Version: 1.0

Enterprise Information Security & Privacy Policy Manual

Effective Date: January 2026

1. Information Security & Access Control Policy

- **Purpose:** To protect the confidentiality, integrity, and availability of system assets, legal case files, and client data.
- **Data Classification:** All data containing Workers' Compensation claims, Protected Health Information (PHI), or Personally Identifiable Information (PII) is classified as **Restricted / Confidential**.
- **Access Control (Least Privilege):** Access to EAMS processing databases, source code, and server environments is restricted solely to authorized engineering personnel who require access to perform their specific job duties.
- **Account Management:** User accounts are uniquely assigned to individuals. Generic or shared administrative accounts are strictly prohibited. Accounts are immediately disabled upon employee termination.
- **Multi-Factor Authentication (MFA):** MFA is strictly required for all users accessing the platform.

2. Password & Authentication Policy

- **Complexity Requirements:** All system and administrative passwords must meet the following minimum thresholds:
    - Minimum length of eight (8) characters.
    - Must contain at least one uppercase letter, one lowercase letter, one number, and one special character.
- **Password Expiry & Reuse:** Administrative passwords must be rotated at least once every 60 days. The system prevents the reuse of the last 5 historical passwords.

- **Account Lockout:** Accounts are automatically locked out for a period of 30 minutes after five (5) consecutive failed login attempts to prevent brute-force attacks.

3. Technical Data Protection & Encryption Policy

- **Encryption in Transit:** All external network traffic entering or leaving the application environment must be encrypted using Transport Layer Security (TLS) 1.2 or higher. Unencrypted HTTP traffic is automatically forced and redirected to HTTPS.
- **Encryption at Rest:** All data files stored within production environment must be encrypted using Advanced Encryption Standard (AES) with a key length of 256 bits.
- **Logging & Monitoring:** Application logs are captured continuously. Logs record login successes/failures, data modifications, and administrative changes. Logs are stored securely with restricted access and retained for a minimum of one (1) year.
- **Software Supply Chain Security (SBOM)**
  The company maintains a dynamic Software Bill of Materials (SBOM) for the application. All third-party libraries, dependencies, framework packages, and open-source components are inventoried, monitored for known CVEs (Common Vulnerabilities and Exposures), and updated during regularly scheduled patch cycles.
- **Session Security & Endpoint Access**
  All administrative and user web sessions automatically terminate following sixty (60) minutes of inactivity. Administrative access to backend management services is restricted through a secret key, and local remote-access software on employee endpoints is strictly monitored to prevent unauthorized session hijacking

4. Incident Response Policy

- **Incident Identification:** A security incident is defined as any suspected or confirmed unauthorized access, data exposure, disruption, or policy violation affecting the production environment.
- **Response Team:** The designated Incident Response Lead is:

  Daniel Lopez**,** CEO Lopez & Associates
  Khalid Mahmood**,** Chief Technology Architect

- **Containment & Mitigation:** Upon discovery, the affected system components will be isolated (e.g., stopping application pools, modifying firewall rules, revoking credentials) to prevent further exposure while maintaining data integrity.
- **Notification Window (HIPAA Compliance):** In the event of a confirmed breach involving unencrypted PHI, we will notify affected covered entities without unreasonable delay and strictly within twenty-four (24) to forty-eight (48) hours of confirmation, assisting fully with necessary HIPAA Breach Notification reporting.

5. Backup, Disaster Recovery & Data Retention Policy

- **Backup Schedule:** Automated full backups of the production environment are performed three (3) times daily.
- **Backup Encryption & Storage:** Backups are encrypted at rest using AES-256 and stored in a geographically redundant, secure environment isolated from the main production app servers.
- **Disaster Recovery (RTO / RPO):**
    - **Recovery Point Objective (RPO):** Maximum target data loss is limited to four (4) hours.
    - **Recovery Time Objective (RTO):** Target time to restore service following a catastrophic outage is twenty-four (24) hours.
- **Data Retention & Disposal:** Active client data is retained for the duration of the active service agreement unless legally required otherwise.
- **Statutory Claims Logs & EAMS Staging**
  While data is securely deleted or anonymized upon contract termination, the system retains immutable transmission logs, JET File transaction receipt numbers, and regulatory submission status codes for the legally mandated statutory period required for workers' compensation system auditing. Any interface files, flat files, or raw XML objects generated dynamically for submission to the California DWC EAMS portal are securely purged from intermediate server directories immediately upon verified transmission confirmation.

6. Corporate Compliance & Employee Security

- **Confidentiality Agreements:** All employees and independent contractors are required to sign a binding Non-Disclosure Agreement (NDA) and Confidentiality Agreement prior to gaining system access.
- **Security Awareness Training:** All personnel undergo mandatory Security Awareness and HIPAA Compliance training upon hire and annually thereafter. Training covers phishing identification, password hygiene, and clean desk practices.
- **Subcontractor Management:** Any third-party subcontractor or downstream utility touching PHI must sign a formal Business Associate Agreement (BAA) verifying compliance with identical technical safeguards.