

Forensic Audit & Record Governance Report: 2026 Compliance Architecture for Sapphos Environmental

1. Executive Legal Overview: The 2026 Regulatory Paradigm

The governance of personnel records and forensic compliance for professional services firms in California is undergoing a fundamental paradigm shift effective January 1, 2026. For Sapphos Environmental, a firm operating at the volatile intersection of highly regulated environmental consulting (CEQA/NEPA) and stringent California employment mandates, the definition of "Good Order" has evolved from simple administrative file maintenance to a complex system of forensic metadata retention, statutory data siloing, and criminal-level custodial responsibility. This report establishes the foundational governance architecture required to withstand the scrutiny of a forensic audit, legal discovery during CEQA litigation, and the enforcement mechanisms of the California Department of Justice (DOJ) and the Department of Industrial Relations (DIR).

The 2026 compliance cycle introduces a trifecta of stringent mandates—SB 513, SB 294, and AB 692—that fundamentally alter how employee data is created, stored, and protected. These state-level requirements are further compounded by the localized wage and hour ordinances of Pasadena, specifically Pasadena Municipal Code (PMC) 4.65, and the overarching federal and state requirements for handling Criminal Offender Record Information (CORI).

1.1 The Forensic Standard of "Good Order"

In the context of this audit and the proposed governance architecture, "Good Order" is defined not merely by the presence of a document but by its *defensibility* and *metadata integrity*. A record is only in Good Order if it meets the specific metadata requirements of the new statutes (e.g., SB 513's requirement for logging specific "equipment or software skills"), adheres to the strict segregation protocols of SB 464 and the Americans with Disabilities Act (ADA), and is under the custodial control of a legally vetted authority. The failure to maintain this standard exposes the firm to cumulative penalties that can exceed \$10,000 per employee for specific violations, alongside the existential risk of having environmental documents invalidated in court due to attacks on the credibility or qualifications of the workforce.

For a firm like Sapphos Environmental, which relies on the specialized credentials of archaeologists, biologists, and geologists, the personnel file is the evidentiary foundation of the firm's work product. In CEQA litigation, opposing counsel frequently target the administrative record, seeking to undermine the technical studies by questioning the qualifications of the preparers. If the training logs for a Qualified SWPPP Developer (QSD) are incomplete under the new SB 513 standards, or if the professional licensing records for a Professional Geologist (PG) are not forensically verifiable, the technical validity of an Environmental Impact Report (EIR) can be successfully challenged. Therefore, record governance is not just an HR function; it is a risk

management function critical to the firm's revenue and reputation.

The architecture proposed herein moves Sapphos Environmental from a reactive posture to a "Forensic Readiness" state. This ensures that every personnel file—from the entry-level field technician to the Principal Associate—serves as a verified evidentiary object capable of proving compliance with wage laws, training mandates, and professional licensing requirements.

1.2 The Pasadena Context and Local Preemption

While California state law provides the baseline for compliance, the firm's physical location in Pasadena introduces specific regulatory overrides that must be integrated into the governance logic. The Pasadena Minimum Wage Ordinance (PMC 4.65) dictates a baseline wage of \$18.04 per hour for the 2025-2026 cycle. This local ordinance interacts complexly with the new state-level prohibitions on contract retentions under AB 692. The governance structure must ensure that payroll and contract records not only reflect the higher local wage but also strip out any now-illegal "stay-or-pay" provisions that might have historically been used to recoup training costs for high-value certifications like the QSP/QSD or Professional Geologist (PG) licenses. The interplay between local and state law creates a "highest standard" compliance environment. Where Pasadena law is more protective (e.g., wage rates), it controls. Where state law imposes stricter prohibitions (e.g., AB 692's ban on training repayment agreements), it controls. The governance architecture must be sophisticated enough to apply these rules simultaneously without conflict.

2. The Custodian of Records (COR): Statutory Authority and Mandate

The linchpin of the 2026 record governance architecture is the designated Custodian of Records (COR). Under the new scrutiny of the 2026 cycle, the COR is no longer a passive administrative title or a role that can be informally assigned to an Office Manager. It is a statutory officer with specific criminal liability, distinct confirmation requirements, and a direct reporting relationship to the California Department of Justice (DOJ).

2.1 Statutory Definition and Duties (Penal Code § 11102.2)

Pursuant to California Penal Code § 11102.2, the COR is defined as the individual designated by an agency or entity who is responsible for the "security, storage, dissemination, and destruction of the criminal records furnished to the agency" and serves as the primary contact for the Department of Justice. This role is critical for Sapphos Environmental because the firm's work likely involves access to sensitive site data, background checks for employees working on secure government contracts (e.g., military bases, critical infrastructure), or access to the California Law Enforcement Telecommunications System (CLETS) for specific project needs. The statute imposes a rigid framework for who may serve in this capacity. The COR is the ultimate gatekeeper. If the COR is compromised, or if the chain of custody for records is broken, the firm loses its ability to legally hold or process criminal history information (CORI), which is often a prerequisite for high-level environmental clearance work. The law treats the COR not merely as an employee of the firm but as a trusted agent of the state, responsible for upholding the integrity of the state's criminal record system within the private entity.

Core Statutory Duties:

1. **Security & Storage:** The COR must ensure that all sensitive records, particularly those containing CORI or sensitive medical data, are stored in physically secure locations (locked cabinets with controlled key access) or digitally encrypted environments that are distinct from general personnel files. This duty extends to the oversight of the "Data Silos" required by SB 464 and the ADA, ensuring that unauthorized personnel cannot bridge the gap between a general file and a protected file.
2. **Dissemination Control:** The COR carries the legal burden of ensuring that information is only released to individuals with a "Need-to-Know" and "Right-to-Know." The concept of "Right-to-Know" is statutory; mere curiosity or general managerial rank does not confer it. Unauthorized release of CORI is a misdemeanor under Penal Code § 11142. The COR must maintain an access log that details exactly who accessed a record, when, and for what purpose.
3. **Destruction Protocols:** The COR must oversee the secure destruction of records once their retention period expires or they are no longer needed. For CORI, this often means destruction immediately after the hiring decision is made, unless specific retention is authorized. The method of destruction must be definitive (e.g., cross-cut shredding or digital wiping) to ensure data cannot be reconstructed.
4. **DOJ Interface:** The COR serves as the sole liaison with the DOJ for confirmation, audits, and compliance reporting. If the DOJ audits the firm—a distinct possibility under the enhanced scrutiny of 2026—the COR is the individual who must answer for the firm's practices.

2.2 The DOJ Confirmation Process and Background Clearance

For the 2026 cycle, strict adherence to the DOJ confirmation process is mandatory. An individual cannot simply be "appointed" internally; they must be confirmed by the state. This process is designed to filter out individuals whose past conduct suggests a risk to the integrity of the records system. The DOJ has tightened these requirements to ensure that those guarding criminal records do not themselves have a history that compromises their reliability.

The Confirmation Workflow:

1. **Application Submission:** The agency (Sapphos Environmental) must submit the prospective COR for confirmation through the Applicant Agency Justice Connection (AAJC) Portal. This digital submission initiates the tracking process.
2. **Live Scan Fingerprinting:** The applicant must undergo a Live Scan fingerprinting process using the specific form BCIA 8016CUS ("Request for Live Scan Service - Custodian of Records"). This is distinct from a standard employment background check. The prints are retained by the DOJ for subsequent arrest notification, meaning the DOJ will actively notify the firm if the COR is arrested in the future. This "subsequent arrest notification" service ensures that the COR remains in good standing throughout their tenure.
3. **Form BCIA 8374:** The applicant must complete the "Custodian of Records Application for Confirmation" (Form BCIA 8374), attesting to their eligibility and understanding of the penalties for misuse. This form is a legal affidavit; any material misstatement is grounds for denial and potential criminal liability.
4. **Disqualification Criteria:** The DOJ will *not* confirm an applicant who has been convicted of a felony or any offense involving "moral turpitude, dishonesty, or fraud". This "moral turpitude" clause is broad and critical; it encompasses crimes that might not be felonies but speak to the individual's trustworthiness (e.g., petty theft, fraud, falsification of

documents). For a forensic auditor, verifying that the COR has not been disqualified is a primary check.

2.3 COR Job Description Deliverable

The following job description is designed to be inserted directly into Sapphos Environmental's HR governance documentation. It reflects the statutory weight of the role under 2026 laws and provides the necessary authority for the COR to enforce the RBAC protocols.

Job Description: Custodian of Records (COR) & Compliance Officer

Position Summary: The Custodian of Records (COR) acts as the statutory gatekeeper for Sapphos Environmental's sensitive personnel and forensic data. Operating under the mandate of California Penal Code § 11102.2, the COR is responsible for the governance, security, and lifecycle management of all physical and digital records. This role requires Department of Justice (DOJ) confirmation and serves as the primary defense against regulatory non-compliance, data breaches, and unauthorized dissemination of protected information. The COR is empowered to deny access to records to any individual, regardless of rank, who does not meet the statutory "Right-to-Know" criteria.

Statutory Authority:

- **Designation:** Officially designated under Penal Code § 11102.2(a)(1).
- **Licensure:** Must maintain active confirmation status with the California Department of Justice.
- **Reporting:** Reports operationally to the Principal/President but holds an independent statutory obligation to the DOJ regarding record security.

Core Responsibilities:

- **Forensic Record Governance:** Oversee the "Good Order" of all 47 employee personnel files, ensuring 100% compliance with SB 513 (Training Metadata), SB 464 (Demographic Siloing), and PMC 4.65 (Wage Records).
- **CORI Management:** Manage the intake, storage, and destruction of Criminal Offender Record Information (CORI). Maintain the "Need-to-Know" access log and enforce physical/digital segregation of CORI from general files.
- **Audit Readiness:** Conduct quarterly internal forensic audits of wage statements and training logs to ensure defensibility in CEQA litigation or DIR investigations.
- **Regulatory Interface:** Serve as the primary point of contact for the DOJ, DIR, and City of Pasadena regarding compliance inquiries.
- **Access Control Administration:** Administer the Role-Based Access Control (RBAC) system, granting and revoking privileges based on statutory clearance levels. Ensure that access permissions are immediately revoked upon employee termination.
- **Training Oversight:** Manage the execution of the Security Awareness Training schedule, ensuring all staff (including non-access staff) receive appropriate training levels (Level 1-4) as mandated by policy and statute.

Essential Requirements:

- **Background Clearance:** Must pass a DOJ/FBI fingerprint-based background check (Live Scan) via Form BCIA 8016CUS and be free of any felony convictions or crimes involving moral turpitude (PC § 11102.2(f)).
- **Certification:** Possession of, or ability to immediately obtain, DOJ COR Confirmation via Form BCIA 8374.

- **Knowledge:** Expert understanding of California Labor Code, Penal Code 11102.2, the California Public Records Act (CPRA), and the specific record-keeping requirements for CEQA administrative records (PRC § 21167.6).
- **Operational Capability:** Ability to manage physical key control systems and digital permission structures (e.g., Active Directory groups) to enforce data siloing.

3. Governance Architecture: Role-Based Access Control (RBAC)

To satisfy the "Data Siloing" constraints of SB 464 and the ADA, Sapphos Environmental must implement a rigid Role-Based Access Control (RBAC) matrix. The historical practice of a "general personnel file" accessible to all HR staff or senior management is obsolete and non-compliant. The 2026 mandates require the *physical and digital segregation* of data into distinct silos to prevent discriminatory bias (SB 464) and protect medical privacy (ADA/CMIA).

3.1 The Necessity of Segregation (SB 464 & ADA)

SB 464 (Demographic Siloing): Effective January 1, 2026, employers must collect and store demographic information (race, ethnicity, sex) for pay data reporting *separately* from the main personnel records. The legislative intent is to prevent this data from influencing employment decisions (hiring, promotion, discipline) by ensuring it is not visible to decision-makers during routine file reviews. If a manager reviewing a file for a promotion decision encounters a document explicitly listing the employee's race or ethnicity (collected for reporting purposes), a claim of bias becomes significantly harder to defend. The data must be "dark" to everyone except the COR and the specific HR analyst compiling the report.

ADA/CMIA (Medical Siloing): The Americans with Disabilities Act (ADA) and California's Confidentiality of Medical Information Act (CMIA) strictly require that medical information—including workers' compensation claims, disability accommodations, drug test results, and notes from interactive process meetings—be kept in separate, locked files distinct from the personnel file. This data must never be commingled with performance reviews or disciplinary records. For example, if an employee is disciplined for attendance issues, the disciplinary notice goes in the Personnel File. If the attendance issue was related to a medical condition discussed in an interactive process meeting, the notes from that meeting go in the Medical Silo. The manager issuing the discipline should not have access to the Medical Silo to "check the details" of the condition.

3.2 The "Need-to-Know" Framework

In a firm of 47 employees, role overlap is common. However, the RBAC matrix must enforce strict boundaries. The "Need-to-Know" principle implies that access is granted only to the extent necessary to perform a specific job function.

- **Finance/Payroll:** Needs access to tax forms, bank account numbers, and wage data (PMC 4.65 compliance). They do *not* need access to disciplinary history or medical records.
- **Executives:** Need access to performance reviews and qualifications (for project assignments). They generally do *not* need access to raw payroll data (unless approving budgets) and definitely do *not* need access to raw CORI or demographic data.

- **HR Director:** While having broad access, even the HR Director should be shielded from raw demographic data if they are involved in hiring/promotion decisions, to maintain the "blind" status intended by SB 464.

3.3 Deliverable: Role-Based Access Control (RBAC) Matrix

This matrix defines the "Need-to-Know" boundaries. It ensures that specific data types are siloed and only accessible to authorized roles.

Role / Authority Level	General Personnel File (Performance, Resumes, SB 513 Training Logs)	Medical/ADA Silo (Accommodations, Workers' Comp, Drug Tests)	Demographic/ Pay Data Silo (SB 464 Race/Ethnicity Data)	CORI/Background Silo (Live Scan Results, DOJ Notifications)	Financial/Payroll Silo (Wage Stmts, Tax Forms, Bank Info)
Custodian of Records (COR)	Full Access (Admin)	Auditor Access (Read-Only for Compliance)	Full Access (For Reporting)	Full Access (Gatekeeper)	Auditor Access
HR Director	Full Access	Full Access (Interactive Process Lead)	No Access (Blind to Bias Data)	Status Only (Pass/Fail)	Read/Write
Finance / Payroll Manager	Read-Only (Verification)	No Access	No Access	No Access	Full Access
Executive / Principal	Case-Specific Access (Performance Review Only)	No Access (Unless Essential for Safety)	No Access	No Access	Read-Only (Budgeting)
Direct Supervisor	Read-Only (Current Perf. & Training Only)	No Access (Only Accommodation <i>Limits</i> Provided)	No Access	No Access	No Access

Operational Logic & Matrix Notes:

- **"Status Only" for CORI:** HR Directors and Executives do not need to see the "rap sheet" or the specific details of an arrest. They only need to know "Cleared" or "Not Cleared." The COR retains the detailed record (if permitted) or the destruction log. This protects the firm from claims that a specific past offense (which might be irrelevant to the job) influenced an employment decision.
- **Bias Prevention:** By blocking HR and Executives from the SB 464 Demographic Silo, the firm creates a structural defense against discrimination claims. If an executive is accused of racial bias in a promotion decision, the audit log can prove they physically and digitally had no access to the demographic data silo.
- **Medical Privacy:** Direct Supervisors are only informed of *functional limitations* (e.g., "Cannot lift over 25 lbs" or "Requires a 10-minute break every hour"), never the *diagnosis* (e.g., "Has a herniated disc" or "Has diabetes"). This distinction is critical for ADA compliance. The Medical Silo remains the exclusive domain of the HR Director and COR.

4. Forensic Metadata & The 2026 Mandates (SB 513, SB 294, AB 692)

The 2026 compliance cycle introduces specific forensic requirements for record contents. The audit must verify that the following metadata exists and is accurate for every employee file. Missing metadata is no longer a clerical error; it is a statutory violation.

4.1 SB 513: The Training Log Mandate

Effective January 1, 2026, SB 513 amends Labor Code § 1198.5 to explicitly include "education and training records" within the definition of personnel records. This legislation addresses a gap where employees often lacked proof of the skills they acquired on the job, hindering their mobility. For Sapphos Environmental, this is a massive operational shift. The firm employs scientists and engineers with complex continuing education requirements for their licenses (QSD/QSP, PG, PE).

Previously, training certificates might have been kept loosely in a "Training" folder or just held by the employee. Now, they are statutory personnel records subject to inspection requests. If an employee requests their file, and the training records are missing or incomplete, the firm is in violation of the Labor Code.

Forensic Metadata Requirements: For every training session (e.g., "CASQA QSD Update," "CEQA Legal Review," or "Field Safety Training"), the record must strictly contain the following fields :

1. **Employee Name:** Full legal name.
2. **Provider Name:** The official entity providing the training (e.g., "California Stormwater Quality Association (CASQA)," "BPELSG," "City of Pasadena," or "Sapphos Environmental Internal Training").
3. **Date & Duration:** Exact date and number of hours. This is critical for verifying Continuing Education (CE) credits for licenses like the QSD/QSP, which requires 6 hours annually.
4. **Core Competencies:** A description of the skills covered. The statute specifically mandates noting **skills in equipment or software**. This is vital for technical staff. A log entry for "GIS Training" is insufficient; it must read "ArcGIS Pro Advanced Analysis - Core Competency: Spatial Analyst Tools & Geodatabase Management."
5. **Certification/Qualification:** The resulting credential (e.g., "QSD Renewal Year 1," "OSHA 10 Certification," or "Certificate of Completion").

Impact on Sapphos Environmental: For the firm's archaeologists and biologists, field safety training (e.g., snake avoidance, heat illness prevention) and technical training (ground-penetrating radar, acoustic monitoring equipment) must now be logged with this specific metadata. A generic "Safety Training - 1 Hour" entry is non-compliant. It must be "Heat Illness Prevention (8 CCR 3395) - 1 Hour - Core Competency: Symptom Recognition, Water Consumption, & Emergency Response Procedures."

4.2 AB 692: The Prohibition of "Stay-or-Pay"

AB 692 fundamentally changes how the firm can handle the costs of professional development. Effective for contracts entered into on or after January 1, 2026, "stay-or-pay" provisions—where an employee must repay training costs or "debt" if they leave within a certain period—are

prohibited. This law targets the practice of trapping employees in jobs by threatening them with significant debt if they quit.

Forensic Audit Trigger: The COR must audit all employment agreements for the 47 active employees. While the law applies to *new* contracts entered into on or after Jan 1, 2026, any *updates, renewals, or promotions* that involve a new contract in 2026 must have these clauses stripped.

- **Prohibited Scenario:** A clause requiring a Geologist to repay \$2,000 for a QSD certification course if they quit within 1 year. Or a clause requiring repayment of a "relocation bonus" that is structured as a debt.
- **Allowed Exceptions:** The exceptions are very narrow and specific. Repayment is only permitted for specific "transferable education credentials" if the agreement is *separate* from the employment contract, the employee has at least 5 business days to consult an attorney, the repayment is prorated based on tenure, and it is interest-free. "Training" that is specific to the employer's internal processes (e.g., "Sapphos Environmental Protocol Training") can *never* be subject to repayment.
- **Risk:** If the firm has a standard "Training Reimbursement Agreement" template, it is likely void and potentially exposes the firm to unfair competition claims and penalties of up to \$5,000 per employee.

4.3 SB 294: The "Know Your Rights" Notice Cycle

By February 1, 2026, and annually thereafter, the firm must issue a standalone "Workplace Know Your Rights" notice. This is a forensic compliance point—the COR must retain proof of delivery (e.g., a signed acknowledgment or digital read receipt) for every employee. The "set it and forget it" approach to labor posters is no longer sufficient; active notification is required.

Content Requirements: The notice must clearly explain rights related to:

- **Workers' Compensation:** Benefits, disability pay, and medical care.
- **Immigration:** Protections against unfair immigration-related practices and rights during inspections.
- **Unionization:** The right to organize and engage in concerted activity.
- **Constitutional Rights:** Specific guidance on 4th and 5th Amendment rights during law enforcement encounters at the workplace. This is particularly relevant for field staff who might encounter enforcement officers on job sites.

Emergency Contact Component: By March 30, 2026, the firm must legally allow employees to designate a specific contact for notification in case of arrest or detention at work. This is a new data field that must be managed. It must be stored in the RBAC system, likely within the General Personnel or Emergency silo, accessible to the COR and HR for immediate use, but protected from general view.

5. Security Accountability: CJIS & CORI Compliance

Given the sensitivity of forensic data, the human element is the weakest link. The governance architecture must include rigorous training and accountability measures for anyone handling CORI (Criminal Offender Record Information).

5.1 CJIS Security Awareness Training

For the COR and any HR staff with "Status Only" access to background check results, compliance with the FBI CJIS (Criminal Justice Information Services) Security Policy is mandatory. This is not optional; access to CLETS and CORI is contingent upon it.

Training Mandate:

- **Frequency:** Initial training must be completed within 6 months of assignment to the role, and then strictly **biennially (every 2 years)** thereafter.
- **Content:** The training is comprehensive. It must cover social engineering (how to spot a manipulator), phishing, physical security (tailgating), password hygiene, and incident response. It effectively turns the HR staff into security assets.
- **Documentation:** The COR must maintain a training log (compliant with SB 513 metadata standards) showing that every authorized user has passed the test (typically with a score of 70%+). Failure to produce these logs during a DOJ audit can result in the revocation of the firm's access to background check data.

5.2 Deliverable: Security Awareness Training Schedule

This schedule ensures the firm remains compliant with both the biennial CJIS requirement and the annual general security best practices. It segments the workforce based on risk profile.

Training Module	Target Audience	Frequency	Mandate Source	Content Focus
Level 1: General Security Awareness	All Employees (47)	Annual	Best Practice / SB 513	Phishing, Password Security, Visitor Control, Data Privacy, "Clean Desk" Policy.
Level 2: CJIS/CORI Security	COR, HR Director, Executives	Biennial (Every 2 Years)	FBI CJIS Policy 5.2 / CLETS PPP	Handling CORI, Disposal/Destruction, Incident Reporting, Social Engineering, Media Protection.
Level 3: Sensitive Data Handling	HR, Finance, Payroll	Annual	SB 464 / ADA	Segregation of Medical/Demographic Data, RBAC Protocols, Handling "Dark Data" Silos.
Level 4: CEQA Record Preservation	Project Managers, Scientists	Annual	PRC 21167.6 (Golden Door)	Email retention, "Official Record" flagging, Draft vs. Final document handling, Avoiding spoliation of evidence.

5.3 Deliverable: Employee Statement Form (CLETS/CORI)

This form is the legal contract between the employee and the firm regarding data misuse. It is

explicitly required by the DOJ/CLETS policies. Every employee with *any* potential access to this data (even incidental) must sign it.

CLETS/CORI Employee Statement of Responsibility

Warning: Misuse of Information is a Crime Access to information from the California Law Enforcement Telecommunications System (CLETS) and Criminal Offender Record Information (CORI) is granted solely for authorized business purposes.

Statutory Penalties:

- **Misdemeanor:** Any person who knowingly furnishes a record or information obtained from a record to a person not authorized by law to receive it is guilty of a misdemeanor (Penal Code § 11142, § 13303).
- **Felony:** Misuse of public records and information from CLETS may constitute a felony under Government Code § 6200.
- **Dismissal:** Violation of these statutes will result in immediate dismissal from Sapphos Environmental and referral to the Department of Justice for criminal prosecution.

Employee Certification: I, [Employee Name], hereby certify that I have read and understand the laws regarding the security and confidentiality of CORI. I agree to:

1. Access CORI only when necessary for the performance of my official duties and based on a valid "Need-to-Know."
2. Never disclose CORI to unauthorized persons, including family, friends, or other employees who do not have a valid "Right-to-Know."
3. Store CORI in the designated secure containers/files as mandated by the Custodian of Records.
4. Immediately report any suspected security breach, unauthorized access, or loss of data to the Custodian of Records.

Signed: _____ **Date:** _____ (To be retained in the CORI/Background Silo - DO NOT place in General Personnel File)

6. Professional Licensure & Defensibility (BPELSG & CASQA)

For a firm like Sapphos Environmental, the validity of its environmental documents (EIRs, MNDs, SWPPPs) rests entirely on the licensure of its authors. A lapsed license can be catastrophic in court. The governance system must track these as "mandatory records" with the same rigor as tax forms.

6.1 BPELSG: Professional Geologists (PG) & Engineers (PE)

The Board for Professional Engineers, Land Surveyors, and Geologists (BPELSG) regulates these licenses. They are the gold standard for technical defensibility.

- **Renewal Cycle:** Biennial (every 2 years). The expiration date is tied to the renewal date, not the calendar year.
- **Continuing Education (CE):**
 - **Professional Engineers (PE):** Currently, California does *not* require mandatory CE for PE licensure renewal. However, the *training records* for any voluntary training must still be logged under SB 513 to prove competence in specific areas if

- challenged.
 - **Professional Geologists (PG):** Similar to PEs, mandatory CE is not currently a state requirement for renewal in California. However, many PGs hold licenses in other states (e.g., Texas, Oregon) which *do* require CE. If a Sapphos PG is working on a multi-state project, their California file must track the CE credits required for their other licenses to ensure they remain legally qualified to stamp documents in those jurisdictions.
- **Forensic Check:** Ensure the license expiration date is tracked 60 days out. A lapsed license means the individual cannot legally stamp documents, potentially halting a project. The COR should maintain a digital copy of the active license card in the "Qualifications" section of the personnel file.

6.2 CASQA: QSP/QSD (Stormwater)

The Qualified SWPPP Developer (QSD) and Qualified SWPPP Practitioner (QSP) certifications are critical for construction monitoring and compliance with the Construction General Permit (CGP). Unlike the PG/PE, this certification has strict CE mandates.

- **Renewal Cycle:** 2 years.
- **CE Requirement:** Strictly enforced. **6 hours of Continuing Education annually** is required. This is not negotiable.
- **Forensic Metadata:** The training log must explicitly show the "Course Name," "Provider" (must be a Trainer of Record or approved source), "Date," and "Duration." Failure to log these 6 hours annually results in loss of certification.
- **2022 CGP Review:** All QSD/QSPs must have completed the "2022 CGP Reissuance Review" modules. The COR must verify this specific certificate is in the file. If this review is missing, the QSD is not qualified to write SWPPPs under the 2022 permit, rendering any SWPPP they sign invalid.

7. Pasadena Municipal Compliance (PMC 4.65)

The location in Pasadena adds a layer of wage compliance that supersedes state minimums.

7.1 The Wage Floor

As of July 1, 2025, the Pasadena minimum wage is **\$18.04 per hour**. This rate applies to any employee who performs at least two hours of work per week within the geographic boundaries of Pasadena.

- **Forensic Audit Point:** Review payroll records for all non-exempt staff (interns, field techs, administrative support). Any rate below \$18.04 is a violation.
- **Overtime Calculation:** Overtime must be calculated based on this regular rate. If a field tech earns the minimum \$18.04, their OT rate is \$27.06. Errors here are common when payroll systems default to state minimums.
- **Notice Requirement:** The "official notice" of the Pasadena minimum wage must be posted in the workplace and included in new hire packets.

7.2 Record Transparency

Pasadena empowers the city to inspect payroll records to verify compliance. The COR must maintain these records for **4 years** (aligning with state practice). The records must clearly show the "Pay basis" (hourly vs. salary), "Applicable hourly rates" (including the \$18.04 floor), and the specific hours worked at each rate. The transparency required by Pasadena reinforces the need for the Financial/Payroll Silo in the RBAC matrix to be meticulously organized.

8. CEQA Administrative Record Retention

Finally, the governance structure must account for the **California Public Resources Code § 21167.6**, which governs the "Administrative Record" for CEQA projects.

8.1 The "Golden Door" Standard

The seminal case *Golden Door Properties, LLC v. Superior Court* (2020) established that lead agencies (and by extension, their consultants who hold the records) must retain *all* written materials relevant to the project, including **emails** and **internal notes**.

- **Risk:** Deletion of project emails after 60 days (a common IT policy to save space) is non-compliant for CEQA projects. If a lawsuit is filed, and the emails discussing the biological impacts are gone, the agency (and Sapphos) can be sanctioned, and the project approval can be jeopardized.
- **Mandate:** The COR must enforce a policy where "project-specific" emails are either archived indefinitely or moved to a dedicated project folder that is immune from auto-deletion policies.
- **Metadata:** These records must be searchable and organized to allow for rapid production. The "Official Record" flag must be applied to substantive communications.

9. Conclusion: The Path to Forensic Readiness

The 2026 compliance cycle for Sapphos Environmental represents a convergence of criminal liability (COR duties), forensic data management (SB 513/SB 464), and strict economic regulation (AB 692/PMC 4.65). The "Good Order" of the firm's 47 personnel files is no longer a bureaucratic nice-to-have; it is a legal shield.

By implementing the **Custodian of Records Job Description**, adhering to the **RBAC Matrix**, utilizing the **Security Awareness Training Schedule**, and enforcing the **Forensic Metadata** standards outlined in this report, Sapphos Environmental will establish a defensible, compliant, and robust governance architecture. This structure protects the firm not only from state penalties but also ensures the professional integrity of the environmental documents that are its core product.

The immediate next step is the formal designation of the COR and the initiation of the DOJ Live Scan process, followed by the rigorous auditing of all employment contracts to strip out prohibited "stay-or-pay" clauses before the January 1, 2026 deadline.

Report Authored By: Senior Legal Compliance Counsel & Forensic Governance Specialist

Date: January 4, 2026 **For:** Sapphos Environmental, Pasadena, CA

Works cited

1. A Look at New California Labor and Employment Laws for 2026 | Insights - Holland & Knight,

<https://www.hklaw.com/en/insights/publications/2025/12/a-look-at-new-california-labor-and-employment-laws-for-2026> 2. CEQA Administrative Records: Challenges and Considerations When Asserting Claims of Privilege - Shute, Mihaly & Weinberger LLP, <https://www.smwlaw.com/2024/11/15/ceqa-administrative-records-challenges-and-considerations-when-asserting-claims-of-privilege/> 3. City of Pasadena Minimum Wage Ordinance, <https://www.cityofpasadena.net/planning/wp-content/uploads/sites/30/Minimum-Wage-Handout-Color-2025.pdf> 4. Minimum Wage Rate - City of Pasadena, <https://www.cityofpasadena.net/planning/wp-content/uploads/sites/30/OFFICIAL-NOTICE-EFFECTIVE-JULY-1-2025-ENGLISH.pdf> 5. California Code, Penal Code - PEN § 11102.2 - Codes - FindLaw, <https://codes.findlaw.com/ca/penal-code/pen-sect-11102-2/> 6. Custodian of Records | State of California - Department of Justice - Office of the Attorney General, <https://oag.ca.gov/fingerprints/custodian> 7. Custodian of Records Duties - California Department of Justice, <https://oag.ca.gov/sites/all/files/agweb/pdfs/fingerprints/forms/cor-duties.pdf> 8. CLETS EMPLOYEE/VOLUNTEER STATEMENT Use of information from the California Law Enforcement Telecommunications System (CLETS) and - County of San Diego, https://www.sandiegocounty.gov/content/dam/sdc/hhsa/programs/bhs/TRL/TRL%20Section%201/CLETS_Employee_Volunteer_Statement.pdf 9. Cal. Code Regs. Tit. 11, § 999.601 - Application for Confirmation | State Regulations, <https://www.law.cornell.edu/regulations/california/11-CCR-999.601> 10. Bill Text: CA AB3235 | 2023-2024 | Regular Session | Introduced - LegiScan, <https://legiscan.com/CA/text/AB3235/id/2932545> 11. California Amends Its Pay Data Reporting Requirements | Seyfarth Shaw LLP, <https://www.seyfarth.com/news-insights/california-amends-its-pay-data-reporting-requirements.html> 12. California Senate Bill 464 Sharpens State's Pay Reporting Teeth - Ogletree Deakins, <https://ogletree.com/insights-resources/blog-posts/california-senate-bill-464-sharpens-states-pay-reporting-teeth/> 13. Medical File | People & Culture - UC Berkeley, <https://hr.berkeley.edu/hr-network/central-guide-managing-hr/personnel-files/medical> 14. Fundamentals of Personnel Files for Employers in California, <https://www.californiaworkplacelawblog.com/2025/03/articles/california/fundamentals-of-personnel-files-for-employers-in-california/> 15. SB 513 Expands Employers' Recordkeeping Requirements for Education and Training Records: Atkinson, Andelson, Loya, Ruud & Romo, <https://www.aalrr.com/Labor-Employment-Law-Blog/sb-513-expands-employers-recordkeeping-requirements-for-education-and-training-records> 16. California Employers, Heads Up: Senate Bill 513 Just Changed the Rules on Personnel Files | Littler, <https://www.littler.com/news-analysis/asap/california-employers-heads-senate-bill-513-just-changed-rules-personnel-files> 17. Senate Bill 513: California Expands Personnel File Requirements, <https://www.californiaworkplacelawblog.com/2025/10/articles/california/senate-bill-513-california-expands-personnel-file-requirements/> 18. AB 692: California Doubles Down on Employee Mobility | CDF Labor Law LLP, <https://www.cdflaborlaw.com/blog/ab-692-california-doubles-down-on-employee-mobility> 19. The Ever-Changing Landscape of "Stay or Pay" Employment Contracts: New Restrictions in California and Existing Restrictions in Every State - Duane Morris, https://www.duanemorris.com/alerts/ever_changing_landscape_stay_pay_employment_contract_s_new_restrictions_california_existing_1125.html 20. California's Assembly Bill 692, Restricting Many So-Called "Stay-or-Pay" Employment Contract Terms, Set to Take Effect January 1, 2026 - Akin Gump, <https://www.akingump.com/en/insights/alerts/californias-assembly-bill-692-restricting-many-so-called-stay-or-pay-employment-contract-terms-set-to-take-effect-january-1-2026> 21. AB 692:

Preparing for California's 2026 restrictions on "stay-or-pay" provisions, <https://www.aoshearman.com/en/insights/ab-692-preparing-for-californias-2026-restrictions-on-stay-or-pay-provisions> 22. Labor Commissioner's Office - California Department of Industrial Relations, <https://www.dir.ca.gov/dlse/> 23. The Workplace Know Your Rights Act: California Mandates New Annual Notice To Employees, <https://calemploymentlawupdate.proskauer.com/2025/11/the-workplace-know-your-rights-act-california-mandates-new-annual-notice-to-employees/> 24. Workplace Know Your Rights Act Notices, Effective February 1, 2026 | CDF Labor Law LLP, <https://www.cdflaborlaw.com/blog/workplace-know-your-rights-act-notices-effective-february-1-2026> 25. User Accounts, Training and Certification Requirements - Department of Justice, <https://www.justice.gov/otj/page/file/1266936/dl?inline=> 26. CJIS Security - County of San Diego, https://www.sandiegocounty.gov/content/dam/sdc/probation/Policies/703_CJISSecurityProcedure.pdf 27. Criminal Justice Information Services (CJIS) Security Policy - FBI.gov, https://le.fbi.gov/cjis-division/cjis-security-policy-resource-center/cjis_security_policy_v5-9-5_20240709.pdf 28. CJIS Information Security Awareness Training for Texas, <https://www.dps.texas.gov/securityreview/secawarenesstraining.pdf> 29. CLETS Employee/Volunteer Statement - Ventura, CA, <https://www.cityofventura.ca.gov/DocumentCenter/View/23209/Exhibit-I-1-CLETS-EmployeeVolunteer-Statement?bidId=> 30. License Renewal Information - Board for Professional Engineers, Land Surveyors, and Geologists, https://www.bpelsg.ca.gov/licensees/renewal_info.shtml 31. California Professional Engineer License Renewal Requirements - PDH Now, <https://www.pdhnw.com/licensing/california> 32. State Licensure - American Institute of Professional Geologists, <https://aipg.org/page/statelicensure> 33. QSD And QSP Qualification | California Stormwater Quality Association, <https://www.casqa.org/training/cgp-training/qsd-qsp-overview> 34. FINAL - Guidelines on the QSD and QSP Continuing Education Requirement - California Stormwater Quality Association, <https://www.casqa.org/wp-content/uploads/2024/09/FINAL-Guidelines-on-the-QSD-and-QSP-Continuing-Education-Requirement-09-20-2024.pdf> 35. CEQA Administrative Record and Email Retention - Caltrans, <https://dot.ca.gov/-/media/dot-media/programs/environmental-analysis/documents/ser/ceqa-admin-record-and-email-retention-a11y.pdf> 36. Court of Appeal Clarifies Rules for Retaining Emails That are Included in CEQA Records, <https://www.hansonbridgett.com/Publications/articles/2020-08-10-court-appeals-emails-CEQA>