BIOMETRIC DATA RETENTION AND DESTRUCTION POLICY

(Mobile Timekeeping Application)

Effective Date: _____

Applies To: All employees, workers, contractors, and applicants whose biometric information is collected by Soulé Software Corporation ("Company").

1. Purpose

This Biometric Data Retention and Destruction Policy ("Policy") establishes guidelines for the collection, storage, retention, use, and destruction of Biometric Information, including photographic biometric images and facial geometry collected through the Company's mobile timekeeping application.

This Policy is intended to ensure compliance with applicable laws, including but not limited to:

- Illinois Biometric Information Privacy Act (BIPA)
- Texas Capture or Use of Biometric Identifier Act (CUBI)
- Washington Biometric Identifiers Law
- California Consumer Privacy Act (CCPA/CPRA)
- New York labor and privacy requirements
- Colorado Privacy Act biometric identifier and biometric data requirements

2. Scope

This Policy applies to all Company operations within the United States, all biometric data collected via mobile applications or related systems, and all employees, workers, and authorized third-party service providers handling such data

3. Definitions

"Biometric Information" is defined as:

- Photographic images of an individual's face used for identity verification;
- Facial geometry, templates, or mappings derived from such images; and/or
- Any data used to uniquely identify an individual through biometric means.

4. Data Collection Principles

The Company collects Biometric Information only for legitimate business purposes, including timekeeping, payroll, fraud prevention, and jobsite compliance. The Company limits collection to the minimum necessary data required for those purposes. It provides advance written notice and obtains written consent where required by law, and does not sell, lease, trade, or otherwise profit from Biometric Information.

5. Retention Schedule

The Company retains Biometric Information only for as long as necessary to fulfill the purposes for which it was collected, subject to the following maximum retention periods:

A. General Rule

Biometric Information will be permanently destroyed at the earliest of: 1) when the original purpose for collection has been satisfied; or 2) three (3) years after the individual's last interaction with the Company via the biometric system.

B. State-Specific Retention Requirements

Where applicable, the Company applies stricter rules:

- Illinois: Retention shall not exceed the earlier of:
  - Purpose fulfilled; or
  - Three (3) years after last interaction.
- Texas: Biometric identifiers will be destroyed within a reasonable time, and no later than one (1) year after purpose is satisfied.
- Washington: Retention limited to what is reasonably necessary for disclosed purposes.
- California: Retention is limited to what is reasonably necessary and proportionate for disclosed purposes.
- New York: Retention consistent with disclosed purpose and standard employment data retention practices.
- Colorado: Privacy Act biometric identifier and biometric data requirements

Where multiple laws apply, the Company will apply the most restrictive retention requirement.

6. Data Storage and Security

The Company implements reasonable standards of care to store, transmit, and protect Biometric Information, including:

- Encryption at rest and in transit, where feasible;
- Access controls limiting data access to authorized personnel;
- Vendor agreements requiring confidentiality and legal compliance;
- Periodic security reviews of systems and service providers.

Where required by applicable law, including Colorado law, the Company will maintain and follow a protocol for responding to any data security incident that may compromise the security of Biometric Information, biometric identifiers, or biometric data, including any legally required notification process.

7. Destruction Procedures

Upon reaching the applicable retention limit, Biometric Information will be permanently destroyed using commercially reasonable methods, including secure deletion of digital files from all production systems, deletion from backups in accordance with scheduled overwrite cycles and irreversible destruction of biometric templates and associated identifiers.

Destruction will be documented internally and performed in a manner that prevents reconstruction or recovery of the data.

8. Third-Party Vendors

Where Biometric Information is processed by third-party vendors:

- The Company will require vendors to implement equivalent retention and destruction controls;
- Written agreements will require compliance with applicable biometric laws; and
- Vendors must delete Biometric Information upon request or termination of services.

9. Individual Rights and Requests

Where required by applicable law (e.g., California), individuals may have the right to request information about how their data is used and to request deletion of their Biometric Information, subject to legal exceptions. The Company will respond to verified requests in accordance with applicable law.

10. Policy Administration

This Policy will be reviewed periodically and updated as needed to reflect changes in law or business practices. The Company may issue supplemental state-specific notices or procedures. Questions regarding this Policy should be directed to: [Privacy Officer / Legal Department Contact Information]

11. No Private Right Expansion

This Policy is intended to reflect compliance obligations and does not create independent contractual rights or expand any legal rights beyond those provided under applicable law.

12. Litigation Hold and Legal Preservation

Notwithstanding any other provision of this Policy, the Company will suspend the destruction of Biometric Information where such information may be relevant to:

- Pending or reasonably anticipated litigation, arbitration, or administrative proceedings;
- Government investigations, audits, or enforcement actions;
- Subpoenas, court orders, or other legal process;
- Internal investigations involving potential legal claims or compliance obligations.

A. Triggering a Hold

A litigation hold will be implemented when the Company, through its Legal Department or authorized leadership, determines that a duty to preserve information has arisen.
Upon issuance of a litigation hold:

- All routine or scheduled deletion of relevant Biometric Information will be immediately suspended;
- Relevant personnel and third-party vendors will be notified of preservation obligations;
- Systems containing Biometric Information will be identified and secured against alteration or deletion.

B. Scope of Preservation

The litigation hold will apply to:

- Biometric templates, facial geometry data, and associated identifiers;
- Photographic biometric images used for timekeeping verification;
- Related timekeeping records, logs, metadata, and audit trails; and
- Any linked payroll, access control, or jobsite records that may be relevant.

Preservation efforts will be reasonable and proportionate to the nature of the matter and consistent with applicable e-discovery standards.

C. Vendor and Third-Party Obligations

Where Biometric Information is maintained by third-party service providers:

- The Company will instruct such providers to preserve all relevant data;
- Vendor contracts will be enforced to ensure compliance with litigation hold requirements;
- Vendors must confirm suspension of deletion practices covering the relevant data.

D. Duration of Hold

The litigation hold will remain in effect until the Legal Department determines that the matter has been fully resolved and a formal release of the hold is issued. Upon release, retained Biometric Information will be returned to the applicable retention schedule or securely destroyed in accordance with this Policy, unless otherwise required by law.

E. No Expansion of Use

Biometric Information preserved under a litigation hold will not be used for new or unrelated purposes and will remain subject to confidentiality, security safeguards, and applicable privacy laws.

F. Priority Over Retention Schedule

This Litigation Hold provision supersedes all retention and destruction timelines set forth in this Policy for any data subject to a hold.