**Disaster Recovery Plan (DRP) for Electronic Incident Management Software**

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

**1. Introduction**

This **Disaster Recovery Plan (DRP)** outlines the procedures to ensure the **Electronic Incident Management Software** remains operational during and after a disaster, including data breaches, system failures, or natural disasters. The plan complies with **SSAE 16 SOC 2 Type II** and **ISO/IEC 27001** security standards as required in the RFP.

**Objectives:**

* Ensure **minimal downtime** (<4 hours Recovery Time Objective, RTO).
* Prevent **data loss** (<1 hour Recovery Point Objective, RPO).
* Maintain **business continuity** during emergencies.

**2. Disaster Scenarios & Mitigation**

| **Disaster Scenario** | **Mitigation Strategy** |
| --- | --- |
| **Server/Data Center Failure** | Automatic failover to a geographically redundant backup site. |
| **Cyberattack (Ransomware/Data Breach)** | Isolate affected systems, restore from clean backups, and activate incident response team. |
| **Natural Disaster (Earthquake, Flood)** | Switch to cloud-based disaster recovery (DR) environment hosted in a separate region. |
| **Human Error (Data Deletion/Corruption)** | Daily backups with 60-day retention for rollback. |

**3. Recovery Procedures**

**A. Data Backup & Restoration**

* **Backup Frequency:**
  + **Real-time replication** of critical databases.
  + **Daily incremental backups** (encrypted, stored off-site).
* **Backup Locations:**
  + Primary: Secure cloud storage (Azure) in North America.
  + Secondary: Physically separate disaster recovery site.
* **Restoration Process:**
  + **Automated scripts** to redeploy databases and configurations.
  + **Manual verification** of data integrity post-restore.

**B. System Failover & Redundancy**

* **High Availability (HA) Setup:**
  + Load-balanced servers with **auto-failover**.
* **Disaster Recovery Site:**
  + Tested every **quarter** to ensure functionality.

**C. Incident Response & Communication**

1. **Detection & Alerting:**
   * **24/7 monitoring** (Azure Alerts).
   * Automated alerts sent to **IT team & Convention Center contacts**.
2. **Declaring a Disaster:**
   * If downtime exceeds **60 minutes**, DRP is activated.
3. **Communication Plan:**
   * **Primary Contact:** Vendor’s DR team lead.
   * **Secondary Contact:** Convention Center IT liaison.
   * **Stakeholder Updates:** Hourly status reports via email/SMS.

**4. Roles & Responsibilities**

| **Role** | **Responsibility** |
| --- | --- |
| **DR Team Lead** | Oversees recovery execution, coordinates with Convention Center. |
| **Systems Admin** | Restores servers, databases, and applications. |
| **Security Team** | Investigates breaches, ensures compliance. |
| **Vendor Support** | Provides emergency patches/updates. |
| **Convention Center IT** | Validates system functionality post-recovery. |

**5. Testing & Maintenance**

* **Quarterly DR Drills:** Simulated failover tests.
* **Annual Full-Scale Test:** Restores the entire system from backups.
* **Post-Recovery Review:** Documents lessons learned.

**6. Compliance & Reporting**

* **Audit Logs:** All recovery actions recorded for compliance.
* **RTO/RPO Metrics:** Reported annually to the Convention Center.

**Appendix A: Contact List**

| **Role** | **Name** | **Phone** | **Email** |
| --- | --- | --- | --- |
| Vendor DR Lead | [Name] | [Phone] | [Email] |
| Convention Center IT | [Name] | [Phone] | [Email] |

**Appendix B: Backup & Recovery Timeline**

| **Activity** | **Time to Execute** |
| --- | --- |
| Failover to DR Site | <30 minutes |
| Full Data Restoration | <4 hours |
| System Validation | <1 hour |

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

**Note:** This plan aligns with **Section 2 (Scope of Work)** and **Section 3 (Bid Form)** of RFP #25-1063. Vendor will provide updates if infrastructure changes affect recovery protocols.