Family Law Software
A CENTERBASE COMPANY

Data Encryption Policy

1. Introduction and Purpose

This Data Encryption Policy establishes the mandatory standards for encrypting data at rest and in transit for all systems, applications, and services within the organization, including the core SaaS product infrastructure. The purpose is to protect **Sensitive Data** from unauthorized access, maintain data integrity, and ensure compliance with relevant regulatory and legislative requirements.

2. Scope

This policy applies to all systems, infrastructure (physical and virtual), applications, databases, and employees that store, process, or transmit Sensitive Data.

3. Policy Statement

All Sensitive Data, as defined in the organization's Data Classification Policy, must be protected by cryptographic controls. Encryption tools and practices must be deployed in line with this **Central Encryption Policy**.

4. Encryption at Rest

4.1. General Requirements

- All stored Sensitive Data must be protected using encryption.
- The organization shall leverage **non-deprecated, industry-standard cryptographic algorithms and protocols**. Algorithms must be reviewed annually or following any significant security advisory.
- Data must be encrypted before being written to persistent storage.

4.2. Full Disk Encryption (FDE)

- **Full disk encryption (FDE)** shall be applied to all corporate endpoints (laptops, desktops) and all infrastructure components (servers, virtual machines, storage appliances) that host or process Sensitive Data.
- FDE must be implemented using FIPS 140-2 validated solutions where required by the applicable data protection standard.

4.3. Database and File-Level Encryption

- In addition to FDE, **application-level** or **database-level encryption** must be used for highly Sensitive Data (e.g., Personally Identifiable Information (PII), payment data) to ensure protection even if the underlying storage layer is compromised.
- Data stored in object storage or shared file systems must be encrypted using strong, approved algorithms.

5. Encryption in Transit

All transmission of Sensitive Data over public, external, or non-trusted networks must be encrypted using secure, up-to-date protocols.

- **Protocols: TLS 1.2** or higher is the minimum acceptable protocol for data in transit over public networks. **SSL and earlier versions of TLS (e.g., TLS 1.0, 1.1)** are strictly **prohibited and deprecated**.
- **APIs and Communications:** All external-facing APIs and internal service-to-service communications carrying Sensitive Data must use encrypted channels.

6. Cryptographic Algorithms and Key Management

6.1. Approved Cryptographic Algorithms

The organization mandates the use of non-deprecated, strong cryptographic algorithms. The current approved algorithms include, but are not limited to:

- **Symmetric Encryption: AES-256** (Advanced Encryption Standard with a 256-bit key).
- **Asymmetric Encryption: RSA** (2048-bit minimum key length) or **Elliptic Curve Cryptography (ECC)**.
- **Hashing: SHA-256** or higher.

Note: The list of approved algorithms is subject to periodic review by the Security Team.

6.2. Key Management

- A **Central Key Management System (KMS)** must be used for the secure generation, storage, rotation, and revocation of all encryption keys.
- Encryption keys must be protected from unauthorized access, disclosure, and modification.
- Keys must be stored separately from the encrypted data they protect.

- Key rotation must occur on a defined schedule (e.g., annually) or upon any suspicion of compromise.

7. Compliance and Review

7.1. Regulatory Alignment

The **Encryption Policy and approach are aligned to relevant regulatory and legislative requirements concerning cryptography**, including but not limited to:

- **FIPS 140-2** (for cryptographic module validation).
- **NIST** (National Institute of Standards and Technology) best practices for cryptography.
- Any applicable industry-specific standards, such as **PCI DSS** (for payment card data) or **SOC 2** requirements.

7.2. Policy Review and Audit

This policy will be reviewed and approved by the Chief Information Security Officer (CISO) **at least annually** and following any major change in security technology, threat landscape, or regulatory requirements. Compliance with this policy will be verified through regular internal and external security audits.