Family Law Software
A CENTERBASE COMPANY

Risk Assessment Policy

1. Purpose

The purpose of this Risk Assessment Policy is to establish the framework, methodology, and requirements for systematically identifying, analyzing, and evaluating risks to the Company's information assets, including client data, intellectual property, and core business operations. This policy is fundamental to protecting the **Confidentiality, Integrity, and Availability (CIA)** of all data and ensuring compliance with applicable legal and regulatory requirements, including those specific to the legal industry.

2. Scope

This policy applies to all employees, contractors, third-party vendors, information systems, applications, infrastructure, and business processes that create, receive, store, transmit, or dispose of Company or client information. This includes all software products developed and maintained by the Company.

3. Policy Statements

3.1. Risk Management Framework

The Company will adopt a recognized risk management framework (e.g., NIST SP 800-30, ISO 27005) to guide all risk assessment activities. The risk assessment process will be an integral part of the overall Risk Management Program.

3.2. Risk Assessment Frequency

A formal, comprehensive risk assessment shall be conducted at least **annually**. Additional risk assessments shall be triggered by:

- Significant changes to the IT environment (e.g., new infrastructure, major system upgrades, cloud migration).
- Deployment of new products, features, or services (e.g., as part of the SDLC).
- Changes in the regulatory or legal landscape that affect the Company or its clients.
- After a major security incident or breach.
- Following the discovery of a significant, high-impact vulnerability.

3.3. Asset Identification

All information assets relevant to the Company's operations and service delivery will be formally documented in an Asset Inventory. This includes, but is not limited to:

- Software products and applications.
- Servers, databases, and network devices.
- Data (e.g., client matter data, personally identifiable information, intellectual property).
- Physical facilities and equipment.
- Third-party services and vendors.

3.4. Risk Assessment Methodology

Each risk assessment will systematically follow these steps:

1. **Asset Identification:** Identify the assets within the scope of the assessment.
2. **Threat Identification:** Identify potential threats (e.g., unauthorized access, malware, natural disaster, insider misuse) that could exploit vulnerabilities.
3. **Vulnerability Identification:** Identify weaknesses in assets, controls, or processes (e.g., unpatched software, weak encryption, lack of training).
4. **Impact Analysis:** Determine the negative impact (financial, reputational, legal/compliance, operational) if a threat exploits a vulnerability. The impact will be categorized (e.g., Low, Medium, High, Critical).
5. **Likelihood Determination:** Estimate the probability of the threat successfully exploiting the vulnerability. The likelihood will be categorized (e.g., Rare, Unlikely, Possible, Likely, Certain).
6. **Risk Calculation:** Calculate the inherent risk level using the formula: **Risk = Likelihood x Impact**.

3.5. Risk Scoring and Criteria

The risk rating will be calculated using a defined matrix (e.g., a 5×5 matrix) resulting in categories such as: **Low, Medium, High, Critical**.

The criteria for each rating level will be clearly documented to ensure consistent application across all assessments.

3.6. Risk Treatment (Mitigation)

For all risks deemed **High** or **Critical**, a formal **Risk Treatment Plan** must be developed and executed. Risk treatment options include:

- **Mitigation:** Applying security controls to reduce the likelihood or impact of the risk.
- **Transfer:** Shifting the risk to a third party (e.g., through insurance or vendor contracts).
- **Avoidance:** Ceasing the activity or removing the asset that generates the risk.
- **Acceptance:** Formally documenting and accepting the risk if the cost of mitigation outweighs the potential loss, or if no reasonable controls exist. High or Critical risk acceptance requires approval from Senior Management/Executive Leadership.

3.7. Residual Risk

After implementing controls, the remaining level of risk is the **Residual Risk**. This risk must be documented and reviewed to ensure it falls within the Company's established **Risk Tolerance** level, as defined by the Executive Team.

3.8. Documentation and Reporting

All risk assessment activities, findings, risk scores, treatment plans, and residual risk levels will be formally documented. The results of the risk assessment will be reported to the Senior Management for review and resource allocation decisions. Documentation must be retained for at least three years for audit purposes.

4. Roles and Responsibilities

Role	Responsibility
Policy Owner	Maintains and reviews this policy.
Information Security Team	Leads the execution of risk assessments, maintains the risk register, and monitors the implementation of risk treatment plans.
Product & Engineering Teams	Collaborates on technical asset identification, vulnerability assessment, and implements mitigation controls for products.
Department Heads	Acts as **Risk Owners** for assets and processes within their purview, aids in impact analysis, and approves localized risk treatment plans.

Role	Responsibility
Executive Leadership	Approves the overall Risk Tolerance level and formally signs off on the acceptance of any High or Critical residual risks.

5. Enforcement

Non-compliance with this policy may result in disciplinary action up to and including termination of employment or contract, and/or termination of the business relationship.