

ADOPTION OF A FORMAL CODE OF ETHICS

<input type="checkbox"/>	Implement a comprehensive code of ethics for all finance officers.
<input type="checkbox"/>	Regularly update the code to reflect new regulations and best practices.
<input type="checkbox"/>	Ensure that all employees are aware of and understand the code.

FINANCIAL CONTROLS

<input type="checkbox"/>	Separate responsibilities for financial transactions among different employees to reduce the risk of fraud.
<input type="checkbox"/>	Conduct regular reconciliations of bank statements, credit card statements, and accounting record.
<input type="checkbox"/>	Establish clear approval processes for all financial transactions, including expenditures, invoices, and payroll.
<input type="checkbox"/>	Implement strict procedures for managing accounts payable and receivable to prevent unauthorized transactions.

EMPLOYEE CONTROLS

<input type="checkbox"/>	Conduct thorough background checks on all new hires, especially those handling financial transactions or sensitive information.
<input type="checkbox"/>	Implement monitoring systems to track employee activities and detect any unusual behavior.

CYBERSECURITY MEASURES

<input type="checkbox"/>	Ensure all systems and software are up to date with the latest security patches.
<input type="checkbox"/>	Use firewalls, antivirus, and anti-malware software to protect against cyber threats.
<input type="checkbox"/>	Require the use of complex passwords and change them regularly.
<input type="checkbox"/>	Enforce multi-factor authentication for all access points.
<input type="checkbox"/>	Conduct regular training sessions on cybersecurity best practices, including recognizing phishing attempts and avoiding unsafe websites.
<input type="checkbox"/>	Encrypt sensitive data both in transit and at rest to protect it from unauthorized access.

PHYSICAL SECURITY

<input type="checkbox"/>	Use security badges, access codes and surveillance systems to monitor and control access to the workplace.
<input type="checkbox"/>	Store sensitive documents in locked cabinets and restrict access to authorized personnel only.
<input type="checkbox"/>	Shred confidential documents before disposal.

VENDOR & THIRD-PARTY MANAGEMENT	
<input type="checkbox"/>	Conduct due diligence when selecting vendors and third-party partners, including background checks and reference verification.
<input type="checkbox"/>	Perform regular audits of vendor invoices and contracts to ensure accuracy and legitimacy.
<input type="checkbox"/>	Include fraud prevention clauses in contracts with vendors and third parties, outlining consequences for fraudulent activities.
FINANCIAL REPORTING & AUDITS	
<input type="checkbox"/>	Schedule regular internal and external audits to review financial statements and business operations.
<input type="checkbox"/>	Develop and maintain strong internal controls to detect and prevent fraud.
<input type="checkbox"/>	Maintain detailed audit trails for all financial transactions to facilitate tracking and investigation of discrepancies.
CUSTOMER & CLIENT INTERACTIONS	
<input type="checkbox"/>	Implement verification procedures for new customers and large transactions to prevent identity theft and fraud.
<input type="checkbox"/>	Use secure payment processing systems and avoid storing sensitive payment information.
<input type="checkbox"/>	Educate customers about common fraud schemes and how to protect their information.

INCIDENT RESPONSE	
<input type="checkbox"/>	Create a comprehensive fraud response plan outlining steps to take in the event of a fraud incident.
<input type="checkbox"/>	Designate a team responsible for managing and investigating fraud incidents.
<input type="checkbox"/>	Document all fraud incidents thoroughly and report them to relevant authorities and stakeholders.
<input type="checkbox"/>	After an incident, review the response and update policies and procedures to prevent future occurrences.

POLICIES & PROCEDURES	
<input type="checkbox"/>	Establish detailed procedures for all financial transactions.
<input type="checkbox"/>	Ensure transparency and accountability in the processing of financial transactions.
<input type="checkbox"/>	Regularly review and update policies to address any emerging issues.
<input type="checkbox"/>	Create a safe and anonymous reporting system for unethical behavior.
<input type="checkbox"/>	Encourage employees to report any suspected unethical practices.
<input type="checkbox"/>	Implement a zero-tolerance policy for retaliation against whistleblowers.