Family Law Software
A CENTERBASE COMPANY

# Remote Work Policy

## 1. Purpose and Scope

### 1.1 Purpose

This policy establishes the rules and security requirements for employees and contractors working outside of the organization's secure physical premises. Its primary goal is to maintain the security of company data and systems while enabling productivity.

### 1.2 Scope

This policy applies to **all personnel** utilizing corporate assets to access organizational networks, systems, or data from a remote location.

## 2. Conditions and Restrictions for Remote Working

### 2.1 Authorized Assets and Secure Authentication

Remote access is **only permitted via organization-owned and managed assets** (laptops, mobile devices) that are configured and deployed by the IT department.

- **Secure Authentication: Strong, multi-factor authentication (MFA)** is mandatory for all remote connections to the corporate network (e.g., VPN) and cloud applications, as per the Authentication Information Management Policy.

### 2.2 Conditions for Remote Work

Personnel granted remote work privileges must adhere to the following conditions:

- Maintain a **private, secure workspace** free from unauthorized observation or access by family members or guests.
- Secure all corporate assets (laptops, mobile phones, etc.) against theft or loss, treating them as if they were in the main office.
- Do **not** use public or untrusted Wi-Fi networks (e.g., cafes, airports) for accessing sensitive data unless a corporate Virtual Private Network (VPN) is actively used.

### 2.3 Restrictions

The following activities are strictly prohibited while remote working:

- Storing **sensitive data** (as defined in Section 3.1) locally on a personal or unauthorized device.
- Printing sensitive corporate information at non-secure, remote locations.
- Allowing family members or guests to use corporate assets.

### 3. Managing Information Sensitivity

#### 3.1 Information Sensitivity and Access Controls

Remote working conditions must be directly managed based on the **sensitivity of the information** being accessed:

| **Information Sensitivity** | **Access Conditions and Restrictions** |
|---|---|
| **Public/Low Sensitivity** | Standard remote access (VPN + MFA) is sufficient. |
| **Internal/Moderate Sensitivity** | Standard remote access required. **No local storage** permitted; all work must be conducted on network drives or approved cloud storage. |
| **Sensitive/High Sensitivity** (e.g., client data, personal data, intellectual property) | Access requires **MFA**. IT-approved, **fully encrypted remote assets** are mandatory. **No printing or downloading** is permitted without explicit, documented management approval. |

#### 3.2 User Training Prerequisite

**Remote working functionality shall only be provided after the user has completed mandatory security awareness training** that includes specific modules on safe remote work practices, social engineering threats, and secure handling of corporate information.

### 4. Policy Governance and Review

#### 4.1 Executive Ownership

This Remote Work Policy is under the direct ownership and authority of the designated **Executive Sponsor** (e.g., Chief Information Officer).

#### 4.2 Policy Audit

This policy and its adherence will be formally **audited on at least an annual basis** by the Internal Audit or Security Team to ensure its continued effectiveness and relevance to the evolving threat landscape and business needs.