CITY OF EL PASO, TEXAS
AGENDA ITEM
DEPARTMENT HEAD'S SUMMARY FORM

REVISED
11:10 am, Aug 27, 2025

DEPARTMENT: Information Technology

AGENDA DATE: September 3 , 2025

PUBLIC HEARING DATE: 09/03/25

CONTACT PERSON NAME: Carolyn Patrick, Chief Information Officer **PHONE NUMBER:** 1-915-212-1408

2nd CONTACT PERSON NAME: Peter Pacillas, Police Chief **PHONE NUMBER:** 1-915-212-4305

DISTRICT(S) AFFECTED: All Districts

STRATEGIC GOAL:

Goal 5: Promote Transparent & Consistent Communication Amongst all Members of the Community

SUBGOAL:

5.2 Leverage and expand the use of current and new technology to reduce inefficiencies and improve communications

SUBJECT:

A resolution authorizing the mayor to sign the Interlocal agreement between the 911 District, City of El Paso, and the County of El Paso for Law Enforcement Information Sharing for the On-Call Records Management System. The City will fund the On-Call Records Management System at 50% and the County of El Paso will fund in the amount of 50%. The 911 District will serve as the provider of the infrastructure, software application, and technical support for the RMS.

BACKGROUND / DISCUSSION:

On February 13, 2003, the City of El Paso and the County of El Paso entered into an agreement to establish the Combined Records Information Management Enterprise (CRIME), a regional law enforcement information system, to facilitate the sharing of law enforcement information. On December 14, 2021, the City of El Paso and the County of El Paso entered an interlocal agreement that superseded the 2003 CRIME agreement, thereby establishing a shared responsibility for the On Call Records (WebRMS) system for law enforcement resource sharing, with costs to be split equally (50/50).

COMMUNITY AND STAKEHOLDER OUTREACH:

N/A

PRIOR COUNCIL ACTION:

February 13,2003 - Agreement to establish a combined law enforcement information sharing system.
December 14,2021 - Agreement to share the cost and responsibility of the On Call Records Management System (WebRMS).

AMOUNT AND SOURCE OF FUNDING:

Dept: 239 Fund:1000 Division:15240 Account: 533025 Program: P1506
Year 1: $639,412.00 Year 2: $369,786.00 Year 3: $369,786.00

REPORTING OF CONTRIBUTION OR DONATION TO CITY COUNCIL:

N/A

NAME	AMOUNT ($)

********************REQUIRED AUTHORIZATION********************

DEPARTMENT HEAD: _____

(If Department Head Summary Form is initiated by Purchasing, client department should sign also)

RESOLUTION

WHEREAS, the Interlocal Cooperation Act, Sec 791.001, et seq., Texas Government Code authorizes local governments to contract with one another to carry out their governmental functions; and

WHEREAS, the City and County of El Paso, Texas agree that providing information sharing and services on a regional basis will provide more efficient, effective, and less costly services for both the City and the County, thereby saving the public costs and serves a governmental purpose; and

WHEREAS, public safety in the region is significantly enhanced with the continued operation of OnCall RMS through improved communication and data availability for participating agencies; and

WHEREAS, the El Paso County 911 District is a participating agency in acquiring OnCall RMS and sharing law enforcement information with other agencies; and

WHEREAS, the El Paso County Sheriff's Office is a participating agency in acquiring OnCall RMS and sharing law enforcement information with other agencies; and

WHEREAS, the El Paso City Police Department is a participating agency in acquiring OnCall RMS and sharing law enforcement information with other agencies; and

NOW, THEREFORE, BE IT RESOLVED:

That, the El Paso City Council authorize the Mayor of the City of El Paso to enter into an Interlocal Agreement with the County of El Paso Texas and the El Paso County 911 District to facilitate the shared administration, management, and use of the OnCall Records Management System for law enforcement agencies

ADOPTED this _____ day of _____,2025.

CITY OF EL PASO

ATTEST:

Renard U. Johnson
Mayor

Laura D. Prine
City Clerk

APPROVED AS TO FORM:

Robert Aguinaga Jr

Roberto Aguinaga
Assistant City Attorney

APPROVED AS TO CONTENT:

Carolyn Patrick

Carolyn Patrick
Director of Information Technology

LAW ENFORCEMENT INFORMATION SHARING

MUTUAL SUPPORT SERVICES

Interlocal Agreement

BETWEEN

El Paso County, The City of El Paso, and El Paso County 911 District

FOR

LAW ENFORCEMENT INFORMATION SHARING

For The

OnCall Records Management System

This agreement supersedes the Interlocal Agreement between El Paso County and the City of El Paso for Law Enforcement Sharing Mutual Support Services for the OnCall Records Management system entered December 20, 2021. This agreement entered into by and between El Paso County, a political subdivision of the State of Texas, hereinafter referred to as "the County", the City of El Paso, a home rule municipal corporation situated in El Paso County, Texas, hereinafter referred to as "the City", and the El Paso County 911 District, an Emergency Communications District situated in El Paso County, Texas, hereinafter referred to as "the 911 District", pursuant to the Interlocal Cooperation Act, Sec. 791.001, et seq., Texas Government Code, for the continued mutual support services of a regional law enforcement information system that provides the means for participating agencies to share law enforcement information. This information sharing is possible through a common system known as the On-Call Records Management System. All parties shall be participating agencies. This agreement includes all items necessary to define the terms and arrangements between the parties.

RECITALS

WHEREAS, the Interlocal Cooperation Act, Sec 791.001, et seq., Texas Government Code authorizes local governments to contract with one another to carry out their governmental functions; and

WHEREAS, the County and the City agree that providing information sharing and services on a regional basis will provide more efficient, effective, and less costly services for both the City and the County, thereby saving the public; and

WHEREAS, public safety in the region is significantly enhanced with the continued operation of OnCall RMS through improved communication and data availability for participating agencies; and

WHEREAS, the El Paso County 911 District is a participating agency in acquiring OnCall RMS and sharing law enforcement information with other agencies; and

WHEREAS, the El Paso County Sheriff's Office is a participating agency in acquiring OnCall RMS and sharing law enforcement information with other agencies; and

LAW ENFORCEMENT INFORMATION SHARING

MUTUAL SUPPORT SERVICES

WHEREAS, the El Paso City Police Department is a participating agency in acquiring OnCall RMS and sharing law enforcement information with other agencies; and

NOW, THEREFORE, in consideration of the mutual promises contained herein, and of other good and valuable consideration, and intending to be bound hereby, the County, the City, and the 911 District agree as follows:

1. Purpose

This Interlocal Agreement (hereinafter referred to as "Agreement") is entered into by and between the County, the City, and the 911 District to facilitate the shared administration, management, and use of the OnCall Records Management System for law enforcement agencies, (hereinafter referred to as "the Software").

2. Scope of Agreement

The County, the City, and the 911 District agree to collaborate on the Software to ensure its effective management, ongoing maintenance, and optimization for enhanced operational efficiency and improved data-sharing capabilities for all participating agencies.

3. Responsibilities

3.1 Software Access

The County and the City shall continue to have access to the Software as participating agencies under the governance of the 911 District. As part of the transition of license ownership and administration, the 911 District will assume responsibility for the Master Services Agreement (MSA) governing the Software. Access for the County and the City will be maintained in accordance with the terms and conditions established by the MSA, ensuring uninterrupted operational use.

The City of El Paso Police Department will assign two (2) EPPD personnel with a primary function of EPPD Tier 1 support. The positions will be co-located with the dedicated 911 District support employees. The two EPPD positions will be fully funded by EPPD.

3.2 Data Sharing

The County, the City, and the 911 District agree to share operational data as necessary for the effective operation of the Software. Data-sharing protocols must adhere to applicable privacy laws and regulations.

3.3 Support Roles and Maintenance

The **City** and the **County** are responsible for providing **Tier 1 Support**, which includes first-line user assistance for their respective agencies as outlined below.

The 911 District will function as **Tier 1 Support** for all other participating agencies, serving as the primary point of contact for basic troubleshooting and issue resolution. Additionally, the 911 District will act as

Tier 2 Support, serving as the RMS System and Application Administrators. This includes addressing escalated issues requiring advanced troubleshooting, managing system configurations, coordinating with the software vendor, supporting external agencies, overseeing system integrations, and ensuring overall system performance and reliability as outlined below.

Tier 1 Support

1. **Basic Troubleshooting**
    - Guiding users through basic application functions (e.g., navigating menus, running basic reports, resetting views).
    - Identifying and addressing connectivity issues (e.g., verifying internet connections or local workstation problems).
    - Recommending best practices for common user errors (e.g., incorrect data entry workflows).
2. **Expanded User Management and Account Creation**
    - **User Account Maintenance:**
        - Updating user profiles with agency-specific details (e.g., rank, role, permissions).
        - Disabling accounts for inactive users or upon employee separation.
        - Periodic reviews of user accounts to ensure alignment with industry's best practices and CJIS requirements.
    - **Role-Based Access Assignments:**
        - Assigning roles based on user responsibilities and permissions approved by agency staff and upon submittal of appropriate forms and documentation.
        - Verifying and applying role-specific restrictions to prevent unauthorized access.
    - **Account Audits:**
        - Conducting basic account usage checks to identify and flag inactive or non-compliant accounts.
        - Reporting anomalies (e.g., multiple failed login attempts, suspicious activity) to Tier 2.
    - **Agency-Specific Workflows:**
        - Configuring users according to agency-specific workflows, such as enabling modules or features based on operational needs.
3. **Knowledge Base and Self-Help Resources**
    - Providing users with access to FAQs, tutorials, and step-by-step guides.
    - Delivering instructions for minor tasks like updating profile settings or system preferences.
4. **Incident Logging and Categorization**
    - Logging incident details, including screenshots, error messages, or timestamps, into a ticketing system.
    - Assigning priorities and categories to tickets to facilitate escalation to Tier 2.
5. **System and Network Connectivity Awareness**
    - Checking user-specific access issues (e.g., incorrect credentials or inactive accounts).
    - Identifying localized outages or connectivity problems (e.g., agency-specific network problems).

- Escalating only when an issue is determined to be beyond local control.

6. **Basic System Maintenance Tasks**
   - **Workstation Requirements Check**
     - Verifying user workstations meet basic system requirements, including sufficient processing power and memory (e.g., CPU, RAM).
     - Properly configured, supported and updated browsers (e.g., ensuring compatibility with the system).
     - Installed and updated operating system and necessary drivers.
     - Network connectivity and speed are sufficient for system use.
   - **Session and Cache Management:** Helping users clear caches, refresh sessions, or restart services as needed to address minor glitches.
7. **Communication and Education**
   - Providing initial guidance for new features or updates.
   - Setting expectations for system limitations and timelines for resolutions.
8. **Monitoring and Pattern Recognition**
   - Noting patterns in user complaints and identifying trends (e.g., multiple users reporting the same error).
   - Escalating grouped incidents to Tier 2 with a consolidated description of the issue.

Tier 2 Support:

1. **24/7 Technical Support and Troubleshooting:**
   - Addressing escalated issues that require advanced problem-solving and technical expertise.
2. **Regular Software Updates and Maintenance:**
   - Applying small changes or fixes to the software, typically addressing bug fixes and security patches.
3. **Regular Software Upgrades and Maintenance:**
   - Managing upgrades to newer software versions with enhanced features and performance improvements.
4. **Issue Escalation and Vendor Coordination:**
   - Escalating unresolved issues to the software vendor via the support portal, providing the respective case number, and communicating progress and resolution details to County and City staff.
5. **Application Configurations:**
   - Managing and maintaining system configurations to ensure the software aligns with agency-specific workflows and operational needs.
6. **Advanced User Support and Troubleshooting:**
   - Resolving technical issues escalated by Tier 1, such as system errors, software malfunctions, and complex configuration problems.
   - Investigating and documenting root causes of recurring issues.
7. **System Configuration and Maintenance:**
   - Maintaining software configurations to align with operational needs and security requirements.
   - Managing database integrity tasks, including data cleanup and validation efforts.
8. **Training and Documentation:**

- Developing and delivering documented training for Tier 1 support staff, and train-the trainers; other identified and agreed upon users as needed.
- Maintaining a centralized knowledge base or support documentation repository to ensure consistency and self-service for common issues.

9. **System Monitoring and Reporting:**
   - Monitoring system performance and generating reports on usage, incident resolution, and recurring issues.
   - Providing statistical insights to identify trends and recommend proactive solutions.
10. **System Integration Support:**
   - Assisting with the implementation and maintenance of integrations with other systems, such as CAD, integrations, or other public safety applications.
   - Addressing issues related to data exchange or integration workflows.
11. **Security and Compliance:**
   - Ensuring the system adheres to security policies, including CJIS compliance.
   - Addressing any data access or breach concerns raised during operations.
   - Collaborating with agencies to review and update access controls as organizational needs evolve.

3.4 Integrations

The County and the City shall be granted the appropriate access to view and evaluate necessary resources, such as data, and database access to support their operational needs. This level of access will enable the evaluation of potential changes, additions, and deletions to integrations with other applications. The 911 District, serving as the overarching system administrator, shall collaborate with the County and the City to ensure the integration infrastructure is properly configured, maintained, and verified for functionality. This includes ensuring that integration endpoints are available and operational to support approved changes and initiatives while safeguarding system integrity and compliance. Additionally, the County and City shall have appropriate access to the database for data extracts and custom reports.

3.5 Configurations

To ensure the performance, integrity, and continuity of the system across all users, any proposed configuration changes must be submitted through the change management process. This process requires appropriate notification and consensus approvals from all relevant stakeholders, including the 911 District, to verify that changes do not inadvertently impact other agencies or the overall functionality of the system. As the overarching system administrator, the 911 District will oversee and coordinate these changes to maintain system stability, ensure alignment with established operational standards, and support the shared objectives of all participating agencies.

3.6 Change Management

The County, City, and 911 District recognize the importance of a coordinated change management process to maintain the integrity, reliability, and security of the shared environment. Given the differences in processes and priorities across the three organizations, a standardized and collaborative

approach is essential for evaluating, agreeing upon, and implementing changes. This ensures that all stakeholders are informed, and potential impacts are minimized.

3.6.1 Change Management Board

A Change Management Board (CMB) shall be established to oversee and approve change requests. The board will be comprised of the following representatives:

- One (1) El Paso Police Department (EPPD) representative
- One (1) El Paso County Sheriff's Office (EPCSO) representative
- One (1) City of El Paso IT representative
- One (1) County IT representative
- One (1) 911 District representative

For a change to be reviewed, at least 50% of the board members must be present. A Change Request must receive majority approval from the members in attendance before proceeding to implementation.

3.6.2 Change Request Submission

Any organization (County, City, or 911 District) may submit a change request. Requests must include:

- A clear description of the proposed change
- Justification for the change, including anticipated benefits
- A preliminary assessment of potential impacts on the shared environment

3.6.3 Evaluation

A joint change management team, with representatives from each organization, shall evaluate the request. The evaluation will consider:

- Technical feasibility
- Operational and security impacts
- Alignment with organizational goals
- Resource requirements

3.6.4 Agreement

Changes shall require documented approval from designated representatives of the County, City, and 911 District, in accordance with section 3.6.1 above. The approval process will involve:

- Finalizing the scope and details of the change
- Setting a timeline for implementation
- Ensuring all resources understand their roles and responsibilities

3.6.5 Implementation

Approved changes shall be implemented according to the agreed-upon plan. Implementation will include:

- Advance notice, where possible, to affected stakeholders
- Coordination with relevant teams to minimize disruptions
- Documentation of the process for future reference and system configuration upkeep with the vendor

3.6.6 Post-Implementation Review

Following implementation, the joint team shall review the change to:

- Verify that it meets the intended objectives
- Identify and address any unforeseen issues
- Update documentation

3.7 Maintenance Notifications

The 911 District shall make every effort to notify the County and the City of scheduled maintenance at least two (2) weeks in advance. The Software maintenance plan, at a minimum, will include the following:

- Resources: Identification of personnel, equipment, and other resources required for successful execution of maintenance activities.
- Maintenance Schedule: Maintenance will be scheduled on mutually agreed dates and times, with agreed-upon hours for the maintenance timeframe. Emergency maintenance will be coordinated with the County, City, and 911 District to minimize operational impact.
- Risk Management: A detailed assessment to identify potential risks associated with the maintenance activity and strategies to mitigate them.
- Contingency Plan: A rollback or recovery process to ensure system stability and continuity in case maintenance activities result in unforeseen issues.
- Communication and Documentation: Maintenance activities will be documented and communicated regarding any Software changes.
- Approval: Maintenance plans must receive prior approval from designated County, City, and 911 District staff to ensure alignment with operational requirements.

4. Infrastructure Systems

4.1 Responsibilities

The 911 District shall serve as the primary infrastructure provider for the Software, ensuring system performance, security, and scalability. This responsibility shall be made in accordance with the Master Terms and Conditions of the vendor, vendor-provided supported environments and relevant infrastructure compatibility matrixes and includes:

- Hardware Specifications: Defining and maintaining minimum hardware requirements to support reliable operation and scalability of the Software
- Network Connectivity: Ensuring robust, secure, and redundant network connections to support system accessibility for all participating agencies.
- Server Infrastructure: Provisioning and maintaining server environments, including virtual or cloud-based solutions, to host the Software and associated applications.
- System Security: Implementing and maintaining comprehensive security protocols, including firewalls, encryption, access control, and regular vulnerability assessments, in compliance with federal, state, and local regulations.
- Infrastructure environment: Ensuring a stable and resilient infrastructure environment to meet operational demands and support high availability.
- Operating System Maintenance: Maintaining operating systems at supported and secure versions and adhering to version limitations to ensure compatibility and vendor support.
- Application Access: Provide secure application access for external agencies including configuration and management of access credentials and role-based permissions

5. Database Management & Support

5.1 Data Ownership

The County, the City, and all participating agencies shall retain ownership of their respective data within

the Software. This ownership includes control over how the data is used, accessed, and shared, in compliance with applicable laws and policies.

5.2 Database Management

The 911 District shall serve as the central repository and be responsible for the overall management and maintenance of the database to ensure system reliability and security, including:

- Data Backups: Regularly scheduled backups to ensure data can be restored in case of an issue.
- Data Integrity checks: Periodic verification and validation of data to ensure accuracy and consistency.
- Database Updates and Maintenance: Ensuring the database remains on supported and secure versions and applying updates to address bugs and vulnerabilities.
- Performance Monitoring and Tuning: Monitoring database and application performance, and optimizing system performance as needed
- Capacity Planning: Anticipating and planning for future storage and capacity requirements
- Database Audits and Improvements: Performing regular audits to identify areas for improvement, optimize processes, and ensure compliance with operational standards

5.3 Database Support

As the steward of the Software, the 911 District shall oversee all database support issues, acting as the central point of contact for database-related concerns. The 911 District shall

- Ensure timely communication with the County and the City regarding database issues or updates
- Resolve database problems promptly and minimize system downtime
- Coordinate with third-party vendors for advanced support when required

5.4 Repository Responsibilities

As the repository, the 911 District shall:

- Maintain secure, centralized storage of the database and associated backups.
- Provide controlled access to authorized stakeholders for data extracts and reporting needs, in alignment with data ownership rights.
- Ensure compliance with applicable data governance, security, and retention policies.

5.5 Access Control

The 911 District shall implement and maintain robust access control measures to ensure the security and integrity of the database. These measures include:

- Granting access based on roles and responsibilities, in alignment with operational needs and security protocols.
- Establishing a request process for data extracts, reporting needs, or additional database access, requiring approval by the appropriate stakeholders.
- Periodically reviewing and auditing database access permissions to ensure compliance with data governance policies and to prevent unauthorized access.

5.6 Data Retention Policy

The 911 District shall adhere to a defined retention policy for database backups and historical data, ensuring compliance with legal, regulatory, and operational requirements. This includes:

- Maintaining routine backups for a specified retention period (e.g., daily, weekly, or monthly, depending on operational needs).
- Retaining historical data required for auditing, reporting, or compliance purposes for the agreed-upon duration.
- Implementing secure deletion processes for purging expired backups or data that is no longer needed, ensuring it is permanently and irretrievably removed.

5.7 Disaster Recovery

The 911 District shall develop and maintain a disaster recovery plan to ensure database availability and business continuity in the event of a system failure or disaster. This includes:

- Regularly testing backup restoration processes to confirm data can be recovered successfully.
- Establishing procedures for failover and recovery to minimize system downtime during emergencies.
- Documenting and communicating the disaster recovery plan to stakeholders, including the County and City, to ensure alignment and readiness.

6. Cybersecurity Requirements

6.1 Compliance

The 911 District shall comply with all applicable federal, state, and local cybersecurity laws, regulations, and standards with particular emphasis on adhering to the current version of the CJIS Security Policy to protect the integrity, confidentiality, and availability of system data. Each participating agency agrees to:

- Develop, implement, and maintain policies, procedures, and training to their personnel regarding the proper use of shared information, including shared tables or any data specifically set up in the system for collaborative use.
- Utilize security devices, technologies, and procedures to prevent unauthorized access to the system and its information.
- Prohibit its employees from attempting to circumvent security controls, devices, or procedures.
- Limit access to security-related system information to personnel with the need-to-know for the performance of their duties under this agreement.
- Make written policies governing employee cybersecurity responsibilities available for review by other participating agencies.

The parties further agree to comply with applicable local, state, and federal laws, rules, and regulations relating to data privacy or confidentiality for the Software. Nothing in this agreement shall restrict or impact the ability of any party to conduct appropriate criminal investigations into misuse of the system or the information contained in the system.

6.2 Security Protocols

The 911 District shall implement and maintain security measures that meet applicable compliance requirements, ensuring the integrity, confidentiality, and availability of the system and its data. Security measures include but are not limited to:

- Firewalls: robust firewalls to protect the system against unauthorized access and external threats.
- Encryption of data: ensuring all data, both at rest and in transit, is encrypted using industry-standard protocols (e.g., AES-256, TLS).
- Regular security audits: conducting periodic internal and external security audits to identify vulnerabilities and ensure compliance with relevant standards.
- Access Control and Authentication: verifying CJIS training, the existence of multi-factor authentication for all user access points; establishing role-based access to ensure users have access only to the data and functions necessary for their role
- Patch Management: Ensuring timely application of updates and security patches to address vulnerabilities in software, operating systems, and hardware.
- Intrusion Detection and Prevention Systems (IDS/IPS): Monitoring for and responding to unauthorized access attempts or network anomalies in real-time.
- Security Monitoring: Continuous monitoring of system logs, user activities, and network traffic to detect and mitigate potential threats.
- Incident Response Plan: Establishing and maintaining a documented incident response plan, including procedures for identifying, reporting, and mitigating security incidents.
- Backup and Disaster Recovery: Ensuring secure, regular backups of critical data, to include VMs, and maintaining a disaster recovery plan to ensure continuity of operations in the event of a breach or failure.
- Vendor and Third-Party Security Compliance: Requiring third-party vendors and partners to adhere to strict cybersecurity standards and conducting regular compliance reviews.

6.3 Incident Response

In the event of a cybersecurity incident, the 911 District shall:

1. **Initial Notification:**

- Notify the County and the City within four (4) hours of discovering the incident
- Prioritize required notifications to appropriate federal, state, and local entities including the FBI, DPS, CISA, and applicable insuring entities, as dictated by the nature and scope of the incident

2. **Incident Response Activation:** Immediately activate its incident response plan, which will outline clear roles, responsibilities, and actions for addressing the incident
3. **Policies and Procedures:** Maintain up-to-date policies and procedures for the effective management of cybersecurity incidents
4. **Communication and Updates:** Provide timely updates to the County and City as the investigation progresses, including details on containment efforts, potential impacts, and estimated resolution timelines.
5. **Collaboration:** Cooperate fully with law enforcement, regulatory agencies, and other stakeholders as required, providing necessary data and access to facilitate investigations.

6.4 Security Breach Notification

In the event the 911 District becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access that compromises or is suspected to compromise the security, availability, confidentiality, or integrity of County and City data or related safeguards required under this agreement, the 911 District shall:

1. **Immediate Notification:** Notify the County's and City's Chief Information Security Officer and/or designated security communication channel within 24 hours of discovering the potential or actual breach
2. **Root Cause Analysis:** Conduct a root cause analysis to identify the actual, potential, or suspected source and nature of the breach
3. **Remediation Plan:** Develop and submit a remediation plan that is acceptable to the County and City within 30 days of verified breach. The plan will address the breach, its impact, and measures to prevent any future occurrences

7. Disaster Recovery Requirements

7.1 Recovery Plan

The 911 District shall develop, implement, and maintain a disaster recovery plan and business continuity plan that integrates the RMS system alongside other critical infrastructure. These plans will ensure the rapid recovery and continuity of operations in the event of a disaster or significant disruption. Key elements include:

1. **Data recovery processes**

- Documented procedures for restoring data to ensure the integrity, availability, and confidentiality of information following an incident.
- Verification of data recovery through periodic testing of backup restorations.

2. **Backup schedules**

- Regularly scheduled backups, including full, incremental, and differential backups, as appropriate for the system's needs.
- Ensure the secure storage of backups in geographically dispersed locations, adhering to the 'Rule of Three'—maintaining at least three copies of data across two different storage media, with one copy kept off-site—to prevent single points of failure.

3. **Responsibilities for the County and the City:**

- Clearly defined roles and responsibilities for County and City personnel in supporting disaster recovery and business continuity efforts.
- Collaborative procedures for ensuring agency-specific needs are addressed during recovery operations.

4. **Communication Protocols:**

- Establishing communication channels and notification procedures for all stakeholders, including the County, City, and relevant external entities.
- Ensuring timely updates throughout the recovery process to maintain transparency and coordination.

5. **Testing and Validation:**
   - Regular testing and updating of the DRP and BCP to validate effectiveness and alignment with operational requirements.
   - Incorporating lessons learned from drills, exercises, or actual incidents to enhance recovery capabilities.

6. **Compliance and Documentation:**
   - Adherence to applicable local, state, and federal regulations governing disaster recovery and continuity planning.
   - Maintenance of comprehensive documentation for all recovery processes, schedules, and roles to facilitate audits and reviews.

8. Testing

Disaster recovery procedures will be exercised regularly to ensure effectiveness and familiarity among the County, the City, and the 911 District.

9. Migration and Costs

9.1 Migration Responsibilities

The County and the City agree to cooperate in the data migration process to the 911 District site, ensuring minimal disruption to services. The 911 District will be responsible for installing the latest Software, (i.e., upgrade, patch, release). The 911 District shall provide a cutover plan to encompass the following: getting full backup of production database from the County; installing full backup of production database; notifications to City, County, and external agencies; downtime expected; data verification from City, County and external agencies; interface testing; Software cutover to 911 District. End-users will connect to the Software through existing City, County, & 911 District networks and provide a unified remote platform for external agencies

The 911 District shall ensure that all agencies will maintain their current access to the Software. The 911 District shall develop policies and procedures, subject to the approval of the County and the City, for agencies operating within the jurisdictional limits of El Paso County to gain access to the Software, modify their access to the Software, or have their access to the Software removed.

9.2 System Cost Sharing

The 911 District shall assume all the costs associated with the hosting of the Software. The costs associated with the Software maintenance and support billed annually by Hexagon and dictated by the executed contract with the vendor will be assumed by the 911 District. The 911 District will bill the County and the City annually, who shall reimburse the 911 District at the following percentages.

- The County: 50%
- The City: 50%

9.3 Hexagon RMS Software Maintenance & Support Changes

The 911 District shall not execute or amend the contract with the software vendor unless agreed upon in writing by the County and the City. Both the County and City must be included in any negotiation impacting service to the Software or changes in cost.

9.4 Resource Reimbursement

The 911 District shall employ two (2) full-time employees dedicated to the management of the system. The costs associated with these two employees will be assumed by the 911 District; however, the 911 District will bill the County and the City annually, who shall reimburse the 911 District at the following percentages.

- The County: 50%
- The City: 50%

The costs of the two (2) full-time employees reimbursed by the County and the City shall not exceed a total cost of $220,000.00. However, to ensure the continued ability to attract and retain qualified personnel, salaries may require adjustments in response to future market conditions. Any proposed salary modifications will be jointly evaluated, and agreed to in writing, with a minimum of 6 months' notice from the end of the current fiscal year of the County & City to allow for proper inclusion in the respective fiscal budgets.

10. Payment Terms

The 911 District shall bill the County and the City annually for their respective share of utilization costs outlined in sections 9.2, 9.3 & 9.4.

11. Termination

11.1 Termination Rights

This agreement commences upon approval by the governing bodies of the parties and shall continue until terminated by any party under the provisions of this agreement or until the parties mutually agree to terminate this agreement for the reason that the Software will be replaced with new technology. A party may terminate this agreement for convenience by giving the other parties twelve months (12) months written notice under the terms outlined in paragraph 11.2 or 11.3 below. Any notices required to be sent to a party of the agreement shall be deemed received five (5) days after deposit in the United States Mail, or on the date of hand delivery, to the following addresses:

CITY:	City of El Paso Office of the Mayor 300 N. Campbell El Paso Texas 79901-1402
With a copy to:	El Paso Police Dept. Office of the Chief of Police 911 N. Raynor El Paso, Texas 79903

COUNTY:	County of El Paso Office of the County Judge Room 301, County Courthouse 500 E. San Antonio El Paso, Texas 79901
With a copy to:	El Paso County Sheriff's Office Office of the Sheriff 3850 Justice Drive El Paso, Texas 79938
911 District:	El Paso County 911 District 6055 Threadgill Ave. El Paso, Texas 79924

11.2 If on or after the date that the system is fully operational, any of the parties to this agreement shall fail to fulfill its obligations under this agreement properly and timely, or if any of the parties violate any of the covenants, agreements, or stipulations of this agreement, thereupon any non-breaching party shall have the right to terminate this agreement if the breaching party has not cured the default within 90 days after receiving written notice. The parties' failure to insist upon strict performance of any covenant, agreement, or stipulation of the agreement or to exercise any right herein contained shall not be a waiver or relinquishment of such covenant, agreement, stipulation, or right, unless the parties consent thereto in writing. Any such written consent shall not constitute a waiver or relinquishment in the future of such covenant, agreement, stipulation or right.

11.3 In the event of widespread or consistent pattern of violation in the manner in which the system is used, including the abuse or disregard of operational policies, after the date the system becomes fully operational, by any participating agency that results in the improper release or use of the data of a party, or which impedes the effective use of the Software, the affected party may send notice to the other party of the alleged violation and request that the violation be cured in 30 days. Such written notice shall contain specific information of the alleged violation and a detailed explanation of the detrimental effect of such violation. In the event that the other party fails to cure the violation to the detriment of the affected party or take steps to prevent future improper release or use of the data of the affected party, the affected party may terminate this agreement upon giving 120 days written notice to the other parties.

11.4 In the event of termination of this Agreement, the 911 District shall provide reasonable assistance to ensure a smooth transition of all services, data, and systems back to the County/City or its designated representative. The 911 District agrees to extend the transition period beyond the 120-day period outlined in this Agreement, if necessary, to facilitate the successful migration of all relevant materials, services, and information. The duration of this extended transition period shall be mutually agreed upon by the parties in writing, taking into consideration the complexity and scope of the services being transitioned.

12. Incident Reporting

- Any incidents, other than those governed by sections 6.3 and 6.4, affecting the Software or its functionality must be reported to the County and the City within one (1) day of occurrence.
- Reports should include details such as the nature of the incident, affected users, and any error messages received.

13. Data Backup Frequency

Implementing a robust data backup strategy is crucial for maintaining the integrity and availability of systems. To enhance our current practices, the 911 District will adhere to the following protocol and incorporate vendor-specific recommendations and best practices to ensure optimal performance:

- Full data backups: shall occur every twenty-four (24) hours to ensure data integrity and availability.
- Data backups retention will be as follows:
    - Daily backups: retained for one week
    - Weekly backups: retained for eight weeks
    - Monthly backups: retained for three months
- Data backups will be tested regularly to ensure functionality and reliability

14. Monitoring and Reporting

14.1 Monitoring

The Software shall be monitored using advanced tools to track uptime, response times, and overall system performance. The 911 District shall ensure proactive performance management to maintain optimal functionality and reliability of the system.

14.2 Performance Reporting

The 911 District is committed to transparency and collaboration with the County and the City. Upon request, the District shall provide performance reports summarizing relevant metrics, including uptime statistics, response times for support requests, resolved issues, and any incidents or outages with actions taken. This approach ensures that the County and the City have access to necessary information without duplicating efforts or creating unnecessary administrative burdens.

15. Escalation Procedures

15.1 Escalation Levels

To ensure timely resolution of issues, escalation procedures shall apply equally to the County, City, and the 911 District. These procedures define a structured approach to addressing unresolved issues within the designated response times.

- Level 1: Support staff within the primary support teams of the 911 District, County, or City depending on where the issue originates
- Level 2: Heads of Information Technology Department or equivalent for the 911 District, the County, and the City, ensuring collaborative engagement across stakeholders
- Level 3: Designated Executive Liaisons from the 911 District, County, and City providing oversight and decision-making at the leadership level

16. Service Level Agreement (SLA) Measures

The 911 District is committed to delivering reliable, high-quality service and continuously striving for excellence in system performance, availability, and support. The following SLA measures outline our approach to ensuring the continued success of the Software and its users.

16.1. Performance Metrics

16.1.1 Uptime and Availability

Target Uptime: The 911 District aims to maintain 99.9% availability for the Software, excluding scheduled maintenance, to ensure uninterrupted access for all participating agencies.

16.1.2 Response Time for Support Requests

To uphold operational efficiency and proactive issue resolution, the 911 District strives to meet the following response times for Tier 2 Support, which handles escalated technical issues, system configurations, and vendor coordination:

- Critical Issues: Response within one (1) hour – Issues that prevent Software use entirely, such as system crashes or data loss.
- High Priority Issues: Response within four (4) hours – Significant disruptions affecting key functionalities or workflows.
- Medium Priority Issues: Response within one (1) business day – Non-critical issues that impact specific features but allow continued operation.
- Low Priority Issues: Response within three (3) business days – Minor errors with minimal operational impact that can be addressed in routine updates.

17. Commitment to Service Excellence

The 911 District remains dedicated to continuous improvement and responsiveness in its operations. In partnership with the governing Board of Managers, which includes representatives from the City and County, we ensure transparency, collaboration, and shared accountability in upholding system performance **17.1 Service Disruption Notifications**

In the event of an unexpected service disruption, the 911 District shall:

- Provide a detailed report outlining the issue, resolution steps, and any preventive measures taken.

- Engage with County and City stakeholders within two business days to discuss the incident, gather feedback, and reinforce strategies for continued service reliability.

17.2 Continuous Improvement Plan

If performance metrics indicate opportunities for enhancement, the 911 District shall proactively implement a structured improvement plan, which may include:

- Ongoing training for support staff to enhance troubleshooting and response efficiency.
- Strategic infrastructure upgrades to strengthen system resilience and performance.
- Collaboration with the Board of Managers to align on priorities, address concerns, and leverage resources for sustained service excellence.

The 911 District values its role as a trusted technology partner and remains dedicated to delivering a secure, efficient, and high-performing system for all agencies it serves.

18. Review and Revision

18.1 SLA Review

The SLA measures may be reviewed upon request by the County, City, and 911 District.

18.2 Adjustments

The County, City, and 911 District will document and mutually agree upon any necessary adjustments to the SLA measures.

LAW ENFORCEMENT INFORMATION SHARING

MUTUAL SUPPORT SERVICES

Dated this _____ day of _____, 2025.

THE CITY OF EL PASO

_____
Renard U. Johnson
Mayor

ATTEST:

_____
Laura D. Prine
City Clerk

APPROVED AS TO CONTENT:

_____
Chief of Police
El Paso Police Department

APPROVED AS TO FORM:
Robert Aguinaga Jr
~~City Attorney's~~ Office

LAW ENFORCEMENT INFORMATION SHARING

MUTUAL SUPPORT SERVICES

Dated this _____ day of _____, 2025.

COUNTY OF EL PASO

_____
County Judge

ATTEST:

_____
County Clerk

APPROVED AS TO FORM:

_____
County Attorney's Office

APPROVED AS TO CONTENT:

_____
Sheriff
El Paso County Sheriff's Office

LAW ENFORCEMENT INFORMATION SHARING

MUTUAL SUPPORT SERVICES

Dated this 30th day of July, 2025.

El Paso 911 District

Scott Calderwood
Executive Director, El Paso 911 District

Kristian Menendez
Board Chair