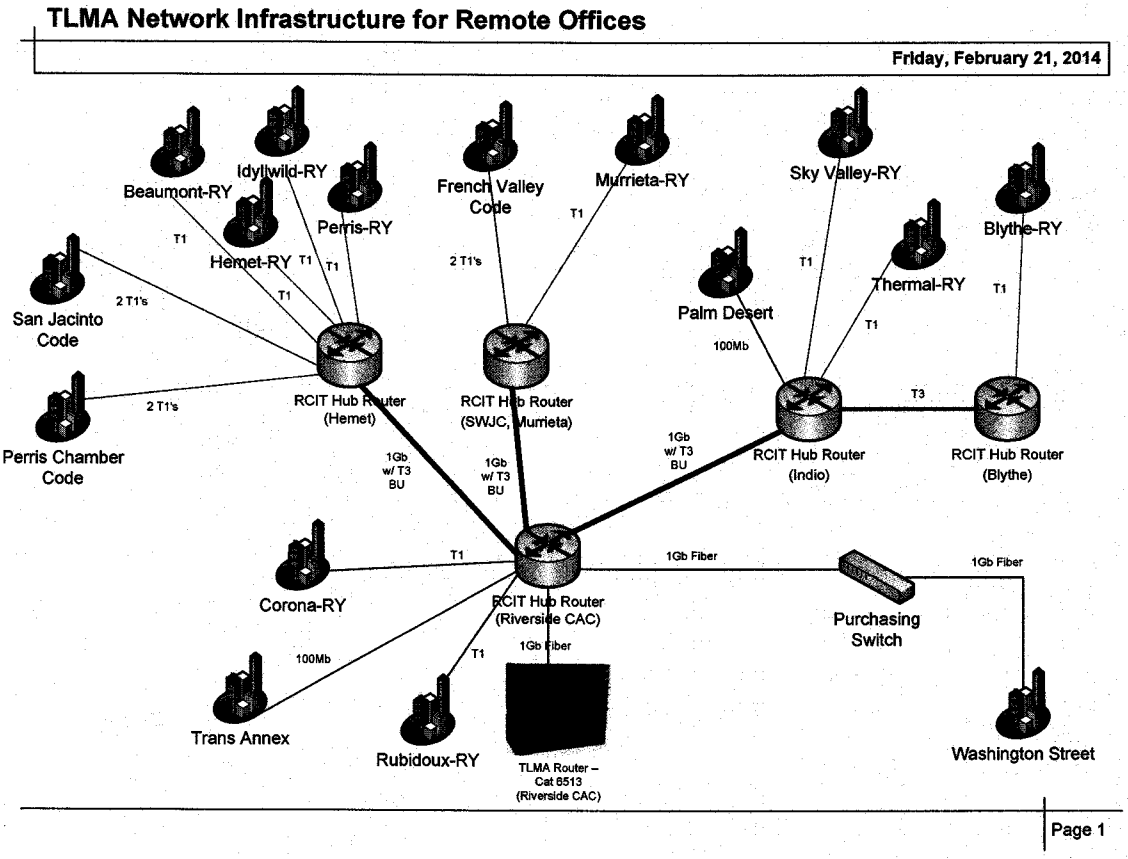
| | Peripheral Description | MFG/Vendor | Model | Quantity | Other Details |
|---|---|---|---|---|---|
| 1 | Scanner | Cannon | DR-5010C, DR-2510C, DR-4010C, DR-3010C, DR-M160, DR-X10C, DR-7550C, DR-6050C, DR-9050C | TBD | |
| | | Fujitsu | Fi-6110, fi-6670, fi-6770, fi-6240Z, fi-6130Z, fi-6140Z, fi-6230Z | TBD | |
| | | Graphtex | CS500 Pro | TBD | |
| | | Hewlett Packard | ScanJet 8250, ScanJet 8350, ScanJet 8390 | TBD | |
| | | Panasonic | KV-S2045C | TBD | |
| | | Xerox | Documate 152 | TBD | |
| 2 | Receipt Printer | Epson | Epson 6000 or Epson 950 | TBD | |
| 3 | Cash Drawer | Media Plus | Media Plus Automated Cash Drawer | TBD | |
| 4 | ID LMS Readers | Magtek | Mag Mini Swipe Reader | TBD | |
| 5 | Barcode Scanner | Topaz | T-L462-HSB-R | TBD | |
| 6 | USB Signature Pad | TBD | TBD | TBD | |
| 7 | QR Code Scanner | TBD | TBD | TBD | |
| 8 | Label printer | Zebra | ZebraGK420T Label printer | TBD | |
| 9 | Tablet | Apple | IPAD 2 or Greater | TBD | |
| 10 | Windows Laptop | HP or Dell | Any Windows 7 Laptop | TBD | |

## Appendix H4 – Configuration Parameters and Settings

(To be completed by Tyler)

| Item Number | Description | Parameter | Setting | Environment | Other Details |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# Appendix I – TLMA Network Design Diagram



# 5 Functional Requirements

## 5.10 Attachment REQ- Functional Requirements

### 5.1.1 Core Product Requirements

FORM APPROVED COUNTY COUNSEL
BY: _____ 6/30/14
NEAL R. KIPNIS DATE

| | | | |
|---|---|---|---|
| All | Application Data and Intake Requirements | 4.a | Ability to begin the application process from a GIS map, using either an assessor parcel number, address or polygon. |
| All | Application Data and Intake Requirements | 4.b | When entering an address, the application must validate the address against the "Master Address File" maintained by County GIS as well as, perform an intelligent table look up for validating common abbreviation and variations into a standard address name format. |

| | | | | |
|---|---|---|---|---|
| All | Application Data and Intake Requirements | 4.c | Application must be able to note the suite, apartment number or space number in the address line and/or separate searchable data field (i.e. spaces in mobile home parks must be easily searchable). | [redacted] |
| All | Application Data and Intake Requirements | 4.d | The application must provide the ability to update site information attributes easily, including bulk refreshes of parcel and parcel owner information from the County Assessor and the addition of new addresses that may be created at application intake. | |
| All | Application Data and Intake Requirements | 4.e | The ability of the system to duplicate part or all of the data from one permit record or application to another and from field to field. | |
| All | Application Data and | 4.f | Does the solution support having | |

| | | | | |
|---|---|---|---|---|
| | Intake Requirements | | site addresses explicitly linked to parcels, so staff can readily verify ownership and other property attributes? | [redacted] |
| All | Application Data and Intake Requirements | 4.g | Once the address or assessor parcel number is provided, does the solution automatically fill in property based information applicable to the permit such as owner name, mailing address, legal description and other site information. | |
| All | Application Data and Intake Requirements | 4.h | Ability of GIS information, like property characteristics, legal description, zoning information and environmental information to link to the permit record to capture that information and permanently associate it with the permit and be unalterable. | |
| All | Application Data and Intake Requireme | 4.i | Description field must allow for capture of a short description and | |

| | | | | |
|---|---|---|---|---|
| | nts | | long description field with unlimited characters, or combination of the two. | [redacted] |
| All | Application Data and Intake Requirements | 4.j | Ability to generate request for refund checks | |
| All | Application Data and Intake Requirements | 4.k | Application must have ability to record multiple people associated with the project as well as show current and previous people associated with the project (i.e. Old owner and new owner, old contractor and new contractor) and date stamp the information. | |
| All | Application Data and Intake Requirements | 4.l | Ability to record the name, company name, address, phone number, e-mail, fax and notation, for numerous people fields. | |
| All | Application Data and Intake Requireme | 4.m | Ability of the application to allow for at least 30 unique people field titles that are | |

| | | | | |
|---|---|---|---|---|
| | nts | | editable and expandable. (i.e. people titles include, owner, applicant, engineer, biologist, payee). | [redacted] |
| All | Application Data and Intake Requirements | 4.n | Ability to change the title of a person associated with the permit without having to re-enter all of the data. (i.e. make the owner, the applicant) | |
| All | Application Data and Intake Requirements | 4.o | Ability to attach multiple addresses, but assign only one primary address to a permit or case, and ability to attach multiple assessor parcel numbers. | |
| All | Application Data and Intake Requirements | 4.p | Ability to make deductions to clearing account and post funds to revenue accounts The ability of the system to remind users about other related permits that may be required given the type of application or permit started. | |

| | | | | |
|---|---|---|---|---|
| All | Application Data and Intake Requirements | 4.q | For case types such as mitigation fees, hourly permits and shopping centers, ability to allow multiple addresses and multiple APNs to be attached without having to select a primary address. | [redacted] |
| All | Application Data and Intake Requirements | 4.r | System must be able to flag incomplete/inaccurate information and prompt the user to edit for corrections prior to "saving" the data/record. | |
| All | Application Data and Intake Requirements | 4.s | Upon entry of address or APN does your solution automatically search for pending projects involving the same address or APN | |
| All | Application Data and Intake Requirements | 4.t | Ability of the system to check for locks/holds/notices, code enforcement actions and other notifications on any APN, address or | |