Family Law Software
A CENTERBASE COMPANY

Access Control Policy

1. Purpose and Scope

1.1 Purpose

The purpose of this policy is to establish the rules, standards, and procedures for controlling access to all organizational networks, information systems, applications, and data. This ensures the **confidentiality, integrity, and availability** of information assets and maintains compliance with regulatory requirements.

1.2 Scope

This policy applies to **all employees, contractors, vendors, and business partners** who require access to the organization's networks and information systems, whether on-premises or cloud-based.

2. Authentication and Authorization

2.1 Employee Authentication to Networks and Information Systems

All users must authenticate using the methods defined below before accessing the network or any information system.

Access Type	Primary Authentication Method	Enhanced/Required Method
Network Access (VPN/Remote)	Strong Password (min. 12 characters)	**Multi-Factor Authentication (MFA)** is mandatory for all remote network access.
Information Systems / Applications	Strong Password (min. 12 characters)	MFA is required for all applications handling sensitive, regulated, or mission-critical data.

Access Type	Primary Authentication Method	Enhanced/Required Method
System Administration / Consoles	Strong Password (min. 14 characters)	**MFA is mandatory** (e.g., hardware token, biometric, or FIDO2 key).

2.2 Methods of Authentication

Method	Definition and Standard
Strong Passwords	Must meet complexity requirements (e.g., length, mixture of character types), not be re-used, and be changed every 90 days.
Multi-Factor Authentication (MFA)	Requires users to provide two or more verification factors (e.g., something they know (password), something they have (token), or something they are (biometric)).
Single Sign-On (SSO)	Utilize centralized Identity Provider (IdP) for all applications to ensure consistent application of access and authentication rules.

3. Access Control Rules and Principles

3.1 Principle of Least Privilege (PoLP)

Access privileges are granted based on the **Principle of Least Privilege (PoLP)**. Users are granted only the minimum access rights necessary to perform their legitimate job duties.

3.2 Role-Based Access Control (RBAC)

Access control rules are primarily determined by **specific user roles** (e.g., "HR Analyst," "Finance Clerk," "System Auditor") rather than individual names. Access is grouped by common job functions to ensure consistency and simplify management.

3.3 Access Reviews

User access privileges must be **formally reviewed and re-approved** by the resource owner or department head at least **quarterly**. Access for departing employees (including contractors) must be revoked immediately upon notification.

4. Privileged Access and Enhanced Authorization

4.1 Identification of Enhanced Access Needs

The organization will maintain a list of **critical systems** (e.g., domain controllers, firewalls, production databases) and the associated **privileged access roles** required to administer them. Access to these systems represents a higher risk and requires enhanced security controls.

4.2 Privileged Access Requirements

Policy Requirement	Control Mechanism
Authentication	Privileged accounts **must** use a dedicated, non-shared account with **MFA mandatory** (preferably hardware-backed or biometric).
Authorization (JIT)	Privileged access should be granted using **Just-In-Time (JIT) principles** where access is requested, approved, and automatically revoked after a limited, specified time window.
Password Management	Privileged account passwords must be managed and rotated by a **Privileged Access Management (PAM) system**.
Session Monitoring	All activity conducted under privileged accounts must be **logged and session-recorded** for audit and forensic purposes.

5. Access Granting and Approval Process

Step	Process Description	Responsibility
1. Request Initiation	The employee's manager initiates a formal access request ticket, specifying the required system/network, the reason, and the user's role.	Manager
2. Access Approval	The request is routed to the **System/Data Owner** (or designated delegate) who determines the appropriateness of the access based on the user's need-to-know and the Principle of Least Privilege.	System/Data Owner

Step	Process Description	Responsibility
3. Security Review	For all *privileged access* requests, the security team conducts an additional review to ensure the necessity and appropriate controls are assigned (e.g., PAM, JIT).	Security Team
4. Access Granting	The IT or System Administrator provisions the access and verifies that the authentication and authorization controls (e.g., MFA, RBAC group assignment) are correctly applied.	IT/System Administrator
5. Confirmation	The manager confirms the access is correct, and the request is marked complete.	Manager

6. Policy Review and Maintenance

This Access Control Policy will be formally reviewed by the Information Security Committee **annually (on or before October 31st)**. An immediate review will be triggered following any **significant business changes** that impact the IT environment, such as:

- Major system migrations (e.g., on-premises to cloud).
- Organizational restructuring that changes job roles and responsibilities.
- Acquisition of new systems that handle high-risk data.
- New regulatory compliance mandates.