DOWNLOAD PDF POLICIES PROCEDURES TO PREVENT FRAUD AND EMBEZZLEMENT

Chapter 1 : ECFA Fraud Prevention

Policies & Procedures to Prevent Fraud and Embezzlement shows you how to proactively safeguard your business's assets and reputation from countless plots, schemes, and even identity theft. This invaluable tool prepares auditing CPAs, internal auditors, fraud investigators, and managers to.

Endnotes An Overview The Red Flags Rule tells you how to develop, implement, and administer an identity theft prevention program. A program must include four basic elements that create a framework to deal with the threat of identity theft. Red Flags are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft. If you have identified fake IDs as a red flag, for example, you must have procedures to detect possible fake, forged, or altered identification. Fortunately, the Rule also gives you the flexibility to design a program appropriate for your company â€" its size and potential risks of identity theft. While some businesses and organizations may need a comprehensive program to address a high risk of identity theft, a streamlined program may be appropriate for businesses facing a low risk. Securing the data you collect and maintain about customers is important in reducing identity theft. A business must implement a written program only if it has covered accounts. Does my business or organization regularly: No to all, the Rule does not apply. Yes to one or more, ask: Does my business or organization regularly and in the ordinary course of business: Yes to one or more, you are a creditor covered by the Rule. Two categories of accounts are covered: A consumer account for your customers for personal, family, or household purposes that involves or allows multiple payments or transactions. For example, there may be a reasonably foreseeable risk of identity theft in connection with business accounts that can be accessed remotely â€" say, through the Internet or the telephone. Your risk analysis must consider any actual incidents of identity theft involving accounts like these. But business models and services change. You may acquire covered accounts through changes to your business structure, process, or organization. FAQs I review credit reports to screen job applicants. Does the Rule apply to my business on this basis alone? I am a professional who bills my clients for services at the end of the month. Am I a creditor just because I allow clients to pay later? In my business, I lend money to customers for their purchases. The loans are backed by title to their car. Anyone who lends money â€" like a payday lender or automobile title lender â€" is covered by the Rule. Their lending activities may make their business attractive targets for identity theft. No one in our organization ever sees the credit reports. Is my business covered by the Rule? Your business is â€" regularly and in the ordinary course of business â€" using credit reports in connection with a credit transaction. The Rule applies whether your business uses the reports directly or whether a third-party evaluates them for you. I operate a finance company that helps people buy furniture. Does the Rule apply to my business? My business accepts credit cards for payments. Are we covered by the Red Flags Rule on this basis alone? How should I structure my program? The Guidelines to the Rule have examples of possible responses. But even a business at low risk needs a written program that is approved either by its board of directors or an appropriate senior employee. A Four-Step Process Many companies already have plans and policies to combat identity theft and related fraud. Different types of accounts pose different kinds of risk. For example, red flags for deposit accounts may differ from red flags for credit accounts, and those for consumer accounts may differ from those for business accounts. When you are identifying key red flags, think about the types of accounts you offer or maintain; the ways you open covered accounts; how you provide access to those accounts; and what you know about identity theft in your business. Sources of Red Flags. Consider other sources of information, including the experience of other members of your industry. Categories of Common Red Flags. Supplement A to the Red Flags Rule lists specific categories of warning signs to consider including in your program. The examples here are one way to think about relevant red flags in the context of your own business. Documents can offer hints of identity theft: Personal identifying information can indicate identity theft: How the account is being used can be a tip-off to identity theft: A customer, a victim of identity theft, a law enforcement authority, or someone else may be trying to tell

you that an account has been opened or used fraudulently. Detect Red Flags Sometimes, using identity verification and authentication methods can help you detect red flags. Consider whether your procedures should differ if an identity verification or authentication is taking place in person, by telephone, mail, or online. Depending on the circumstances, you may want to compare that to information you can find out from other sources, like a credit reporting company or data broker, or the Social Security Number Death Master File. You may be using programs to monitor transactions, identify behavior that indicates the possibility of fraud and identity theft, or validate changes of address. If so, incorporate these tools into your program. Your response will depend on the degree of risk posed. It may need to accommodate other legal obligations, like laws about providing and terminating service. Consider whether any aggravating factors raise the risk of identity theft. Update The Program The Rule recognizes that new red flags emerge as technology changes or identity thieves change their tactics, and requires periodic updates to your program. Factor in your own experience with identity theft; changes in how identity thieves operate; new methods to detect, prevent, and mitigate identity theft; changes in the accounts you offer; and changes in your business, like mergers, acquisitions, alliances, joint ventures, and arrangements with service providers. Administering Your Program Your Board of Directors â€" or an appropriate committee of the Board â€" must approve your initial plan. The Board may oversee, develop, implement, and administer the program â€" or it may designate a senior employee to do the job. Remember that employees at many levels of your organization can play a key role in identity theft deterrence and detection. In administering your program, monitor the activities of your service providers. One way to make sure your service providers are taking reasonable steps is to add a provision to your contracts that they have procedures in place to detect red flags and either report them to you or respond appropriately to prevent or mitigate the crime. Other ways to monitor your service providers include giving them a copy of your program, reviewing the red flag policies, or requiring periodic reports about red flags they have detected and their response. As a result, the Guidelines are flexible about service providers using their own programs as long as they meet the requirements of the Rule. The person responsible for your program should report at least annually to your Board of Directors or a designated senior manager. The Red Flags Rule is published at 16 C. See also 72 Fed. You can find the full text at http: The preamble B pages 63,, â€" discusses the purpose, intent, and scope of coverage of the Rule. The text of the FTC rule is at pages 63,, The Rule includes Guidelines B Appendix A, pages 63,, â€" intended to help businesses develop and maintain a compliance program. The Supplement to the Guidelines â€" page 63, â€" provides a list of examples of red flags for businesses and organizations to consider incorporating into their program. Transaction accounts include checking accounts, negotiable orders of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts. See also Regulation B. This Rule may be a helpful starting point in developing your program.

DOWNLOAD PDF POLICIES PROCEDURES TO PREVENT FRAUD AND EMBEZZLEMENT

Chapter 2 : Fraud Corruption and Control Management Policy and Procedure - University of Southern Que

Embezzlement and fraud are realities that all organizations must confront, with the growing list of collapsed corporate giants serving as evidence of the destruction caused by financial abuses. Policies & Procedures to Prevent Fraud and Embezzlement offers provocative new strategies to deal with this ongoing dilemma and serves as a road map to.

Management of each TBR institution is responsible for maintaining a work environment that promotes ethical and honest behavior. Additionally, it is the responsibility of management of each TBR institution to establish and implement internal control systems and procedures to prevent and detect irregularities, including fraud, waste and abuse. Management at all levels should be aware of the risks and exposures inherent in their areas of responsibility, and should establish and maintain proper internal controls to provide for the security and accountability of all resources entrusted to them. Fraudulent activities may include, but are not limited to the following: Theft, misappropriation, misapplication, destruction, removal, or concealment of any institutional assets or resources, including but not limited to funds, securities, supplies, equipment, real property, intellectual property or data. Improper use or assignment of any institutional assets or resources, including but not limited to personnel, services or property. Improper handling or reporting of financial transactions, including use, acquisitions and divestiture of state property, both real and personal. Authorization or receipt of compensation for hours not worked. Inappropriate or unauthorized use, alteration or manipulation of data, computer files, equipment, software, networks, or systems, including personal or private business use, hacking and software piracy. Forgery or unauthorized alteration of documents. Falsification of reports to management or external agencies. Concealment or misrepresentation of events or data. Acceptance of bribes, kickbacks or any gift, rebate, money or anything of value whatsoever, or any promise, obligation or contract for future reward, compensation, property or item of value, including intellectual property. Waste - Waste involves behavior that is deficient or improper when compared with behavior that a prudent person would consider a reasonable and necessary business practice given the facts and circumstances. Waste is a thoughtless or careless act, resulting in the expenditure, consumption, mismanagement, use, or squandering of institutional assets or resources to the detriment or potential detriment of the institution. Waste may also result from incurring unnecessary expenses due to inefficient or ineffective practices, systems, or controls. Waste does not necessarily involve fraud, violation of laws, regulations, or provisions of a contract or grant agreement. Abuse - Abuse involves behavior that is deficient or improper when compared with behavior that a prudent person would consider a reasonable and necessary business practice given the facts and circumstances. Abuse also includes misuse of authority or position for personal financial interest or those of an immediate or close family member or business associate. Abuse does not necessarily involve fraud, violation of laws, regulations, or provisions of a contract or grant agreement. To do so, management at all levels must behave ethically and communicate to employees and others that they are expected to behave ethically. Management must demonstrate through words and actions that unethical behavior will not be tolerated. Implementing Effective Internal Control Systems Management of each TBR institution has the responsibility to establish and implement internal control systems and procedures to prevent and detect irregularities, including fraud, waste and abuse. Internal controls are processes performed by management and employees to provide reasonable assurance of: Safeguards over institutional assets and resources, including but not limited to cash, securities, supplies, equipment, property, records, data or electronic systems; Effective and efficient operations; Reliable financial and other types of reports; and Compliance with laws, regulations, contracts, grants and policies. To determine whether internal controls are effective, management should perform periodic risk and control assessments, which should include the following activities: Review the operational processes of the unit under consideration. Determine the potential risk of fraud, waste, or abuse inherent in each process. Identify the controls included in the process or controls that could be included that result in a reduction in the inherent risk. Assess whether there are internal controls that need to be improved or added to the process under

consideration. Implement controls or improve existing controls that are determined to be the most efficient and effective for decreasing the risk of fraud, waste or abuse. Most managers will find that processes already include a number of internal controls, but these controls should be monitored or reviewed for adequacy and effectiveness on a regular basis and improved as needed. Typical examples of internal controls may include, but are not limited to: Adequate separation of duties among employees. Sufficient physical safeguards over cash, supplies, equipment and other resources. Appropriate documentation of transactions. Independent validation of transactions for accuracy and completeness. Documented supervisory review and approval of transactions or other activities. Proper supervision of employees, processes, projects or other operational functions. Reviews of Internal Control Systems Audits or other independent reviews may be performed on various components of the internal control systems. Internal Audit Internal Audit is responsible for assessing the adequacy and effectiveness of internal controls that are implemented by management and will often recommend control improvements as a result of this assessment. During an audit of a department or process, Internal Audit will also perform tests designed to detect fraud, waste or abuse that may have occurred. State Audit will also perform tests designed to detect fraud, waste or abuse that may have occurred. Other Reviews Various programs may be subject to audits or reviews by federal, state or other outside agencies based on the type of program, function or funding. Although audits and reviews may include assessments of internal controls, the primary responsibility for prevention and detection of fraud, waste or abuse belongs to management. Therefore, management should take steps to review internal controls whether or not audits are to be performed. Reporting Fraud, Waste or Abuse Responsibility for Reporting Fraud, Waste or Abuse Any official of any agency of the state having knowledge that a theft, forgery, credit card fraud, or any other act of unlawful or unauthorized taking, or abuse of, public money, property, or services, or other shortages of public funds has occurred shall report the information immediately to the office of the Comptroller of the Treasury T. Institutional administration with knowledge of fraud, waste or abuse will report such incidents immediately. Others, including institutional management, faculty and staff with a reasonable basis for believing that fraud, waste or abuse has occurred are strongly encouraged to immediately report such incidents T. Students, citizens and others are also encouraged to report known or suspected acts of fraud, waste or abuse. Although proof of an improper activity is not required at the time the incident is reported, anyone reporting such actions must have reasonable grounds for doing so. Employees with knowledge of matters constituting fraud, waste or abuse, that fail to report it or employees who knowingly make false accusations may be subject to disciplinary action. Protection from Retaliation State law T. The Higher Education Accountability Act of directs that a person who knowingly and willingly retaliates or takes adverse action of any kind against any person for reporting alleged wrongdoing pursuant to the provisions of this part commits a Class A misdemeanor. Confidentiality of Reported Information According to T. Although every attempt will be made to keep information confidential, circumstances such as an order of a court or subpoena may result in disclosure. Also, if TBR or one of its institutions has a separate legal obligation to investigate the complaint e. Methods for Reporting Fraud, Waste or Abuse Any employee who becomes aware of known or suspected fraud, waste or abuse should immediately report the incident to an appropriate departmental official. Incidents should be reported to one of the following officials or offices: A supervisor or department head; an institutional official; the Office of System-wide Internal Audit at or reportfraud tbr. If the incident involves their immediate supervisor, the employee should report the incident to the next highest-level supervisor or one of the officials or offices listed above. Employees should not confront the suspected individual or initiate an investigation on their own since such actions could compromise the investigation. A department official or other supervisor who receives notice of known or suspected fraud, waste or abuse must immediately report the incident to the following: The System-wide Chief Audit Executive will notify the Comptroller of the Treasury of instances of fraud, waste or abuse. After initial notification, each institution should refer to TBR Guideline B, Reporting and Resolution of Institutional Losses, for additional reporting procedures. The refusal by an employee to provide such assistance may result in disciplinary action. Remedies Available The Tennessee Board of

Regents will evaluate the information provided and make a determination concerning external reporting obligations, if any, and the feasibility of pursuing available legal remedies against persons or entities involved in fraud, waste or abuse against the institution. Remedies include, but are not limited to; terminating employment, requiring restitution, and forwarding information regarding the suspected fraud to appropriate external authorities for criminal prosecution. Resignation of Suspected Employee An employee suspected of gross misconduct may not resign as an alternative to discharge after the investigation has been completed. If the employee resigns during the investigation, the employment records must reflect the situation as of the date of the resignation and the outcome of the investigation General Personnel Policy, 5: Effect on Annual Leave An employee who is dismissed for gross misconduct or who resigns or retires to avoid dismissal for gross misconduct shall not be entitled to any payment for accrued but unused annual leave at the time of dismissal Annual Leave Policy, 5: Student Involvement Students found to have participated in fraud, waste or abuse as defined by this guideline will be subject to disciplinary action pursuant to the TBR Policy 3: The identities of persons communicating information or otherwise involved in an investigation or allegation of fraud, waste or abuse will not be revealed beyond the institution and staff of the TBR Offices of General Counsel, Business and Finance and System-wide Internal Audit unless necessary to comply with federal or state law, or if legal action is taken. Once such activities have been identified and reported, the overall resolution should include an assessment of how it occurred, an evaluation of what could prevent recurrences of the same or similar conduct, and implementation of appropriate controls, if needed.

DOWNLOAD PDF POLICIES PROCEDURES TO PREVENT FRAUD AND EMBEZZLEMENT

Chapter 3 : Preventing and Reporting Fraud, Waste or Abuse : | calendrierdelascience.com

Embezzlement and fraud are realities that all organizations mustconfront, with the growing list of collapsed corporate giantsserving as evidence of the destruction caused by financial calendrierdelascience.comes & Procedures to Prevent Fraud and Embezzlement offersprovocative new strategies to deal with this ongoing dilemma andserves as a road map to.

Staff training and education; and Client and community awareness. The University shall use the risk assessment model outlined in SharePoint and is briefly described below. The Vice-Chancellor is supported by the senior executive team in ensuring appropriate and effective control systems are operating. These systems will include requirements for fraud and corruption prevention in all aspects of University activity, including financial, administration, information communication technology, and academic areas. An internal control system consists of the policies, structure, procedures, processes, tasks and other tangible and intangible factors that enable the University to respond appropriately to operational, financial, compliance or any other type of risk. Managers and supervisors are responsible for daily operations and for maintaining cost effective internal controls within their individual areas of responsibility. All managers and supervisors must share responsibility for the prevention and detection of fraud. Equally, all Employees and officers of the University must share the responsibility for the prevention and detection of fraudulent and corrupt activities, which includes the reporting of suspected instances of such activity. The internal control environment will be periodically reviewed by the Planning and Quality Unit, the Internal Audit Office and the external auditors. The review will also include the Compliance Register and other internal controls. Accordingly, all Employees are encouraged to report suspected or known instances of fraud and corruption. Where an individual has an honest and reasonable belief that a University Member may have engaged in, is engaging in or will engage in any of the conduct outlined in the definitions of Public Interest Disclosures, information concerning that conduct should be reported to the University. A report made to a person other than an appropriate entity and not made in accordance with this policy may not be afforded the protection of the legislation. Reports of Public Interest Disclosures should be made verbally, in writing via the form below or by email to: If a report is made to any of the individuals or entities indicated in i to iv above, the report is to be referred, in writing, to the Director Integrity and Professional Conduct as soon as is practicable, to ensure that the whistleblower process is adhered to thereafter. If the report concerns the Director Integrity and Professional Conduct , the report must be referred to the Vice-Chancellor. External agencies to which reports on fraud and corruption are made will be determined by legislative requirements, and may include such agencies as the CCC, the Queensland Police Service, and the Queensland Audit Office. The Investigations Officer may consult with other appropriate University officers or external experts as necessary, whilst maintaining the confidentiality of the individual making the report. The CCC Facing the facts describes the various steps involved in conducting a formal investigation as follows: If the initial recommendation is to proceed with a detailed investigation, the Investigations Officer will provide interim and final reports to the Director Integrity and Professional Conduct. The Director Integrity and Professional Conduct will review the outcomes and recommendations made by the Investigations Officer and commence appropriate action. Where the reported conduct concerns the Director Integrity and Professional Conduct , the above processes shall be conducted and managed by the Vice-Chancellor. Instances of fraud and corruption on the part of individuals other than Employees will be managed in accordance with contractual conditions specified in their association with the University, following an investigation process conducted by the University as outlined in the investigations section of the Disciplinary Action for Misconduct or Serious Misconduct Procedure. Fraud and corruption can result from departures from the expected standards of behavior, and the University code provisions underpin many of the operational practices designed to minimize these integrity risks. Staff should refer to the Code of Conduct Policy for further information. Employees should be made aware of the importance of reporting fraud,

corruption and illegal practices, and actively encouraged to do so. This should be done as part of new Employee induction as well as be included on the ongoing training programme. The undesirability of malicious or vexatious reporting, and the result of false reporting will also be emphasised. Fraud and Corruption Control as an additional resource when the need is determined by the seriousness and level of difficulty an applicable case.

DOWNLOAD PDF POLICIES PROCEDURES TO PREVENT FRAUD AND EMBEZZLEMENT

Chapter 4 : 10 Essential Tips for Preventing Corporate Fraud | i-Sight

He also offers individuals advice on avoiding identity theft. McMillan covers everything from case histories to the details of hiring agreements, and how to fire an employee who commits fraud. Each chapter contains recommendations, sample documents, key points and checklists.

Fraud Prevention Program Experts estimate that companies lose five to six per cent of their annual revenue to fraud, so a comprehensive fraud prevention program is essential. This consists of three things: And while fraud prevention efforts are designed to stop employee fraud, investigations of suspected fraud should deter other employees from committing fraud. Suspect an employee is committing fraud? Establish clear and easy to understand standards from the top down. Have an employee manual that clearly outlines these standards and keeps the rules from becoming arbitrary. Always check references and perform background checks that include employment, credit, licensing and criminal history for all new hires. Review all disbursements regularly. Segregation of duties of employees. Separate important accounting and account payable functions. Small-business owners and managers should review every payroll check personally. The person who has custody of the checks should never have check signing authority. The person opening the mail should not record the receivables and reconcile the accounts. Independent checks on performance, using audits, surprise check-ups, inventory counts, or other procedures to verify compliance with policies and procedures, as well as accuracy. Instill an anonymous reporting mechanism, such as an employee fraud hotline. Small-business owners should control who first receives the bank statements and other sensitive documents. Consider a separate post office box for the purpose of receiving bank statements, customer receipts or any other sensitive documents. All account reconciliations and general ledger balances should have an independent review by a person outside the responsibility area such as an outside accountant. This allows for reviews, better ensuring nothing is amiss and providing a deterrent for fraudulent activities. Conduct annual audits to motivate all bookkeeping-related staff to keep things honest because they can never be sure what questions an auditor is going to ask or what documents an auditor may request to review. Payroll fraud is one of the most common types of employee fraud. Get ahead of it with our free cheat sheet: How to Detect Payroll Fraud. While no company, even with the strongest internal controls, is completely protected from fraud, strengthening internal control policies, processes and procedures will go a long way towards making your company a less attractive target to both internal and external criminals. He holds a B.

Chapter 5 : Policies and Procedures to Prevent Fraud and Embezzlement - 20 CPE Credit Hours

Policies & Procedures to Prevent Fraud and Embezzlement offers provocative new strategies to deal with this ongoing dilemma and serves as a road map to reduce financial dishonesty in the workplace. Buy Both and Save 25%!

Chapter 6 : Employee Theft Prevention Policies | calendrierdelascience.com

Policies and Procedures to Prevent Fraud and Embezzlement: Guidance, Internal Controls, and Investigation By Edward J. McMillan pages; softcover John Wiley & Sons Inc., Hoboken, N.J., Nearly every enterprise is a potential victim of fraud, and CPAs well-versed in the scope of fraudulent.