QATAR CINEMA

قطر سينما

سياسة مخاطر الغش

دليل السياسات والاجراءات

أغسطس ٢٠٢٤

معلومات الوثيقة وتاريخ المراجعة:

اسم الوثيقة	سياسة مخاطر الغش
الاصدار	1.0
الحالة	قيد التنفيذ (سارية المفعول)
الكاتب	مكتب رسل بدفورد و شركاه
تاريخ الإنشاء	٢٠٢٤/٨/٢٠م
تاريخ النفاذ	٢٩ سبتمبر ٢٠٢٤

سجل التعديل:

الاصدار	التاريخ	تحديث من قبل (المسمى الوظيفي والقسم)	التغييرات المضمنة	تمت الموافقة عليها من قبل (المسمى الوظيفي والقسم)	تاريخ الموافقة

اعتماد السياسة :

الإســـــــم	الصفـــــــة	التوقيـــــــع
جمال الدين البنا	المدير المالي	
عبد الرحمن نجدي	المدير العـــام	
علي إسحاق ال إسحاق	الرئيس التنفيـذي	
محمد علي جمعة السليطي	رئيس مجلس الإدارة	

١. تعريف المصطلحات الأساسية

١,١. تعريف الغش

الغش هو "عمل متعمد من الإهمال أو الإتيان به من قبل أي شخص، يتم تنفيذه خلال معاملة أو عملية تُجرى يدويًا أو تحت نظام حاسوبي، مما يؤدي إلى الحصول على مكاسب غير مشروعة لأي شخص لفترة مؤقتة أو خلاف ذلك، سواء كان هناك خسارة مالية للشركة أم لا".

كما يُعرّف الغش أيضًا بأنه (عمل غير قانوني - سواء كان فعلًا أو إهمالا لفعل - يُنفَّذ باستخدام وسائل متعمدة وغير عادلة وشخصية، وأحيانًا حتى وسائل قانونية، بهدف الحصول بشكل مباشر أو غير مباشر على ميزة ملموسة أو غير ملموسة غير مستحقة، أو للهروب من التزامات من أي نوع، لتحقيق المنفعة الشخصية أو منفعة لطرف ثالث).

بالنسبة للتحقيقات في حالات الغش، يتم تعيين فريق متخصص بناءً على موضوع الغش وتقرير الإبلاغ عن المخالفات.

١,٢. تقرير الإبلاغ عن المخالفات

يشير تقرير الإبلاغ عن المخالفات إلى:

- **الإفصاح عن المخالفات:** الإبلاغ عن الأنشطة غير القانونية أو غير الأخلاقية التي يتم ملاحظتها داخل المنظمة.
- **التقرير الرسمي:** وثيقة أو تواصل منظم يوضح طبيعة المخالفة والأدلة التي تدعم الادعاء.
- **حماية المبلغين عن المخالفات:** آليات وسياسات داخلية مصممة لحماية الأفراد الذين يبلغون عن المخالفات من الانتقام أو العواقب السلبية.

تم إضافة "نموذج تقرير الإبلاغ عن المخالفات" في الملحق.

١,٣. الإرشادات

يمكن أن يكون الغش داخليًا أو خارجيًا.

المبادئ العامة التالية أساسية لإطار منع الغش واكتشافه:

- **الوقاية والكشف:** يجب أن تُدار الوقاية والكشف عن الغش بشكل أساسي من خلال الخطوط الأولى للدفاع. مثل أي خطر تشغيلي آخر، يجب على هذه الخطوط تحديد مخاطر الغش الداخلية والخارجية ضمن نطاق تدخلها، وتقييم هذه المخاطر، وتحديد وتشغيل إطار مراقبة يتماشى مع إرشادات المجموعة، واللوائح المعمول بها، وبيئة المخاطر الخاصة بها.
- **الخط الثاني للدفاع:** يتعلق بإدارة مخاطر الغش تحت إشراف وظيفة المخاطر، والتي تتكون من المسؤولين عن المخاطر العاملين على ضمان تنسيقًا لإطار المراقبة الدائمة لمنع الغش داخل الشركة وتطوير أفضل الممارسات.

٢. أنواع الغش

يمكن أن يتخذ الغش أشكالاً عديدة، كل منها يتضمن أساليب وأهداف محددة. فيما يلي بعض أنواع الغش الشائعة:

٢,١. الغش الداخلي

الغش الداخلي، المعروف أيضًا باسم غش/الاحتيال الموظفين أو السرقة الداخلية، يتضمن الأنشطة الاحتيالية التي يقوم بها الأفراد داخل المنظمة، مثل الموظفين أو المديرين. يمكن أن يكون لهذا النوع من الغش عواقب خطيرة، بما في ذلك الخسائر المالية، والتداعيات القانونية، وإلحاق الضرر بسمعة المنظمة. فيما يلي الجوانب الرئيسية للغش الداخلي:

أولا: أنواع الغش الداخلي الشائعة

- **الاختلاس:** يقوم الموظفون بتحويل أموال أو موجودات من المنظمة لاستخدامهم الشخصي. غالبًا ما يتضمن ذلك التلاعب بالسجلات المالية أو إجراء تحويلات غير مصرح بها.
- **الغش في تقارير المصاريف:** يقدم الموظفون تقارير مصاريف مزيفة أو مبالغ فيها للحصول على تعويض عن مصاريف شخصية أو مصاريف غير متكبدة.
- **الغش في الرواتب:** تعديل سجلات الرواتب لإنشاء موظفين وهميين، أو تضخيم ساعات العمل، أو تحويل الأجور إلى حسابات غير مصرح بها.
- **استغلال الأصول:** سرقة أو سوء استخدام الموجودات المادية أو الفكرية، مثل المخزون، المعدات، أو المعلومات الخاصة.

- **الغش في البيانات المالية:** تقديم بيانات مالية مضللة أو حذف معلومات مالية لتضليل أصحاب المصلحة، مثل تضخيم الإيرادات أو إخفاء الالتزامات.
- **الغش في المشتريات:** التلاعب بعمليات الشراء لتحقيق مكاسب شخصية، مثل التواطؤ مع الموردين، قبول الرشوات، أو تزوير العروض.
- **الرشوة والفساد:** قبول، أو تقديم رشوات، أو عمولات، أو حوافز أخرى للتأثير على قرارات العمل أو الحصول على معاملة جيدة.
- **تضارب المصالح:** اتخاذ قرارات تعود بالنفع على الذات أو الأطراف ذات العلاقة بدلاً من المنظمة، مثل منح عقود لشركة مملوكة لأحد أفراد العائلة.
- **تلاعب بالبيانات:** تعديل أو تزوير البيانات في الأنظمة المالية أو التقارير لتغطية السرقة، الأخطاء، أو الأنشطة الاحتيالية الأخرى.
- **الغش بالوثائق:** تزوير أو تعديل الوثائق، مثل العقود، الفواتير، أو الإيصالات، لخداع المنظمة أو المدققين.

ثانيا: مؤشرات الغش الداخلي

- السلوكيات غير المعتادة: إظهار الموظفين لتغيرات في نمط حياتهم، أو التكتّم، أو التوتر غير المعتاد.
- المخالفات في السجلات المالية: التناقضات في البيانات المالية، أو المعاملات غير المبررة، أو الأخطاء المحاسبية.
- التناقضات غير المبررة: عدم التطابق بين المخزون أو الموجودات المسجلة.
- الافتقار إلى الضوابط الداخلية: ضعف أو عدم كفاية الضوابط على العمليات المالية والوصول إلى المعلومات الحساسة.

يجب على كل موظف يلاحظ أحد التصرفات المذكورة أعلاه أن يُبلغ عنها وفقًا لسياسة الإبلاغ عن الغش والفساد الإداري والمالي و نموذج تقرير الابلاغ (الملحق ٢).

ثالثا: الإجراءات الوقائية

- تنفيذ ضوابط داخلية قوية: إنشاء وتطبيق سياسات وإجراءات صارمة للمعاملات المالية، وضوابط الوصول، والتدقيق.
- إجراء عمليات تدقيق منتظمة: تنفيذ إجراءات تدقيق منتظمة ومفاجئة للكشف عن التناقضات وضمان الالتزام بالسياسات.
- فصل المهام: تقسيم المسؤوليات بين الموظفين بحيث لا يكون لأي شخص واحد السيطرة الكاملة على جميع جوانب المعاملة المالية.
- تعزيز ثقافة الأخلاق: تشجيع بيئة عمل حيث يتم تعزيز السلوك الأخلاقي ومكافأته، ويكون الموظفون على دراية بعواقب الغش.
- تقديم التدريب: تكوين الموظفين عن مخاطر الغش، السلوك الأخلاقي، وكيفية الإبلاغ عن الأنشطة المشبوهة.
- تنفيذ سياسات الإبلاغ عن المخالفات: إنشاء قنوات إبلاغ سرية يمكن للموظفين استخدامها للإبلاغ عن حالات الغش المشتبه به دون خوف من الانتقام.
- مراقبة الأنظمة والمعاملات: استخدام التكنولوجيا لمراقبة وتحليل المعاملات بحثاً عن علامات النشاط غير المعتاد أو المشبوه.

الإجراءات	المسؤول	التوقيت
تنفيذ ضوابط داخلية قوية	مسؤول الشؤون المالية والادارية	بشكل مستمر
إجراء عمليات تدقيق منتظمة	المدقق الداخلي	مرة في السنة
فصل المهام	المديرون	بشكل مستمر
تعزيز ثقافة الأخلاق	المديرون ومسؤول المخاطر والامتثال	بشكل مستمر
تقديم التدريب	مسؤول المخاطر والامتثال مع مسؤول الموارد البشرية والادارية	مرة في السنة
مراقبة الأنظمة والمعاملات	مسؤول المخاطر والامتثال مع مسؤول تقنية المعلومات	في نهاية كل شهر

٢,٢. الغش الخارجي

يتضمن الغش الخارجي أنشطة احتيال يرتكبها أفراد أو كيانات خارج المنظمة. تهدف هذه الجهات الخارجية إلى خداع أو احتيال على المنظمة أو المساهمين فيها لتحقيق أرباح مالية. وفيما يلي الأنواع الشائعة من الغش الخارجي وخصائصها:

أولا: أنواع الغش الخارجي الشائعة

- الاحتيال الإلكتروني: يقوم المحتالون بإرسال رسائل بريد إلكتروني أو رسائل خادعة لخداع الأفراد للكشف عن معلومات حساسة مثل كلمات المرور أو تفاصيل الحسابات.
- سرقة الهوية: يستخدم المجرمون معلومات شخصية مسروقة لفتح حسابات أو إجراء عمليات شراء أو ارتكاب أنشطة احتيالية أخرى باسم شخص آخر.
- احتيال بطاقات الائتمان: استخدام غير مصرح به لمعلومات بطاقة الائتمان لشخص ما لإجراء عمليات شراء أو سحب الأموال.
- اختراق البريد الإلكتروني الخاص بالعمل: يستخدم المجرمون الإلكترونيون التزوير في البريد الإلكتروني أو الاختراق لتقمص شخصية المديرين التنفيذيين أو الشركاء في الشركة لطلب تحويلات مالية غير مصرح بها أو معلومات حساسة.
- الاحتيال عبر الإنترنت: مخططات احتيالية تتم عبر المنصات الإلكترونية، بما في ذلك مواقع التجارة الإلكترونية المزيفة، الاحتيال في المزادات، أو الاحتيال المتعلق بالرسوم المسبقة حيث يتم خداع الضحايا لدفع أموال مقابل بضائع أو خدمات غير موجودة.
- احتيال الاستثمار: ممارسات خادعة تشمل فرص استثمارية وهمية أو احتيالية تعد بعوائد عالية مع مخاطر قليلة، مثل الشركات الناشئة المزيفة.
- اختراق الحساب: يحصل المجرمون الإلكترونيون على وصول غير مصرح به إلى حساب فرد أو منظمة لسرقة الأموال أو إجراء معاملات غير مصرح بها أو ارتكاب أنشطة احتيالية أخرى.
- الهندسة الاجتماعية: التلاعب بالأفراد للكشف عن معلومات سرية أو القيام بإجراءات تعرض الأمن للخطر، غالبًا من خلال التلاعب النفسي أو الخداع.
- احتيال التأمين: يقدم الأفراد الخارجيون مطالبات كاذبة أو مبالغ فيها لشركات التأمين، وغالبًا ما يتضمن ذلك حوادث مفبركة أو خسائر مزيفة.
- احتيال الموردين أو البائعين: تشارك الكيانات الخارجية في ممارسات احتيالية تتعلق بتوريد البضائع أو الخدمات، مثل تقديم منتجات مزيفة أو تقديم فواتير مزيفة.
- احتيال ضريبي: يقوم المحتالون بتزوير إقرارات الضرائب أو تقديم معلومات كاذبة للسلطات الضريبية لتفادي الضرائب أو الحصول على استردادات غير مستحقة.
- احتيال الجمعيات الخيرية: التظاهر بتمثيل منظمة خيرية لجمع التبرعات من الأفراد ذوي النوايا الحسنة، بنية تحويل الأموال لتحقيق مكاسب شخصية.

ثانيا: مؤشرات الاحتيال الخارجي

- طلبات غير عادية: طلبات مفاجئة أو مشبوهة للحصول على المال أو المعلومات أو الوصول إليها من مصادر غير معروفة.
- معاملات غير منتظمة: معاملات مالية غير مفسرة أو غير عادية، خاصةً إذا لم تتوافق مع الأنشطة التجارية المعتادة.
- تواصل غير متسق: تواصل يبدو غير مناسب أو متناقض مع السلوك المعروف للمرسل المزعوم.
- وثائق احتيالية: مستندات مزورة أو معدلة تُستخدم لخداع أو تضليل.

ثالثا: مؤشرات الاحتيال الخارجي

- طلبات غير عادية: طلبات مفاجئة أو مشبوهة للحصول على المال أو المعلومات أو الوصول إليها من مصادر غير معروفة.
- معاملات غير منتظمة: معاملات مالية غير مفسرة أو غير عادية، خاصةً إذا لم تتوافق مع الأنشطة التجارية المعتادة.
- تواصل غير متسق: تواصل يبدو غير مناسب أو متناقض مع السلوك المعروف للمرسل المزعوم.
- وثائق احتيالية: مستندات مزورة أو معدلة تُستخدم لخداع أو تضليل.

رابعا: التدابير الوقائية

- تعزيز الأمن السيبراني: تنفيذ تدابير قوية للأمن السيبراني، بما في ذلك جدران الحماية، وبرامج مكافحة البرامج الضارة، والتشفير، لحماية البيانات من الهجمات الإلكترونية والاختراقات.
- تثقيف وتدريب الموظفين: تقديم تدريبات منتظمة حول كيفية التعرف على محاولات الاحتيال الخارجية والرد عليها، بما في ذلك تقنيات التصيد الاحتيالي والهندسة الاجتماعية.
- التحقق من الطلبات: دائماً تحقق من مصداقية الطلبات للحصول على معلومات حساسة أو تنفيذ معاملات مالية من خلال قنوات مستقلة.
- مراقبة وتحليل المعاملات: استخدام أدوات آلية لمراقبة المعاملات وتحديد الأنماط غير المعتادة التي قد تشير إلى نشاط احتيالي.
- إنشاء أنظمة للكشف عن الاحتيال: إنشاء أنظمة للكشف عن الاحتيال يمكنها التعرف على الأنشطة المشبوهة والابلاغ عنها في الوقت الفعلي.
- تطبيق المصادقة القوية: استخدام المصادقة متعددة العوامل لتأمين الوصول إلى الأنظمة والحسابات الحساسة.
- الإبلاغ عن الاحتيال: تشجيع وتسهيل الإبلاغ عن الأنشطة الاحتيالية المشتبه بها للسلطات المعنية أو الفرق الداخلية لمكافحة الاحتيال.
- مراجعة سياسات الأمان بانتظام: مراجعة وتحديث سياسات وإجراءات الأمان بشكل مستمر لمعالجة التهديدات والثغرات الجديدة.

الإجراءات	المسؤول	التوقيت
تعزيز الأمن السيبراني	مسؤول تقنية المعلومات	مرة في السنة
تثقيف وتدريب الموظفين	مسؤول المخاطر والامتثال مسؤول الموارد البشرية والادارية	مرة في السنة
التحقق من الطلبات	كل الموظفين	بشكل مستمر
مراقبة وتحليل المعاملات	مسؤول المخاطر والامتثال مع مسؤول تقنية المعلومات	في نهاية كل شهر
الإبلاغ عن الاحتيال	الإدارة العامة	في حالات الاحتيال
مراجعة سياسات الأمان بانتظام	مسؤول المخاطر والامتثال	مرة في السنة

يمكن أن يكون الاحتيال الخارجي معقدًا ومتنوعًا، ولكن من خلال اتخاذ نهج استباقي في الوقاية والكشف والاستجابة، يمكن للمنظمات تقليل تعرضها للمخاطر والتقليل من الأضرار المحتملة

٣. كشف الاحتيال – عملية التحقيق والعقوبات

٣,١. عملية التحقيق

في حال وجود شك في حدوث احتيال، يجب على مسؤول المخاطر بمساعدة المدير المعني باتباع العملية التالية:

أ. تحديد الشكوك

- الأحداث المسببة: تحديد علامات الاحتيال المحتمل من خلال الاختلافات في التقارير المالية، أو المعاملات غير المنتظمة، أو سلوك الموظفين.
- تقارير المبلغين عن المخالفات: تقييم التقارير الواردة من الموظفين أو الأطراف الثالثة الذين يشتبهون في وجود أنشطة احتيالية.

ب. التقييم الأولي

- المراجعة الأولية: إجراء مراجعة أولية لتحديد ما إذا كانت هناك أدلة كافية لضمان إجراء تحقيق كامل.
- تحديد النطاق: تحديد نطاق التحقيق لضمان تخصيص الموارد بشكل مناسب.

ت. تخطيط التحقيق

- فريق التحقيق: تشكيل فريق ذو خبرة ذات صلة مثل المدققين الداخليين، والمستشارين القانونيين، والمتخصصين في تكنولوجيا المعلومات.
- المنهجية: وضع خطة تحقيق مفصلة تحدد إجراءات جمع البيانات، والمقابلات، والتحليل.
- التوثيق: الحفاظ على توثيق دقيق لجميع الخطوات التي تم اتخاذها خلال التحقيق.

ث. جمع الأدلة

- تحليل البيانات: مراجعة السجلات المالية، وسجلات المعاملات، ورسائل البريد الإلكتروني، والبيانات ذات الصلة الأخرى لتحديد التناقضات أو الأنشطة الاحتيالية.
- المقابلات: إجراء مقابلات مع الموظفين والشهود والأفراد الآخرين ذوي الصلة لجمع معلومات إضافية.
- الفحص الجنائي: استخدام الأدوات والتقنيات الجنائية لتحليل الأدلة الرقمية، مثل ملفات الحاسب الآلي، وحركة المرور على الشبكة، والاتصالات الإلكترونية.

ج. التحليل

- تحديد الأنماط: تحليل الأدلة لتحديد الأنماط أو الاتجاهات التي تشير إلى سلوك احتيالي.
- التأكيد: التحقق من النتائج بمصادر أخرى لتأكيد دقة الأدلة وأهميتها.

ح. إعداد التقارير

- تقرير التحقيق: إعداد تقرير شامل يلخص النتائج والأدلة والاستنتاجات. يجب أن يتضمن التقرير توصيات للإجراءات المستقبلية.
- العرض: تقديم النتائج للإدارة العليا أو الجهة المسؤولة عن اتخاذ القرار.

خ. إجراءات المتابعة

- خطة العمل: تطوير وتنفيذ خطة عمل بناءً على نتائج التحقيق، والتي قد تشمل تغييرات في السياسات أو الإجراءات أو الضوابط.
- المراقبة: إنشاء آليات مراقبة لضمان فعالية الإجراءات التصحيحية وتقليل احتمال وقوع حوادث مماثلة.

د. العقوبات

- **الإجراءات التأديبية**
  - إجراءات التوظيف: بناءً على خطورة الاحتيال، قد تشمل العقوبات توبيخًا، أو إيقافا، أو تخفيضًا في المنصب، أو إنهاء الخدمة.
  - الإجراءات الخاصة بالدور الوظيفي: تعديل المسؤوليات أو إعادة تعيين الأدوار لمنع المزيد من المخاطر إذا كانت مشاركة الموظف أقل خطورة.

- **الإجراءات القانونية**
  - الدعاوى المدنية: رفع دعاوى مدنية لاسترداد الخسائر أو الأضرار الناتجة عن الاحتيال.
  - التهم الجنائية: التعاون مع الجهات المختصة لتقديم تهم جنائية إذا كان الاحتيال يتضمن أنشطة إجرامية.

- **التدابير المتعلقة بالسمعة**
  - الإفصاح العام: اتخاذ قرار بشأن ما إذا كان سيتم الكشف عن الاحتيال علنًا، مع مراعاة تأثير ذلك على سمعة المنظمة وثقة الأطراف ذات الصلة.
  - إدارة السمعة: تنفيذ استراتيجيات لإدارة وإصلاح سمعة المنظمة بعد حادثة الاحتيال.

- **التدابير الوقائية**
  - تحديث السياسات: مراجعة وتحديث سياسات وإجراءات منع الاحتيال بناءً على الدروس المستفادة من التحقيق.
  - التدريب والتوعية: تعزيز برامج تدريب وتوعية الموظفين حول منع الاحتيال لتقليل خطر الحوادث المستقبلية.

- **إجراءات الاسترداد**

– استرداد مالي: اتخاذ خطوات لاسترداد أي خسائر مالية من خلال مطالبات التأمين أو الإجراءات القانونية أو التدابير الداخلية.

– تحسين الأنظمة: الاستثمار في تحسين الأنظمة والضوابط لمنع الاحتيال المماثل في المستقبل.

ذ. التواصل

- التواصل الداخلي: إبلاغ جميع الموظفين بنتائج التحقيق وأي تغييرات في السياسات أو الإجراءات لتعزيز التزام المنظمة بمنع الاحتيال.
- التواصل الخارجي: إذا لزم الأمر، التواصل مع الأطراف الخارجية مثل المستثمرين أو الهيئات التنظيمية لإبلاغهم بالإجراءات المتخذة وأي تداعيات.

ر. حملات التوعية

- الهدف: تثقيف الموظفين حول أساليب الاحتيال الشائعة وأهمية اليقظة.
- المحتوى: تطوير مواد توضيحية تسلط الضوء على أنواع مختلفة من الاحتيال (مثل التصيد الاحتيالي، الهندسة الاجتماعية، التهديدات الداخلية) وتقديم أمثلة عملية.
- الوسائط: استخدام مزيج من النشرات البريدية الإلكترونية، الملصقات، التحديثات على شبكة الإنترنت الداخلية، والندوات التفاعلية للوصول إلى الموظفين بفعالية.
- التحديثات: تحديثات منتظمة - يفضل أن تكون شهرية أو ربع سنوية للحفاظ على الوعي مرتفعًا والتكيف مع التهديدات الناشئة.
- الملاحظات: تتضمن اختبارات أو استبيانات لقياس الفهم وتحديد المجالات التي تحتاج إلى مزيد من التركيز.

ز. تدريب الموظفين

- التدريب الأولي: تقديم تدريب شامل للموظفين الجدد حول الوقاية من الاحتيال، التعرف على الأنشطة المشبوهة، وإجراءات الإبلاغ.
- التدريب المستمر: جدولة دورات تنشيطية دورية لإبقاء الموظفين على اطلاع بأحدث مخططات الاحتيال وتقنيات الوقاية.
- التمارين العملية: تتضمن سيناريوهات لعب الأدوار والمحاكاة لتزويد الموظفين بخبرة عملية في التعرف على الاحتيال المحتمل والرد عليه.
- المواد المرجعية: توفير سهولة الوصول إلى دليل منع الاحتيال أو الموارد عبر الإنترنت للرجوع إليها بسرعة.
- التقييم: إجراء تقييمات أو اختبارات منتظمة لقياس معرفة الموظفين واستعدادهم.

س. التصيد عبر البريد الإلكتروني

- اختبارات التصيد الاحتيالي: إجراء اختبارات تصيد احتيالي بانتظام لتقييم وعي الموظفين واستجابتهم.
- التخصيص: تخصيص محاكاة التصيد الاحتيالي لتعكس الاتجاهات والتهديدات الحالية الخاصة بصناعتك أو مؤسستك.
- الملاحظات الفورية: بعد المحاكاة، قم بتقديم ملاحظات فورية للموظفين الذين وقعوا في اختبار التصيد، مع توفير تدريب إضافي أو موارد تعليمية.
- المقياس: تتبع وتحليل النتائج لتحديد الأنماط أو المجالات التي قد تحتاج إلى تدريب إضافي.
- التشجيع: تعزيز بيئة غير عقابية حيث يُشجع الموظفون على الإبلاغ عن محاولات التصيد المشبوهة دون خوف من العقوبات.

٤. الأدوار والمسؤوليات

٤,١ مجلس الإدارة

- **الإشراف**: توفير الإشراف العام على برنامج مكافحة الاحتيال وضمان توافقه مع أهداف المنظمة والمتطلبات القانونية.
- **الموافقة** :الموافقة على سياسة مكافحة الاحتيال وأي تغييرات مهمة عليها.
- **المراجعة** :مراجعة التقارير الدورية حول فعالية ضوابط مكافحة الاحتيال وأي حوادث احتيال كبيرة.

٤,٢ لجنة التدقيق الداخلي

- **الإشراف**: الإشراف على تنفيذ وفعالية ضوابط وإجراءات مكافحة الاحتيال.

- **الموافقة** :فحص تقارير التدقيق والتحقيقات المتعلقة بالاحتيال.
- **المراجعة** :تقديم الإرشادات بشأن إدارة المخاطر واستراتيجيات الوقاية من الاحتيال.

٤,٣. التدقيق الداخلي
- **التقييم**: إجراء تدقيقات ومراجعات دورية لتقييم فعالية ضوابط مكافحة الاحتيال.
- **التحقيق** :التحقيق في حالات الاحتيال المشتبه بها وتقديم النتائج إلى الإدارة ولجنة التدقيق.
- **التوصيات** :تقديم التوصيات لتعزيز تدابير مكافحة الاحتيال بناءً على نتائج التدقيق.

٤,٤. الإدارة العامة
- **القيادة** :إظهار الالتزام بتدابير مكافحة الاحتيال وتعزيز ثقافة النزاهة والامتثال.
- **التنفيذ** :ضمان تنفيذ سياسة مكافحة الاحتيال بفعالية ضمن مجالات مسؤوليتهم.
- **تخصيص الموارد** :تخصيص الموارد لمبادرات مكافحة الاحتيال، بما في ذلك التدريب والأنظمة.

٤,٥. مسؤول المخاطر والامتثال
- **التطوير** :تطوير وتحديث سياسة مكافحة الاحتيال والإجراءات ذات الصلة.
- **الامتثال التنظيمي** :ضمان توافق سياسة مكافحة الاحتيال مع القوانين واللوائح ذات الصلة.
- **التدريب** :تنظيم وإجراء برامج تدريبية حول الوعي بالاحتيال والوقاية منه.
- **المراقبة** :مراقبة فعالية ضوابط مكافحة الاحتيال وتوصية بالتحسينات.
- **التقارير** :تقديم تقارير عن القضايا والحوادث المتعلقة بالاحتيال إلى الإدارة العامة ولجنة التدقيق.

٤,٦. المديرون
- **التنفيذ**: تنفيذ سياسات وإجراءات مكافحة الاحتيال ضمن أقسامهم.
- **التقارير**: الإبلاغ عن أي سلوكيات احتيالية أو مشبوهة يتم ملاحظتها عبر القنوات المناسبة.
- **الدعم**: دعم مبادرات مكافحة الاحتيال من خلال تعزيز السلوك الأخلاقي وضمان الالتزام بالضوابط.

٤,٧. الموظفون
- **الامتثال**: الالتزام بسياسة مكافحة الاحتيال وإجراءاتها.
- **التقارير**: الإبلاغ عن الاحتيال المشتبه به أو السلوك غير الأخلاقي عبر القنوات المعتمدة.
- **الوعي**: المشاركة في برامج التدريب والبقاء يقظين بشأن مخاطر الاحتيال المحتملة.

٤,٨. المستشار القانوني
- **النصائح** :تقديم المشورة القانونية بشأن القضايا المتعلقة بالاحتيال، بما في ذلك التحقيقات والإجراءات القانونية المحتملة.
- **الامتثال** :ضمان توافق سياسات مكافحة الاحتيال مع المتطلبات القانونية والتنظيمية.
- **الدعم** :تقديم الدعم في تنفيذ الإجراءات القانونية المتعلقة بالاحتيال.

٤,٩. المدققون الخارجيون
- **المراجعة** :تقديم تقييم مستقل لفعالية ضوابط مكافحة الاحتيال.
- **التقارير** :تقديم تقارير عن أي مشكلات أو ضعف كبير تم تحديده خلال التدقيق إلى لجنة التدقيق والإدارة.

الملحق ١: أمثلة على حالات الاحتيال

دراسة الحالة هذه توضح كيف يمكن تحديد التحقيق في الغش الداخلي / الخارجي ومعالجته من خلال نهج منهجي، بما في ذلك فرض العقوبات المناسبة واتخاذ التدابير الوقائية لحماية المنظمة.

مثال (الغش الداخلي)

دراسة الحالة: الغش الداخلي

أ. الخلفية:

تم العثور على موظفة، جين سميث، التي تعمل كمحاسبة أولى في شركة إكس واي زي، متورطة في أنشطة احتيالية. كانت جين مسؤولة عن إدارة الحسابات الدائنة ولديها وصول إلى أنظمة مالية متعددة. على مدار ١٢ شهراً، قامت بتزوير الفواتير وإنشاء حسابات موردين وهمية لنهب الأموال.

ب. تحديد الشكوك

- الحدث المحفز: كشف التدقيق الدوري عن تناقضات في سجلات الذمم الدائنة، بما في ذلك دفعات مكررة وفواتير موردين غير منتظمة.
- تقرير المبلغ: قام محاسب مبتدئ بالإبلاغ بشكل مجهول عن نشاط مشبوه بعد ملاحظته نمط وصول غير عادي وتعديلات في السجلات المالية.

ت. التقييم الأولي

- المراجعة الأولية: أشارت المراجعة الأولية للتناقضات إلى احتمال حدوث نشاط احتيالي. تم اتخاذ القرار بإجراء تحقيق شامل.
- تحديد النطاق: حدد فريق التحقيق النطاق ليشمل مراجعة معاملات جين وسجلات الوصول وسجلات الاتصالات.

ث. تخطيط التحقيق

- فريق التحقيق: ضم الفريق مدققين داخليين، خبير في الأدلة الجنائية الرقمية، ومستشار قانوني.
- المنهجية: شملت الخطة تحليل بيانات مفصل، فحص جنائي للأدلة الرقمية، ومقابلات مع الموظفين المعنيين.
- التوثيق: تم توثيق جميع خطوات التحقيق بدقة لضمان وضوح ونزاهة العملية.

ج. جمع الأدلة

- تحليل البيانات: تم تحليل السجلات المالية للكشف عن أي مخالفات، مثل المدفوعات للمتعاملين غير الموجودين والتغييرات غير المصرح بها في تفاصيل الدفع.
- المقابلات: تم إجراء مقابلة مع جين، إلى جانب موظفين آخرين تفاعلوا معها أو كانت لديهم إمكانية الوصول إلى الأنظمة ذات الصلة.
- الفحص الجنائي: قام خبراء تكنولوجيا المعلومات بتحليل ملفات الحاسب الآلي، والاتصالات عبر البريد الإلكتروني، وسجلات النظام لتتبع الأنشطة غير المصرح بها وتأكيد تورط جين.

ح. التحليل

- تحديد الأنماط: كشفت التحليلات عن نمط من الأنشطة الاحتيالية حيث قامت جين بإنشاء حسابات بائعين وهميين ووافقت على المدفوعات لتلك الحسابات.
- التحقق: تم التحقق من النتائج من خلال مطابقتها مع كشوف الحسابات البنكية وسجلات البائعين لضمان الدقة وتأكيد الاحتيال.

خ. التقرير

- تقرير التحقيق: تم إعداد تقرير مفصل يلخص النتائج والأدلة ودور جاين في الاحتيال. شملت التوصيات اتخاذ إجراءات تأديبية وتحسينات في النظام.
- العرض: تم تقديم التقرير للإدارة العليا ومجلس الإدارة.

د. إجراءات المتابعة

- خطة العمل: شملت التدابير الفورية إلغاء وصول جاين إلى الأنظمة المالية وتعزيز الضوابط الداخلية.
- المراقبة: تم تنفيذ خطة مراقبة لمراجعة فعالية الضوابط الجديدة ومنع حدوث حوادث مماثلة.

ذ. العقوبات

- الإجراءات التأديبية: تم إنهاء خدمة جين من منصبها، وتم الإبلاغ عن أفعالها إلى السلطات القانونية لاتخاذ إجراءات قانونية إضافية.
- الإجراءات القانونية: رفعت الشركة دعوى مدنية لاسترداد الأموال المختلسة وتعاونت مع سلطات إنفاذ القانون للملاحقة الجنائية.
- الإجراءات المتعلقة بالسمعة: اختارت الشركة إصدار بيان عام حول الحادث لتهدئة الشركاء وضمان التزامها بالنزاهة والشفافية.
- الإجراءات الوقائية: تم تحديث السياسات والإجراءات، بما في ذلك تعزيز الرقابة والموازين في الذمم الدائنة. كما تم إجراء تدريب إضافي على الوقاية من الاحتيال لجميع الموظفين.
- إجراءات الاسترداد: سعت الشركة إلى استرداد الأموال المسروقة من خلال القنوات القانونية وطبقت ضوابط مالية جديدة لمنع الغش في المستقبل.

ر. التواصل

- التواصل الداخلي: تم إبلاغ الموظفين بالحادث والإجراءات الجديدة المتخذة لمنع الاحتيال في المستقبل.
- التواصل الخارجي: تم تحديث المستثمرين والمساهمين بالإجراءات التي تم اتخاذها لمعالجة المشكلة والجهود المستمرة لحماية الشركة من الاحتيال.

دراسة الحالة: الاحتيال الخارجي

أ. الخلفية

قام محتال خارجي، يعمل تحت ستار مورد ذو سمعة طيبة، بخداع شركة أي بي سي تيك من خلال التلاعب بعقد شراء. قدم المحتال فواتير مزورة وتلقى مدفوعات مقابل بضائع لم تُسلم أبداً.

ب. تحديد الشكوك

- الحدث المحفز: لاحظ موظفو الذمم الدائنة أنماط دفع غير عادية، بما في ذلك دفعات كبيرة لمورد جديد بدون أي معاملات سابقة أو فحوصات خلفية.
- علامات التحذير: كانت هناك تناقضات في فواتير المورد، مثل معلومات الاتصال غير المتسقة وتفاصيل مشكوك فيها حول البضائع المسلمة

ت. التقييم الأولي

- المراجعة الأولية: أكدت التحقيقات الأولية وجود تناقضات في مستندات المورد وغياب أي سجلات تشير إلى استلام البضائع.
- تحديد النطاق: تم تحديد النطاق ليشمل مراجعة جميع المعاملات مع المورد، التحقق من سجلات التسليم، وتقييم عملية الشراء.

ث. تخطيط التحقيق

- فريق التحقيق: ضم الفريق مدققين داخليين، محقق احتيال خارجي، ومستشار قانوني.
- المنهجية: تضمنت الخطة مقابلة الموظفين المعنيين، تحليل سجلات المعاملات، وإجراء فحوصات خلفية على المورد.
- التوثيق: تم الاحتفاظ بسجلات مفصلة للتحقيق لضمان الشفافية والمساءلة.

ج. جمع الأدلة

- تحليل البيانات: تم تحليل السجلات المالية وسجلات المعاملات لتحديد المخالفات في المدفوعات والفواتير.
- التحقق من المورد: تم تتبع معلومات الاتصال بالمورد، مما كشف أن الشركة لم تكن موجودة في العنوان المقدم وأن الشخص المتصل كان وهميًا.
- المقابلات: تم إجراء مقابلات مع موظفي المشتريات، وموظفي الذمم الدائنة، والشخص الذي وافق على عقد المورد.

ح. التحليل
- تحديد الأنماط: كشفت التحقيقات أن المحتال استخدم هوية شركة مزيفة لإنشاء فواتير احتيالية وتحويل الأموال من خلال معاملات وهمية.
- التأكيد: تم التحقق من النتائج عبر مصادر خارجية وسجلات تجارية أخرى لتأكيد أنشطة المحتال الاحتيالية.

خ. التقارير
- تقرير التحقيق: تم إعداد تقرير شامل يوضح خطة الاحتيال، الأدلة التي تم جمعها، ومدى الخسائر المالية.
- العرض: تم عرض التقرير على الإدارة العليا، وإذا لزم الأمر، على مجلس الإدارة لتوضيح الحادث والتوصية بالإجراءات اللازمة.

د. إجراءات المتابعة
- خطة العمل: شملت الخطوات الفورية وقف المدفوعات الإضافية للمورد الاحتيالي، مراجعة سياسات الشراء، وتعزيز إجراءات التحقق من الموردين.
- المراقبة: تم تنفيذ مراقبة معززة لتتبع ومراجعة المعاملات المستقبلية بشكل أكثر دقة.

ذ. العقوبات
- الإجراءات القانونية: قامت شركة أي بي سي تيك بالإبلاغ عن الاحتيال إلى وكالات إنفاذ القانون. تم بدء تحقيق جنائي، وتعاونت الشركة بالكامل.
- الدعاوى المدنية: رفعت الشركة دعوى مدنية لاسترداد الأموال المختلسة. على الرغم من عدم إمكانية تتبع المورد الاحتيالي، كان الهدف من الدعوى استرداد أي موجودات متاحة.
- الإجراءات المتعلقة بالسمعة: أصدرت الشركة بيانًا للمستثمرين حول الحادث والإجراءات التي تم اتخاذها لمنع حدوث مثل هذه الحوادث في المستقبل.
- الإجراءات الوقائية: تمت مراجعة عمليات الشراء لتشمل إجراءات تحقق أكثر صرامة وعمليات العناية الواجبة. تم تعزيز تدريب الموظفين على التعرف على الأنشطة الاحتيالية والإبلاغ عنها.

ر. التواصل
- التواصل الداخلي: تم إبلاغ الموظفين بالاحتيال، والخطوات المتخذة لمعالجته، والتدابير الجديدة لمنع حدوث حوادث مماثلة.
- التواصل الخارجي: تم تحديث الأطراف المعنية، بما في ذلك العملاء والشركاء، حول الحادث وطمأنتهم بشأن تدابير منع الاحتيال المعززة التي اتخذتها الشركة.

الملحق ٢: نموذج تقرير الابلاغ

---

١. معلومات التقرير

- **تاريخ التقرير :**(أدخل التاريخ)
- **رقم التقرير (إن وجد) :**(أدخل رقم التقرير)
- **مقدّم التقرير :**(اسمك (إذا لم يكن مجهول الهوية)
- **معلومات الاتصال :**(بريدك الإلكتروني / رقم هاتفك (إذا لم يكن التقرير مجهولاً))
- **طلب السرية :**(نعم / لا)

٢. وصف المخالفة

- **طبيعة القضية :**(صف نوع التصرفات أو الأنشطة غير القانونية (مثل، الاحتيال، التحرش، انتهاكات السلامة))
- **الوصف التفصيلي :**(قدم وصفاً شاملاً للقضية. اذكر الحوادث المحددة، التواريخ، والمواقع).

٣. الأفراد المتورطون

- **الأسماء والأدوار :**(سرد أسماء، مناصب، وأدوار الأفراد المتورطين أو الشهود على المخالفة).
- **العلاقة بالمنظمة :**(وصف علاقتهم بالمنظمة (مثل، موظف، مقاول، مدير)).

٤. **الأدلة**

- **الوثائق الداعمة :**(سرد وإرفاق أي مستندات داعمة، مثل رسائل البريد الإلكتروني، السجلات المالية، أو بيانات الشهود).
- **وصف الأدلة :**(وصف باختصار كل قطعة من الأدلة وأهميتها للتقرير).

٥. **تأثير المخالفة**

- **العواقب :**(وصف تأثير المخالفة على المنظمة، الأفراد، أو الجمهور).
- **المخاطر المحتملة :**تسليط الضوء على أي مخاطر أو أضرار محتملة قد تنشأ إذا لم يتم معالجة القضية).

٦. **الإجراءات السابقة المتخذة**

- **الإبلاغ الداخلي :**(تحديد ما إذا كانت القضية قد تم الإبلاغ عنها مسبقاً، وإذا كان الأمر كذلك، لمن وماذا كانت النتيجة).
- **الإجراءات المتخذة :**(وصف أي إجراءات تم اتخاذها لمعالجة أو التحقيق في القضية قبل هذا التقرير).

٧. **التوصيات (إذا وجدت)**

- **الإجراءات المقترحة :**(تقديم أي توصيات لمعالجة القضية، مثل التحقيق الإضافي، اتخاذ تدابير تصحيحية، أو إجراءات تأديبية).

٨. **تعليقات إضافية**

- **معلومات إضافية :**(تتضمن أي معلومات أو تعليقات أخرى قد تكون مفيدة في التحقيق).

٩. **الإقرار:**

- **دقة المعلومات :**(أقر بأن المعلومات المقدمة دقيقة حسب معرفتك).
- **الاقرار :**(أقر بأنك تفهم تبعات تقديم تقرير والإجراءات الوقائية المتاحة للمبلغين).

١٠. **التوقيع:**

- (توقيعك (إذا لم يكن التقرير مجهولً الهوية)

١١. **ملاحظات:**

- **السرية :**إذا كنت ترغب في عدم الكشف عن هويتك، يمكنك عدم إدراج معلومات الاتصال الخاصة بك والاشارة الى أن السرية مطلوبة.
- **التفاصيل :**قدم أكبر قدر ممكن من التفاصيل لضمان إمكانية اتخاذ اجراء بشأن التقرير.
- **المرفقات :**تأكد من إرفاق جميع الوثائق الداعمة ووضع علامات عليها بوضوح.

يعتبر هذا النموذج دليلاً ويجب تعديله ليتناسب مع أي متطلبات أو إرشادات محددة تقدمها مؤسستك.