Family Law Software
A CENTERBASE COMPANY

Data Backup Policy

This document establishes the organization's policy for backing up critical data, information systems, and applications. The purpose is to ensure the availability, integrity, and timely recovery of information assets in the event of a disaster, system failure, or data loss incident.

1. Scope and Applicability

This policy applies to **all systems and data** owned or managed by the organization, including, but not limited to:

- Critical business applications and databases.
- Server operating systems and configurations.
- User data stored on network file shares, collaboration platforms, and cloud services.
- System configurations for network devices and security tools.

2. Policy Objectives and Standards

2.1. Backup Strategy (3-2-1 Rule)

The organization adheres to the industry-standard **3-2-1 Backup Rule**:

- Maintain at least **three (3)** copies of the data (the production data and two backups).
- Store the copies on at least **two (2)** different types of media (e.g., disk and cloud).
- Keep at least **one (1)** copy **off-site** (or logically separated in a secure cloud environment).

2.2. Criticality and Frequency

Data is classified by criticality, dictating the required backup frequency and Recovery Point Objective (RPO):

Data Criticality	**Examples**	**Backup Frequency**	**Retention Period**	**Recovery Point Objective (RPO)**
Mission-Critical	Transactional databases, core financial systems, critical business applications.	Continuous or Hourly	90 Days (daily), 1 Year (monthly)	Maximum 1 hour of data loss.
Business-Critical	File servers, email, user network shares, application servers.	Daily (Full or Incremental)	30 Days (daily), 6 Months (monthly)	Maximum 24 hours of data loss.
Non-Critical	General internal documentation, development/test environments.	Weekly (Full)	7 Days	Negotiable based on business need.

2.3. Backup Types and Encryption

1. **Backup Types:** A combination of Full, Incremental, and Differential backups is used to balance speed, storage efficiency, and recovery time.
2. **Encryption:** All backup data, both **in transit** and **at rest** (on media or in the cloud), **must be encrypted** using industry-standard, approved cryptographic algorithms to protect data confidentiality.

3. Storage and Off-Site Requirements

1. **Media Rotation:** Backup media is managed and rotated according to documented schedules to ensure data integrity and availability.
2. **Off-Site Storage:** The off-site backup copy is secured from physical and environmental threats that could affect the primary data center. This storage location must meet the same security and compliance standards as the primary location.

3. **Isolation (Immutability/Air-Gapping):** Critical backups must be logically or physically isolated from the production network (e.g., using immutable storage or air-gapped systems) to protect them from ransomware attacks or other internal compromises.

4. Testing and Monitoring

4.1. Backup Monitoring

- Backup jobs must be monitored daily to verify successful completion.
- Failed or partially failed jobs require immediate investigation and resolution.

4.2. Restore Testing

- **Routine Restoration Tests:** Regular, documented restoration tests are performed at least **quarterly** on a randomly selected sample of backups (systems and data).
- **Disaster Recovery (DR) Testing:** The entire recovery process, including restoring key systems from backups, is validated during annual DR exercises.
- **Documentation:** All successful and failed restore tests, along with corrective actions, are formally documented. A backup is only considered valid if it has been successfully restored and verified.

5. Roles and Responsibilities

Role	**Responsibility**
IT Operations Team	Execution of scheduled backups, daily monitoring, and prompt remediation of failed jobs.
System Owners	Defining the data criticality, RPO, and required retention periods for their systems.
Security Team	Reviewing and approving the encryption methods and security controls applied to backup data and storage locations.
Management	Annual review and approval of this policy and allocation of necessary resources.