Family Law Software
A CENTERBASE COMPANY

Securing Access on Public Networks

This policy establishes the organization's requirements for securing all data, transactions, and communications that occur over public-facing networks (e.g., the internet) with external parties.

1. Confidentiality and Integrity of Information Transactions

The organization must maintain the **confidentiality and integrity of information transactions** taking place over public networks.

1. **Encryption Methods: Encryption methods must be used for any communications with external parties**, in accordance with the organization's comprehensive **Encryption Policy**. This includes, but is not limited to:
    - Using **Transport Layer Security (TLS) 1.2 or higher** for all web-based access.
    - Employing Secure Shell (SSH) or Virtual Private Networks (VPNs) for secure remote access and data transfer.
2. **Input/Output Validation:** All public-facing applications must implement strict input validation to prevent common attacks (e.g., SQL injection, Cross-Site Scripting) and maintain data integrity.
3. **Authentication:** All access to application services on public-facing networks must require strong, multi-factor authentication (MFA) where feasible, especially for privileged or sensitive transactions.

2. Formal Agreements and Authorization Processes

2.1. Terms of Agreement with External Parties

The organization **applies a formal terms of agreement with external parties for any application services on public-facing networks**. These agreements must clearly define:

- The **roles and responsibilities** of all parties concerning data security and privacy.

- Required **security controls** and compliance mandates (e.g., adherence to this policy, patch management standards).
- Procedures for **incident notification and response**.
- Data **ownership, retention, and destruction** requirements.

2.2. Authorization of Transactional Documents

The organization **sets authorization processes for the approval, and signatory of key transactional documents** that are exchanged or processed over public networks.

- **Approval Workflow:** Key transactions (e.g., service contracts, data sharing agreements, financial approvals) must follow a documented workflow requiring approval from defined roles (e.g., Legal, Finance, Business Owner).
- **Non-Repudiation:** Digital signature technologies and audit trails must be utilized to ensure the authenticity and **non-repudiation** of the signatory for key electronic documents and contracts.

3. Compliance for Payment Transactions (PCI-DSS)

For all processing, storage, and transmission of cardholder data across public networks, the organization:

1. **PCI-DSS Compliance:** The organization is **certified against PCI-DSS** (Payment Card Industry Data Security Standard) for securing payment transactions across public networks. This includes:
   - Maintaining a secure network and systems (Requirement 1, 2).
   - Protecting stored cardholder data (Requirement 3).
   - Encrypting transmission of cardholder data across open, public networks (Requirement 4).
   - Regularly testing security systems and processes (Requirement 11).
2. **Annual Validation:** PCI-DSS compliance is validated annually through a Qualified Security Assessor (QSA) or internal resources, as required by the standard.