ecclesiastical

Bulletin

Fidélité des employés et fraude en milieu de travail

Argent qui disparaît de la petite caisse, fausse facturation, chèques falsifiés, formulaire de remboursement falsifié, fraude par carte de crédit, fausse représentation financière...

Un vol peut avoir lieu dans tous les types d'organismes, y compris les petites entreprises, les organismes à but non lucratif, les maisons de retraite, les écoles et les groupes confessionnels. Malheureusement, les coupables sont souvent des « initiés », c'est-à-dire des gestionnaires, des employés et des bénévoles qui ont déjà été des membres importants et dignes de confiance de la communauté.

La fraude commise par des employés varie d'un simple vol, par exemple prendre des dons d'un récipient dans un lieu de culte ou voler de l'argent comptant et d'autres objets de valeur dans un foyer de soins, à la falsification de chèques, l'envoi de fausses factures ou les manœuvres frauduleuses de comptabilité. Dans certains cas, des employés ont détourné de petites sommes d'argent de façon régulière. Après plusieurs années, parfois même des décennies, ces sommes d'argent peuvent devenir très importantes.

Selon l'Association of Certified Fraud Examiners (ACFE), les cas typiques de fraude au Canada entraînent une perte moyenne de 90 000 $, et les statistiques démontrent que les manœuvres frauduleuses relatives à la facturation sont les plus courantes, c'est-à-dire dans plus du tiers des cas de fraude.[1]

Fidélité des employés et fraude en milieu de travail

La fraude en milieu de travail peut avoir lieu dans tous les types d'organismes, y compris les petites entreprises, les organismes à but non lucratif, les maisons de retraite, les écoles et les groupes confessionnels. De nombreux organismes à but non lucratif sont souvent plus susceptibles à la fraude, car elles n'ont pas mis en place les contrôles nécessaires pour prévenir les pertes et elles seront les plus touchées financièrement.

Les coupables sont souvent des « initiés », c'est-à-dire des gestionnaires, des employés et des bénévoles qui ont déjà été des membres importants et dignes de confiance de la communauté.

Il y a trois types principaux de fraude en milieu de travail, soit la corruption, l'appropriation illicite d'actifs et la fraude dans les états financiers.

Des signes de fraude incluent l'impossibilité de faire concorder les états financiers mensuels et des changements dans les comportements individuels, par exemple une personne qui change son style de vie (vivre au-delà de ses moyens), qui travaille plus d'heures que les heures régulières et qui ne prend pas de congé (de peur que ses activités frauduleuses ne soient détectées pendant son absence). Une personne peut brouiller les pistes de la fraude en créant ou en modifiant des documents sur papier ou électroniques existants.

En ce qui a trait à aborder la question des employés malhonnêtes, la première étape consiste à reconnaître que le risque existe dans pratiquement tous les organismes. L'étape suivante est de déterminer les domaines vulnérables où la fraude pourrait se produire, par exemple les dons en argent comptant, les transactions bancaires, la tenue de livres, la commande de fournitures, etc. Cet exercice ne devrait pas se limiter à la direction de votre organisme. En incluant les employés et les bénévoles, même de façon informelle, vous transmettez un message clair et puissant au sujet des normes de votre organisme et des standards que vous avez établis pour le comportement en milieu de travail.

Pratiques exemplaires

Voici certaines des pratiques exemplaires qui peuvent aider votre organisme à prévenir la fraude en milieu de travail.

1. Vérification des antécédents et du crédit

Incluez la vérification des antécédents dans vos pratiques d'embauche. Les mêmes vérifications devraient être effectuées pour les bénévoles que vous engagez. Incluez également la vérification du crédit pour les gens qui manipuleront de l'argent comptant ou d'autres fonds.

2. Code de conduite

Élaborez un code de conduite qui inclut des politiques, des processus et des mesures de contrôle pour prévenir les comportements frauduleux. Assurez-vous que chaque personne lit le code de conduite et signe un formulaire confirmant qu'elle a lu le code et qu'elle accepte de se conformer aux politiques et aux procédures présentées.

3. Politique antifraude

Une politique antifraude est un outil essentiel qui peut contribuer à protéger votre organisme contre la fraude. Une politique antifraude

officialise votre approche envers la prévention de la fraude, établit les mesures de contrôle nécessaires et présente les mesures qui seront prises envers les personnes coupables de fraude. Il est recommandé d'inclure votre service de ressources humaines (RH) dans l'élaboration de cette politique. La politique démontre aux employés et au public que l'organisme a adopté une culture antifraude et que la fraude ne sera pas tolérée. La politique doit être lue par tous les nouveaux employés et bénévoles au moment de leur embauche et doit être révisée et signée chaque année. Conservez la copie signée dans le dossier des RH de chaque personne.

4. Vérifications

Effectuez des vérifications internes et externes régulièrement. Avisez tout le monde que des vérifications sont effectuées régulièrement et que des renseignements sont activement recherchés au sujet des comportements frauduleux. De plus, effectuez des vérifications sans préavis pour combattre et détecter la fraude.

5. Examen par la direction

Pour appuyer davantage la culture antifraude de votre organisme, des examens doivent être effectués régulièrement par la direction concernant les contrôles internes, les processus, les comptes, les transactions et l'attestation des états financiers.

6. Rapprochement de comptes

Effectuez chaque mois des rapprochements de comptes à l'aide du rapprochement bancaire, de l'état de compte en banque et des images des chèques. Afin de réduire l'activité frauduleuse possible, le rapprochement des comptes doit se faire par une personne qui ne s'occupe pas des comptes ou des finances, des fournisseurs et de l'approvisionnement. Dans le cadre du rapprochement des comptes, il faut vérifier les noms des fournisseurs. Les fournisseurs doivent être inscrits à la liste approuvée et leur nom doit correspondre au nom qui apparaît sur le chèque. Faites des recherches et des enquêtes au sujet de tout fournisseur inconnu et de la raison de la dépense pour vous assurer qu'il s'agit d'une dépense légitime et non d'une activité potentiellement frauduleuse.

7. Formation

Formez les membres du personnel pour qu'ils soient attentifs en tout temps. Offrez une façon de permettre aux gens de signaler de façon anonyme les infractions ou les comportements frauduleux soupçonnés.

8. Ligne directe pour les dénonciateurs

Créez une façon pour les personnes qui sont à l'intérieur ou à l'extérieur de l'organisme, par exemple des clients, des fournisseurs

ou des entrepreneurs, de signaler de façon anonyme les infractions ou les comportements frauduleux soupçonnés.

9. Règle de deux personnes

Établissez un système de double contrôle pour la manipulation des fonds. Une politique qui exige que deux personnes qui occupent des postes non reliés manipulent l'argent permettra de réduire grandement la tentation et la possibilité de vol.

10. Séparation des responsabilités

Faites en sorte que plusieurs personnes partagent les responsabilités afin d'assurer un certain contrôle interne.

11. Accès

Faites en sorte que le nombre d'employés qui ont accès aux finances soit le plus petit possible. Lorsque vous minimisez l'accès, vous minimisez les risques.

12. Fournisseurs

Pour éviter les fausses factures et autres manœuvres frauduleuses liées à la facturation, assurez-vous que tous les fournisseurs ont été validés et approuvés.

13. Processus officiel d'approbation

Établissez une limite pour les employés et les bénévoles qui commandent des produits et des services. Lorsqu'ils doivent dépasser cette limite, des signatures supplémentaires doivent être obtenues.

14. Documents financiers

Tous les documents, physiques ou numériques, doivent être conservés de façon sécuritaire. Par exemple, les documents entreposés dans des endroits où des dégâts d'eau pourraient se produire, comme au sous-sol, doivent être à au moins six pouces du plancher. Une autre façon de prévenir les pertes est de numériser les documents et de les sauvegarder dans les archives infonuagiques ou sur des serveurs situés ailleurs. Consultez des professionnels des TI pour vous assurer que les documents sont entreposés de façon appropriée et protégés contre des cyberattaques.

Voici d'autres mesures à considérer :

15. Cyberattaques

Des pertes financières peuvent aussi être causées par des cyberattaques, ou des attaques par fraude psychologique, où des cybercriminels trompent les gens en envoyant de faux courriels, textos ou messages vocaux qui semblent venir d'un ami, d'un collègue ou d'une source fiable afin de tenter d'obtenir des mots de passe et des renseignements financiers. Une formation doit être offerte régulièrement aux membres du personnel et aux bénévoles qui ont accès aux ordinateurs, aux mots de passe et aux renseignements financiers de l'organisme pour qu'ils soient à l'affût d'attaques possibles de fraude psychologique. Consultez notre site Web https://ecclesiastical.ca pour lire notre document sur le contrôle des risques au sujet de la gestion des cyberrisques.

16. Dons

Si votre communauté accepte les dons en argent comptant, assurez-vous de les déposer le même jour. Utilisez la règle de deux personnes pour compter et déposer les fonds. La règle de deux personnes doit également être mise en œuvre pour traiter les dons qui sont envoyés par la poste. Si les fonds doivent rester dans vos bureaux, gardez-les dans un coffre-fort ou un bureau fermé à clé. Si possible, demandez à vos donateurs réguliers de faire leurs dons par transfert électronique de fonds.

17. Rotation des tâches

Dans la mesure du possible, faites la rotation des tâches et des responsabilités pour prévenir et détecter les activités frauduleuses. Encouragez les membres du personnel et les bénévoles à prendre des vacances obligatoires (idéalement deux semaines à la fois) pour vous aider à détecter des activités frauduleuses potentielles en leur absence.

En mettant en œuvre ces pratiques exemplaires, et si possible en établissant un comité des finances pour surveiller toutes les questions financières, votre organisme pourra plus facilement atténuer les risques liés à la fraude en milieu de travail et protéger sa réputation. En assurant la sécurité de vos dons, vous assurez également la confiance de vos donateurs.

Si vous soupçonnez des activités frauduleuses ou si vous recevez des allégations de fraude, assurez-vous d'inclure le service des ressources humaines et le service juridique dans l'enquête pour déterminer la meilleure façon de procéder, ce qui pourrait inclure des mesures disciplinaires et l'implication du service de police locale pour la poursuite d'accusation au criminel. L'utilisation des services de professionnels pour déterminer la meilleure façon de procéder peut protéger un organisme contre une incidence juridique potentielle, par exemple des demandes d'indemnité liées à l'emploi.

Si vous avez besoin d'aide juridique ou en matière de ressources humaines, communiquez avec votre courtier ou un spécialiste de la gestion des risques d'Ecclesiastical, ou consultez notre site Web à l'adresse **https://ecclesiastical.ca** pour obtenir des renseignements sur l'accès gratuit à ces services grâce à nos tiers fournisseurs de services LegalConnex et HRAssist.

Les pertes financières peuvent également être causées par des cyberattaques. Pour en savoir plus sur la gestion des cyberrisques, consultez notre site Web **https://ecclesiastical.ca.**

Références

Rapport 2020 aux nations sur la fraude et l'abus en milieu de travail de l'Association of Certified Fraud Examiners (ACFE)
https://www.acfe.com/fraud-resources/report-to-the-nations-archive

https://www.canadianunderwriter.ca/features/opportunity-for-fraud/

http://lrzconsulting.com/reviewing-bank-reconciliations-to-prevent-and-detect-fraud/

À PROPOS D'ECCLESIASTICAL INSURANCE

Ecclesiastical Insurance Office plc est une compagnie d'assurance commerciale spécialisée. Nous sommes vivement engagés à protéger les besoins des organismes qui enrichissent la vie des autres, à préserver l'histoire, les cultures et les communautés distinctes du Canada, et à appuyer les initiatives qui contribuent à améliorer la vie des gens dans le besoin.

ecclesiastical

Fier membre du BENEFACT GROUP

ecclesiastical.ca | @EIOCanada