Security Protocol

Data handling, credential management, and operational hygiene standards for finance teams.

> **ZERO TRUST DOCTRINE:** Assume every network is hostile, every email is a phishing attempt, and every device is vulnerable. Convenience is the enemy of security. We do not trade safety for speed.

PROTOCOL 01 // CREDENTIAL MANAGEMENT

Password & Access Control

- **No Browser Storage:** Never select "Remember Password" in Chrome, Safari, or Edge. This data is easily extracted by malware.
- **The Manager:** All credentials must be stored in the designated Password Manager (1Password/LastPass).
- **Entropy Rule:** Passwords must be randomly generated strings of 16+ characters. No human-readable phrases (e.g., "Company2026!").
- **2FA/MFA is Absolute:** Two-Factor Authentication must be enabled on every account that supports it. Use an Authenticator App (Authy/Google); avoid SMS 2FA whenever possible.

PROTOCOL 02 // DATA TRANSMISSION

Handling Sensitive Financial Data

- **The "No Email" Rule:** Never send bank statements, tax IDs, or payroll files via standard email attachments. Email is unencrypted plain text.
- **The Secure Link:** Use the Client Portal or ephemeral secure links (e.g., 1Password "Share" or Box "Link with Expiry") to transfer files.
- **Screenshots:** Do not screenshot sensitive PII (Personally Identifiable Information) and share via Slack/Teams. This creates an unmanaged data trail.
- **Download Discipline:** Immediately delete sensitive files from your local "Downloads" folder after uploading them to the permanent storage drive.

PROTOCOL 03 // DEVICE HYGIENE

Hardware & Environment

- **Disk Encryption:** FileVault (Mac) or BitLocker (Windows) must be active on all workstations.
- **The 5-Minute Lock:** Screens must auto-lock after 5 minutes of inactivity.
- **Public Networks:** Never access banking portals or the General Ledger via public Coffee Shop/Airport WiFi without a VPN.
- **Clean Desk:** No physical notes containing passwords or financial figures may be left on desks or visible on whiteboards during video calls.

PROTOCOL 04 // SOCIAL ENGINEERING

Verification Standards

- **Vendor Change Requests:** If a vendor emails requesting a change in bank routing numbers, you must VERIFY via phone call using a number on file (not the number in the email signature).
- **Urgency is a Red Flag:** Any request from a "CEO" or "Founder" demanding immediate wire transfer or gift cards is a scam. Protocol dictates verbal confirmation for all outbound wires.

I acknowledge that I have read and understood the Bkept Security Protocol. I understand that adherence to these standards is a condition of my access to financial data.

EMPLOYEE SIGNATURE

DATE