Family Law Software
A CENTERBASE COMPANY

Information Handling and Classification Policy

This policy establishes the rules for handling information based on its classification level to ensure data security, integrity, and confidentiality. All employees, contractors, and other authorized parties must adhere to these guidelines.

---

1. Information Classification

All information created, stored, or processed by the organization must be classified into one of the following levels. The classification level dictates the required security controls for handling and storage.

Classification	Definition	Examples
Confidential	Data whose unauthorized disclosure could cause significant harm to the organization, customers, or partners. **Strict access controls are mandatory.**	Customer PII (Personally Identifiable Information), financial records, unreleased source code, legal documents, security vulnerability reports.
Internal	Data intended for use only within the organization. Disclosure outside of the company should be avoided.	Internal memos, organizational charts, general HR policies, internal project plans, standard operating procedures.
Public	Data that is approved for public dissemination and poses no risk to the organization upon disclosure.	Press releases, marketing materials, public website content, job postings.

---

2. Information Handling Requirements

The following sections define the mandatory handling procedures for each classification level across various common scenarios.

2.1. Access and Authorized Parties

Classification	Authorized Parties	Access Control Principle
Confidential	Only individuals with a **documented business need-to-know**.	**Principle of Least Privilege:** Access must be strictly restricted and regularly audited.
Internal	All employees and authorized contractors.	Standard employee access rights; sharing with external parties requires management approval.
Public	The general public.	No access restrictions.

2.2. Classification Labeling

Classification	Labeling Requirement	Method
Confidential	**Mandatory.** Must be clearly marked.	Include the word **"CONFIDENTIAL"** in the header/footer of all digital documents, emails, and physical copies.
Internal	Recommended, especially when sharing.	Include the word "Internal" in the header/footer of digital documents.
Public	Not required.	N/A

2.3. Encryption Requirements

Classification	Data-in-Transit (During Transfer)	Data-at-Rest (In Storage)
Confidential	**Mandatory.** Must use secure protocols (e.g., HTTPS, SFTP, secure VPN).	**Mandatory.** Data must be encrypted using approved strong encryption standards (e.g., AES-256).
Internal	Recommended. Standard protocols (e.g., corporate email) are acceptable.	Required for endpoints (laptops/workstations). Recommended for centralized storage.
Public	Not required.	Not required.

2.4. Public Cloud Storage (e.g., AWS, Azure, Google Cloud)

Classification	Permissible Use	Requirements
Confidential	**Permitted only in approved, secured, and compliant cloud environments.**	Storage must use **mandatory data-at-rest encryption**, strict identity and access management (IAM) controls, and be located in approved geographic regions.
Internal	Permitted in approved corporate cloud storage/collaboration tools (e.g., SharePoint, Google Drive).	Must be stored in designated corporate accounts/tenants and protected by multi-factor authentication (MFA).
Public	Permitted.	Must be hosted on a public-facing service (e.g., corporate website server) and configured for public access.

2.5. Removable Media (e.g., USB drives, external hard drives)

Classification	Permissible Use	Requirements
Confidential	**Strictly prohibited** unless explicitly approved by the Information Security Officer for a specific, temporary need.	If approved, the media **must be full-disk encrypted** and tracked through an inventory log. The data must be securely erased immediately upon project completion.
Internal	Discouraged. Use approved cloud storage or corporate network drives instead.	If absolutely necessary, the media should be encrypted, used only on corporate devices, and data transferred back to a secure location as soon as possible.
Public	Permitted.	N/A

3. Policy Enforcement

Action	Description
Training	All personnel must complete mandatory annual training on this Information Handling and Classification Policy.

Action	Description
Auditing	The Security and IT teams will conduct periodic audits of access logs, encryption settings, and cloud configurations to verify compliance.
Violation	Any known or suspected violation of this policy must be reported immediately. Violations may result in disciplinary action, up to and including termination of employment or contract, and potential legal action.