**Security Plan for Electronic Incident Management Software**

**Prepared for:** San Diego Convention Center Corporation  
**RFP #25-1063**

**1. Introduction**

This **Security Plan** outlines the technical and administrative safeguards for the **Electronic Incident Management Software** to ensure confidentiality, integrity, and availability of data, as required in **Section 2 (Scope of Work)** of RFP #25-1063. The plan complies with **SSAE 16 SOC 2 Type II**, **ISO/IEC 27001**, and **Azure AD** integration standards.

**2. Data Security & Encryption**

**A. Data Encryption**

| **Data State** | **Encryption Protocol** | **Key Management** |
| --- | --- | --- |
| **Data in Transit** | TLS 1.2+ (HTTPS) | Certificate Authority (e.g., DigiCert) |
| **Data at Rest** | AES-256 | AWS KMS / Azure Key Vault |
| **Database Fields** | Column-level encryption (PII) | Role-based key access |

**B. Backup Encryption**

* All backups encrypted with **AES-256**.
* Keys stored in **hardware security modules (HSMs)**.

**3. Access Controls**

**A. Authentication**

* **Single Sign-On (SSO):** Azure Active Directory integration.
* **Multi-Factor Authentication (MFA):** Required for all admin accounts.

**B. Authorization (RBAC)**

| **Role** | **Permissions** |
| --- | --- |
| **Public Safety Admin** | Full access to incident reports, dispatch queue, analytics. |
| **Field Staff** | Submit incident reports, attach media, view assigned tasks. |
| **Auditor** | Read-only access to logs and reports. |

**C. Session Management**

* **Timeout:** 59 minutes of inactivity.

**4. Network & Infrastructure Security**

**A. Hosting Environment**

* **Cloud Provider:** Azure (SOC 2, ISO 27001 certified).
* **Data Sovereignty:** Hosted in **North America** with logical separation.

**B. Network Protections**

* **Firewalls:** Web Application Firewall (WAF) for SQL injection/XSS prevention.
* **VPN Access:** Required for remote administration.

**C. Intrusion Detection & Monitoring**

* **SIEM Tools:** Splunk or Azure Sentinel for real-time alerts.
* **Log Retention:** 1 year (audit logs, access attempts).

**5. Certifications & Compliance**

| **Requirement** | **Compliance Status** |
| --- | --- |
| **SSAE 16 SOC 2 Type II** | Annual audit reports available. |
| **ISO/IEC 27001** | Certified; documentation on request. |
| **GDPR/CCPA** | Data subject request (DSR) process in place. |
| **NIST SP 800-53** | Controls mapped to NIST framework. |

**6. Incident Response**

**A. Breach Protocol**

1. **Detection:** SIEM alerts on anomalous activity.
2. **Containment:** Isolate affected systems.
3. **Eradication:** Patch vulnerabilities, reset credentials.
4. **Recovery:** Restore from clean backups.
5. **Reporting:** Notify Convention Center within **1 hour** of confirmed breach.

**B. Penetration Testing**

* **Frequency:** Quarterly (external) + annual internal audits.
* **Vendor:** Independent third-party (e.g., Qualys, Rapid7).

**7. Physical Security**

* **Data Centers:** Biometric access, 24/7 surveillance.
* **Device Policies:** Full-disk encryption for laptops/USBs.

**8. Vendor Security Obligations**

* Subcontractors must adhere to this Security Plan.
* Annual security training for all personnel.

**9. Documentation & Audits**

* **SOC 2 Reports:** Provided to Convention Center annually.
* **Vulnerability Scans:** Shared quarterly.

**Appendix A: Encryption Certificates**

* SSL Certificate: [Issuer] (Expires: [Date]).
* Key Vault Audit Logs: Retained for 3 years.

**Appendix B: Access Control Matrix**

| **User Type** | **Allowed Actions** |
| --- | --- |
| Admin | Create/delete users, modify system settings. |
| Field Officer | File reports, upload photos, view assignments. |

**Prepared by:** CHABEZTECH LLC  
**Date:** [Submission Date]

**Note:** Aligns with RFP requirements for **"Security Plan detailing encryption, access controls, and certifications."** Updates required for infrastructure changes.