SAFEGUARDING OF RECORDS & RECORD RETENTION POLICY
CALIFORNIA SOFTWARE COMPANY LIMITED

This revised SOP/Policy has been prepared for California Software Company Limited to strengthen governance, information security, legal compliance, and operational integrity relating to safeguarding, retention, archival, and disposal of records.

1. PREAMBLE

California Software Company Limited (“the Company” or “Calsoft”) recognizes that effective records management is essential for regulatory compliance, operational continuity, information security, corporate governance, audit readiness, and protection of business interests.

---

2. OBJECTIVES

• Ensure proper safeguarding and retention of records
• Protect records from unauthorized access, alteration, damage, or loss
• Establish retention and archival framework
• Ensure compliance with legal and regulatory requirements
• Support business continuity and audit readiness

---

3. APPLICABILITY

This Policy applies to:

• Physical records
• Electronic records and databases
• Emails and communications
• Financial and legal documents
• HR and employee records
• Customer and vendor records
• Cloud and digital storage systems

---

4. DEFINITIONS

Record: Any document, file, data, communication, image, contract, or information created or maintained by the Company.

Electronic Record: Information stored digitally in systems, databases, servers, cloud, or electronic media.

Retention Period: Duration for which records are required to be maintained.

Archival: Secure storage of inactive records for future reference or compliance.

---

5. RESPONSIBILITIES

• Process owners shall maintain records under their control
• IT Department shall manage electronic storage, backups, and cybersecurity
• HR Department shall manage employee-related records
• Compliance and Legal teams shall ensure regulatory retention requirements
• All employees shall comply with this Policy

---

6. RECORD CLASSIFICATION

Records may be classified as:

• Confidential
• Internal Use
• Restricted
• Public
• Critical Business Records

---

7. RECORD RETENTION FRAMEWORK

• Records shall be retained as per legal, operational, and business requirements
• Retention schedules shall be periodically reviewed
• Financial, legal, tax, HR, and statutory records shall be preserved as per applicable laws
• Open matters such as litigation or investigations shall not be destroyed until closure

---

8. ELECTRONIC RECORD MANAGEMENT

• Electronic records shall be securely stored and backed up
• Cloud and server infrastructure shall be protected through cybersecurity controls
• Access controls and authorization mechanisms shall be implemented
• Backup and recovery procedures shall be periodically tested

---

9. RECORD SAFEGUARDING

The Company shall implement safeguards including:

• Secure storage rooms and fire protection systems
• Access control mechanisms
• Encryption and password protection
• CCTV and physical security where applicable
• Disaster recovery and business continuity systems

---

10. ACCESS CONTROL

• Access to records shall be role-based and authorized
• Confidential records shall be accessible only to authorized personnel
• Unauthorized copying, disclosure, or alteration is prohibited

---

11. BACKUP & DISASTER RECOVERY

• Periodic backups shall be maintained for critical records and systems
• Disaster recovery plans shall be implemented for business continuity
• Backup retention and restoration procedures shall be periodically reviewed

---

12. ARCHIVAL OF RECORDS

• Inactive records may be archived securely
• Archived records shall remain retrievable for legal, operational, or audit purposes
• Archival may be maintained in physical or electronic form

---

13. DISPOSAL OF RECORDS

Records due for disposal shall be destroyed securely through:

• Shredding of physical documents
• Secure deletion of electronic data
• Media destruction procedures

Disposal shall comply with legal and regulatory requirements.

---

14. LEGAL & REGULATORY COMPLIANCE

The Company shall comply with:

• Companies Act, 2013
• SEBI Regulations
• Income Tax and GST laws
• Data privacy and cybersecurity requirements
• Labour and employment laws

---

15. CONFIDENTIALITY & INFORMATION SECURITY

Employees shall maintain confidentiality of records and comply with Information Security, Data Privacy, and Access Control policies.

---

16. AUDIT & MONITORING

The Company may conduct periodic reviews and audits relating to:

• Record retention compliance
• Data security controls
• Access management
• Backup effectiveness
• Disposal procedures

---

17. VIOLATION OF POLICY

Any violation of this Policy may result in:

• Disciplinary action
• Legal action
• Financial penalties
• Termination of employment where applicable

---

18. REVIEW & AMENDMENT

This Policy may be reviewed and amended periodically by Management, Compliance Team, or Board based on legal, operational, or business requirements.

---

19. EFFECTIVE DATE

This revised Policy shall come into effect upon approval by the competent authority of California Software Company Limited.

APPROVAL

Approved by the Board / Competent Authority of California Software Company Limited.

Revised Date: April 10, 2026

Place: Chennai, Tamil Nadu, India

Chairman / Managing Director
Authorized Signatory