

EMBEZZLEMENT PREVENTION CHECKLIST

Use this checklist quarterly, and anytime you hire or promote financial staff.




OWNER OVERSIGHT (NON-NEGOTIABLE)

- I personally open and review all bank statements
- I review canceled checks and deposits each month
- I understand the basic flow of money through my business
- I know who has access to each financial system
- I regularly ask questions about financial reports



ACCOUNTING & BOOKKEEPING CONTROLS

- No employee has end-to-end control of any financial process
- The bookkeeper cannot sign checks
- Bank reconciliations are done monthly by someone other than the bookkeeper
- Payroll is processed by someone different from bookkeeping
- Credit card statements are reviewed monthly
- All deposits match invoices and receipts  Purchasing & Vendor Controls



PURCHASING & VENDOR CONTROLS

- Purchase orders are required for all non-emergency purchases
- Vendor names are reviewed for accuracy and duplication
- New vendors require owner approval
- Bills are matched to purchase orders before payment
- I periodically review the vendor list myself



CASH, CHECKS & DEPOSITS

- Customers are discouraged from paying in cash

EMBEZZLEMENT PREVENTION CHECKLIST

- All checks are stamped “For Deposit Only”
- No “Less Cash” deposits are allowed
- Deposits are made intact and documented
- After-hours calls are matched to invoices and deposits



EMPLOYEE & PAYROLL SAFEGUARDS

- Background checks are performed on all key employees
- Payroll reports are reviewed every pay period
- Employee lists are reviewed for accuracy
- Bonuses and reimbursements require approval
- Confidentiality agreements are signed



SOFTWARE & AUDIT TRAIL CONTROLS

- Accounting software security is enabled
- Strong, unique passwords are required
- Audit trails are turned on and reviewed monthly
- Only the owner has full administrative rights
- Transaction deletion permissions are disabled
- Void transaction authority is limited



PHYSICAL & DATA SECURITY

- The company database is stored on a secure server
- Server access is physically restricted
- Nightly automated backups are running
- At least one backup is stored offsite
- Backup media is protected from fire and theft



PERIODIC REVIEWS & AUDITS

- I perform a deep financial review at least once per year
- An outside audit is conducted annually if partners are involved
- Audit trail anomalies are investigated immediately
- follow up on anything that doesn't make sense



FINAL REALITY CHECK

- I assume theft *can* happen and have controls in place
- I rely on systems, not trust alone
- I am visibly involved in financial oversight