Family Law Software
A CENTERBASE COMPANY

Client Confidential Information Policy

1. Introduction and Purpose

This policy establishes the rules and procedures for identifying, handling, marking, and securely disposing of all **Client Confidential Information (CCI)**. The purpose is to ensure the organization meets its legal, contractual, and ethical obligations to protect clients' sensitive data.

2. Identification and Classification

2.1. Defined Process for Identification

The organization has a **defined process for identifying information marked as confidential**. This process is integrated into the Data Classification Policy and occurs at the point of creation, capture, or ingestion of data.

- **Contractual Designation:** Any information received from a client that is explicitly labeled as "Confidential," "Proprietary," or "Restricted" in a contract, Statement of Work (SOW), or Data Processing Agreement (DPA) is automatically classified as **Client Confidential Information (CCI)**.
- **Default Classification:** Any information that, if disclosed, would cause harm to the client (e.g., PII, financial data, intellectual property, unreleased product features) must be **classified as CCI by default** by the business unit receiving or generating it.
- **Annual Review:** Data owners must periodically review data inventories to ensure that CCI is correctly identified and classified according to current client agreements and regulatory requirements.

3. Handling and Marking

3.1. Marking Confidential Information

Confidential information is clearly marked upon creation or transfer to ensure proper handling by all personnel and systems.

- **Digital Files:** All electronic files (documents, spreadsheets, presentations) containing CCI must include a mandatory footer or header on every page stating, "CLIENT CONFIDENTIAL" and the date of creation/classification.

- **Physical Documents:** Any printouts of CCI must be stamped or clearly labeled "CLIENT CONFIDENTIAL" on the front cover and/or every page.
- **Databases/Systems:** CCI stored in databases or applications must be tagged or flagged with metadata indicating its confidentiality status, which drives the necessary access controls and security logging.

3.2. Access and Transmission

Access to CCI is restricted to personnel who have a **"need-to-know."** Any transmission of CCI must adhere strictly to the **Data Encryption Policy** and the **Information Transfer Policy**, mandating strong encryption for data both at rest and in transit.

4. Removal and Destruction

4.1. Processes for Destruction

Processes are in place for removing and destroying confidential information when it is no longer required for business purposes or when a client agreement mandates its return or destruction.

1. **Retention Schedule:** A formal data retention schedule dictates the maximum period CCI can be stored, ensuring compliance with contractual and regulatory mandates.
2. **Authorization:** The destruction of CCI must be formally approved by the data owner and recorded in an **Audit Log of Destruction.**
3. **Wiping/Sanitization:** Before decommission, storage media (hard drives, solid-state drives, tapes) that contained CCI must be wiped using a secure data sanitization process, such as those prescribed by **NIST Special Publication 800-88**.

4.2. Disposal to Baseline Standards

Confidential information is disposed to baseline standards to ensure data is permanently unrecoverable.

- **Digital Data:** CCI must be destroyed using cryptographic erasure (destroying encryption keys), logical sanitation tools (e.g., permanent deletion utilities), or physical destruction (shredding, disintegration) of the media. Standard file deletion (moving to the recycle bin) is strictly prohibited as a disposal method for CCI.
- **Physical Records:** Physical records containing CCI must be destroyed using a cross-shredding device to render them illegible, followed by secure disposal.

These procedures ensure that the destruction of CCI is irreversible and documented.