صندوق التنمية للعراق

مذكرة الأمور الظاهرة من عملية تدقيق نظام المعلومات

وزارة المالية

٣١ كانون الأول ٢٠١١

إرنست وَيُونغ

ارنست و يونغ بغداد
محاسبون قانونيون
صندوق بريد ٦٠٠٤
بغداد – جمهورية العراق
هاتف ٠٠٩٦٤١٥٤٣٩٨٥٩ (٤ خطوط)
فاكس ٠٠٩٦٤١٥٤٣٩٨٥٩

٣٠ نيسان ٢٠١٢

السادة رئيس وأعضاء لجنة الخبراء الماليين
صندوق التنمية للعراق
بغداد – العراق

تحية طيبة وبعد،

لقد قمنا بتدقيق نظام المعلومات في وزارة المالية والمؤسسات التابعة لها. ويسرنا ان نبين ما يلي:
يوجد في قسم المحاسبة التابع لوزارة المالية نظامين تم تطويرهما داخليا من قبل مبرمجي الوزارة وذلك لتسجيل جميع العمليات المالية المتعلقة بصندوق التنمية للعراق سواء كانت ايرادات او نفقات.

١. **نظام الدينار العراقي**: وقد تم تطويره بإستخدام برنامج الفيجيوال فوكس برو، ويستخدم لتسجيل جميع الحركات المالية التي تتم بالدينار العراقي الخاصة بصندوق التنمية للعراق.
٢. **نظام الدولار الأمريكي**: وقد تم تطويره بإستخدام برنامج مايكروسوفت اكسس، ويستخدم لتسجيل جميع الحركات المالية التي تتم بالدولار الامريكي الخاصة بصندوق التنمية للعراق.

إن قسم تكنولوجيا المعلومات في البنك المركزي العراقي يستخدم **نظام سويفت** وذلك لعمل التحويلات الالكترونية الخاصة بصندوق التنمية للعراق. وقد تم شراء هذا النظام من شركة مجموعة المهندسين المتحدين.
إن الانظمة أعلاه تؤثر على البيانات المالية الخاصة بصندوق التنمية للعراق، لذلك، فقد قررنا القيام بعملية مراجعتها وتدقيقها.

إن المذكرة المرفقة تتضمن اقتراحات لتحسين تكنولوجيا المعلومات ومحددات السرية المتعلقة بها والتي لفتت إنتباهنا أثناء مراجعتنا لنظم المعلومات المختارة والمتعلقة بصندوق التنمية للعراق للسنة المنتهية في ٣١ كانون الأول ٢٠١١.
إن مراجعتنا للانظمة التي قمنا بإختيارها يهدف الى مساعدتنا في إبداء رأينا حول البيانات المالية وليس للكشف عن عمليات الاحتيال التي قد تحدث. إن عملية المراجعة والتدقيق التي نقوم بها ليس من الضرورة ان تشمل جميع التحسينات الممكنة لكافة نقاط الضعف القائمة.

سيكون من دواعي سرورنا أن نقوم بمناقشة هذه التوصيات معكم وكذلك مساعدتكم في تنفيذها.
ختاما، نشكركم على إتاحة هذه الفرصة لنا لتقديم خدماتنا ونشكر كافة العاملين في جميع دوائر ومؤسسات الدولة لما أبدوه من تعاون لتسهيل مهمتنا، راجين لكم دوام التقدم والازدهار.

وتفضلوا بقبول فائق الاحترام ،،،،

إرنست ويونـــغ/ العراق

بشـــر بكـــر

مفتاح الرموز

يحتوي هذا التقرير على الرموز التالية:

الرمز	البيان
درجة المخاطرة عالية	تتعلق الملاحظة بضعف جوهري يؤثر في تحقيق الأهداف الأساسية أو النتائج المالية أو تؤثر في السمعة المهنية. نوصي بضرورة إتخـــاذ إجراءات معالـــجة فورية.
درجة المخاطرة متوسطة	تتعلق الملاحظة بالأمور متوسطة الخطورة و التي قد تؤدي إلى ضعف في نظام الرقابـــة الداخلي و/أو كفـــاءة الأنشطـــة التشغيليـــة والتي يجب أن يتـــم الأفصاح عنها. نوصي باتخاذ إجراءات معالجة خلال فترة قصيرة.
درجة المخاطرة منخفضة	تتعلق الملاحظة بأمور قمنا بملاحظتها قد لا تؤثر على نظام الرقابة الداخلي و/أو فاعلية وكفاءة الأنشطة التشغيليـــة، ولكـــن يجـــب الإهتمام بها من قبـــل الإدارة. نوصي بإتخاذ إجراءات معالجة خلال فترة معقولة.
إمتثال	سبب الملاحظة عدم الإمتثال للتعليمات والإجراءات المطلوبة.
دليل إجراءات	سبب الملاحظة عدم وجود دليل إجراءات موافق عليه أو عدم تحديث دليل الإجراءات المعمول به حاليا.
إشراف وتوجيه	سبب الملاحظة ضعف أو عدم وجود إشراف وتوجيه كافي.
خطأ بشري	سبب الملاحظة خطأ بشري نتجت عنه درجة من المخاطرة.
موارد بشرية	سبب الملاحظة ضعف أو نقص في الموارد البشرية.

رقم الملاحظة	الوزارة	الملاحظة	درجة المخاطرة	السبب
١.	وزارة المالية	سياسات وإجراءات تقنية المعلومات – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة عالية	دليل إجراءات
٢.	وزارة المالية	الوصف الوظيفي – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة	إشراف وتوجيه
٣.	وزارة المالية	التدقيق الداخلي لتقنية المعلومات – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة	دليل إجراءات
٤.	وزارة المالية	عملية تغيير المقاييس وتطبيق التعديلات – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة عالية	دليل إجراءات
٥.	وزارة المالية	تعديل البرامج – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة عالية	دليل إجراءات
٦.	وزارة المالية	فصل المهام – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة عالية	موارد بشرية
٧.	وزارة المالية	فصل بيئات التطوير والاختبار للأنظمة – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة عالية	إشراف وتوجيه
٨.	وزارة المالية	مراجعة سجلات التدقيق - نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة متوسطة	إشراف وتوجيه
٩.	وزارة المالية	ضوابط كلمة السر – نظام الدينار العراقي	درجة المخاطرة عالية	إشراف وتوجيه
١٠.	وزارة المالية	ضوابط الدخول المتزامن للنظام – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة متوسطة	إشراف وتوجيه
١١.	وزارة المالية	ضوابط الخروج التلقائي – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة	إشراف وتوجيه
١٢.	وزارة المالية	ضوابط اغلاق حساب مستخدم – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة متوسطة	إشراف وتوجيه
١٣.	وزارة المالية	أمن نظام التشغيل – نظام السويفت	درجة المخاطرة متوسطة	إشراف وتوجيه
١٤.	وزارة المالية	مشاركة حساب المستخدم – نظام الدينار العراقي	درجة المخاطرة متوسطة	إشراف وتوجيه
١٥.	وزارة المالية	أمن الدليل النشط (Active Directory) لنظام التشغيل ويندوز سيرفر – نظام سويفت	درجة المخاطرة عالية	إشراف وتوجيه
١٦.	وزارة المالية	برامج مكافحة الفايروسات – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة عالية	إشراف وتوجيه

١٧.	وزارة المالية	الشبكات المحلية و الواسعة (LAN/WAN) – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة	إشراف وتوجيه
١٨.	وزارة المالية	إدارة النسخ الاحتياطية لتطبيقات – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة عالية	دليل إجراءات
١٩.	وزارة المالية	واجهات أنظمة صندوق التنمية للعراق – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة عالية	إشراف وتوجيه

الملاحظات

١. سياسات وإجراءات تقنية المعلومات – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة عالية	دليل إجراءات

الملاحظة:

من خلال مراجعتنا، لاحظنا عدم وجود دليل سياسات وإجراءات موثق لتقنية المعلومات وذلك لإدارة نظم المعلومات والبنية التحتية لتقنية المعلومات.

بدون تطوير سياسات وإجراءات شاملة لتقنية المعلومات، ستجد المؤسسة أنه من الصعوبة أن تدير بشكل فعال ومستمر نشاطات تقنية المعلومات وتسيطر على مخاطر الأعمال المتعلقة بها وتطوير عملياتها اللازمة لتحقيق الأهداف الداخلية والخارجية.

التوصية:

نوصي بتطوير سياسات وإجراءات لتقنية المعلومات وتوثيقها وجعلها متاحة بأيدي الموظفين.

يجب على الإدارة الموافقة على السياسات والإجراءات لضمان مايلي:

- توافق مهام تقنية المعلومات مع أهداف المؤسسة.
- يتم تنفيذ الوظائف التكنولوجية حسب الممارسات المنهجية.

إن السياسات والإجراءات يجب أن تركز وبشكل غير محدد على ما يلي:

- المستخدمين وصلاحيات الدخول.
- اجراءات تعديل البرامج.
- العمليات اليومية والتقارير.
- حل المشاكل التقنية والبرمجية ومحاولة تجنبها.
- صيانة ومراقبة ملفات الدخول.
- التدريب والتعليم.
- عمل النسخة الاحتياطية.
- طرق اختيار وتطوير وصيانة البرمجيات والاجهزة.
- مراقبة الأداء والقدرة على التخطيط.

أن المراجعة المستقلة هي عملية ضرورية لضمان الفهم والتطبيق الصحيح للسياسات والإجراءات.

مراقبة ومتابعة الأعمال المنجزة وذلك لضمان أن العمل المنجز قد تم حسب السياسات والإجراءات الموضوعة.

رد الادارة:

٢. الوصف الوظيفي – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا، لاحظنا عدم وجود دليل رسمي وموثق للتوصيف الوظيفي، والذي يشرح بصورة واضحة مسؤوليات ومهام كل وظيفة وكذلك المؤهلات والمهارات التقنية التي يجب توافرها في الكادر.

بدون تطوير دليل للتوصيف الوظيفي بحيث يتم تحديثه بشكل دوري، سيكون من الصعب على الإدارة توزيع حمل العمل على الأشخاص أو الموظفين المناسبين لتلك الأعمال والذي يؤدي الى التداخل غير المناسب في تنفيذ المهام. بإستمرار عملية تعيين الكوادر من الممكن أن تزيد المشكلة بسبب كون الكادر الجديد لا يمتلك الدراية الكافية بماهو متوقع منه أو المخاطر الناتجة من كونهم ليسو ملائمين للأعمال المناطة بهم، حيث أن ذلك يؤدي الى عدم كفائتهم في تنفيذ المهام.

التوصية:

على الإدارة الأخذ بعين الإعتبار تطوير دليل توصيف للوظائف خاص بدائرة تقنية المعلومات بحيث يشتمل على المهام والمسؤوليات لكل كادر من كوادر الدائرة بالإضافة الى الصلاحيات والمهارات التقنية والمؤهلات العلمية لكل وظيفة وضمان التحديث الدوري للدليل.

رد الادارة:

٣. التدقيق الداخلي لتقنية المعلومات – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة	دليل إجراءات

الملاحظة:

من خلال مراجعتنا، لاحظنا بأنه لايوجد تدقيق داخلي لتقنية المعلومات وذلك لمراجعة النشاطات التي تقوم بها بالإضافة الى ضمان وجود السيطرة الفعالة.

الإدارة قد لا تكون متأكدة من فعالية أداء التدقيق الداخلي في المناطق التي تعتمد على وجود انظمة المعلومات. وكذلك عدم وجود عملية تقييم مستقلة يؤدي الى عدم قدرة الإدارة على ضمان أن برامج ومعدات تقنية المعلومات يتم استخدامها بشكل فعال بحيث يتم المحافظة على سرية البيانات.

التوصية:

يجب ان تأخذ الإدارة بعين الإعتبار تعيين مدقق داخلي لتقنية المعلومات لكي يؤدي مايلي:

- التأكد من التعديلات التي تنفذ على البرامج وعملية الدخول الى البيانات والملفات تتم بصورة مناسبة ومسيطر عليها.
- استخدام نظام متخصص لبيان كفاية وكفاءة المحددات الداخلية.
- مراجعة محددات الدخول المستخدمة لجميع أنظمة تقنية المعلومات وبصورة دورية.
- المشاركة في مراجعة معايير المحددات الداخلية خلال مرحلة تصميم الأنظمة الجديدة، هذه المشاركة تساعد على ضمان تطبيق محددات مناسبة لتلك الأنظمة وكذلك ضمان فحصها وتعديلها بطرق مناسبة وموافق عليها.

رد الادارة:

٤. عملية تغيير المقاييس وتطبيق التعديلات – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة عالية	دليل إجراءات

الملاحظة:

من خلال مراجعتنا على نظامي الدينار العراقي والدولار الأمريكي، لاحظنا أن تغيير المقاييس الخاصة بواجهات وتقارير الأنظمة يتطلب الدخول إلى البرامج لعملها وتعديلها.

بالنظر الى الآلية المتبعة حاليا، يتشكل خطر حدوث خطأ ما في ظل أبسط تغيير في المقاييس الخاصة بواجهات وتقارير الأنظمة يؤثر على البرامج الاساسية والذي يؤدي الى التأثير على كمالية وفعالية وسرية البيانات.

التوصية:

نوصي الإدارة بأن تكون عملية تغيير المقاييس الخاصة بواجهات وتقارير الأنظمة تحت اجراءات رسمية موثقة و كذلك أن يتم عمل آلية لإجراء هذه التغييرات دون الحاجة الى الدخول الى البرامج وذلك لحماية كمالية وفعالية وسرية البيانات.

رد الادارة:

٥. تعديل البرامج – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة عالية	دليل إجراءات

الملاحظة:

فيما يتعلق بتعديل البرامج، لاحظنا ما يلي:

- لا يتم تسجيل التعديلات التي تتم على الانظمة.
- لا يوجد وصف لماهية التعديل.
- لا يوجد معايير لتسمية متغيرات الانظمة.
- لا يتم عمل إصدارات للبرامج.

من دون وجود منهجية لتسجيل التعديلات فإن الإدارة لن تكون قادرة على ضمان ان التعديلات التي تجرى على الانظمة موافق عليها وتم اعتمادها. بألاضافة الى ذلك، مع عدم وجود معايير لتسمية المتغيرات واصدارات للبرامج فإن قسم تكنولوجيا المعلومات سيجد صعوبة في تحديد آخر تعديل أو تحديث تم على الأنظمة.

التوصية:

نوصي بوضع وصف كامل ودقيق فوق كل تعديل يتم على برامج الأنظمة، وهذا سوف يساعد في تسريع عملية تحديد التعديلات. بالأضافة الى ذلك، ينبغي لقسم تكنولوجيا المعلومات أن يأخذ بنظر الاعتبار وضع آلية يتم اتباعها في تسمية متغيرات البرامج وكذلك لعمل إصدارات للبرامج والأنظمة.

رد الادارة:

٦. فصل المهام – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة عالية	موارد بشرية

الملاحظة:

من خلال مراجعتنا لاحظنا أن نفس الشخص الذي يدير قاعدة بيانات ونظام التشغيل هو / هي نفس الشخص الذي يقوم بعمل وطوير الأنظمة.

إن الخطر الموجود من كون كادر تقنية المعلومات من الممكن أن يقوم بعمل تعديلات على الأنظمة غير مصرح لهم القيام بها، حيث أنه من الممكن أن يؤدي الى تعريض أمن وسرية البيانات للخطر.

التوصية:

نوصي الإدارة أن تعمل على ضمان الفصل بين مهام وواجبات مبرمجي الأنظمة والمشرفين على نظم التشغيل ومديري قاعدة البيانات.

رد الادارة:

٧. فصل بيئات التطوير والاختبار للأنظمة – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة عالية	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا لنظامي الدينار العراقي والدولار الأمريكي، لاحظنا أنه لا يتم فصل بيئات التطوير والاختبار ، حيث انه يتم تطوير البرامج الجديدة وفحصها على نفس الجهاز.

من دون الفصل الفعلي لبيئات التطوير والاختبار للأنظمة، البرامج الجديدة من الممكن أن يتم نسخ برامج قديمة عليها بالخطأ بحيث يتم الغاؤها بعد أن تم فحصها واعتمادها، وهذا قد يؤدي الى النتائج التالية:

- وضع وادخال برامج غير معتمدة على الأنظمة.
- ظهور اخطاء في الأنظمة من الصعوبة حلها.

التوصية:

ينبغي على الإدارة إنشاء بيئتين منفصلتين لتطوير البرامج وفحصها، وذلك لضمان الفصل في الأدوار والمسؤوليات بين مطوري الأنظمة ومديري قاعدة البيانات ونظم التشغيل.

رد الادارة:

٨. مراجعة سجلات التدقيق - نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة متوسطة	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا لنظامي الدينار العراقي والدولار الأمريكي، لاحظنا أنه لم يتم تفعيل خاصية التدقيق الخاصة بقاعدة البيانات ونظام التشغيل والمتعلقة بالأنظمة وذلك لتسجيل الحركات التي تتم عليها.

إن تفعيل هذة الخاصية يساعد على كشف التغييرات الغير معتمدة والتي من الممكن أن تحدث على البرامج بحيث تبين من الذي قام بعملية التغيير والتاريخ الذي تمت فيه هذه العملية.

التوصية:

ينبغي للإدارة التأكد من تفعيل خاصية التدقيق الخاصة بقواعد البيانات ونظم التشغيل وذلك لتسجيل التغييرات والأنشطة على التي تتم على الأنظمة.

يعتبر تفعيل التدقيق طريقة فعالة لمراقبة التغييرات وتحديد الغير معتمد منها ومتابعة حالتها.

رد الادارة:

٩. ضوابط كلمة السر – نظام الدينار العراقي	درجة المخاطرة عالية	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا لنظام الدينار العراقي، لاحظنا ما يلي فيما يتعلق بضوابط كلمة السر :

- المستخدمين ليس لديهم الحق في اختيار كلمات السر الخاصة بهم.
- يتم حفظ كلمات السر في قاعدة بيانات بنص واضح.
- كلمات السر غير معقدة.
- كلمة السر غير قابلة للتغيير.
- لا يتم الاحتفاظ بأرشيف كلمة السر.
- ليس هناك تحديد أدنى لطول كلمات السر.

بمرور الزمن، اذا لم يتم تغيير كلمات السر من فترة لأخرى يؤدي ذلك الى فقدانها لفاعليتها وسريتها وبالتالي الى زيادة الفرص لإختراق قاعدة البيانات من قبل أشخاص غير مسموح لهم بدخولها بحيث يصبحوا قادرين على الدخول الى النظام والإطلاع على البيانات.

إن إستخدام كلمات سر بسيطة ومستخدمة سابقا يؤدي الى السهولة النسبية في معرفتها مما يؤثر على فعالية ضوابط الدخول الى النظام والإطلاع على البيانات السرية.

التوصية:

على الإدارة أن تسعى الى تطبيق ما يلي:-

- إجبار المستخدمين تغيير كلمات سرهم الإساسية عند دخولهم الأول الى النظام.
- عمر كلمات السر يجب أن يكون ملائما (شهر أو شهرين) وأن يكون هذا التحديد مقياس لكل المستخدمين.
- تحديد الحد الأدنى لطول كلمات السر (لا يقل عن ستة أحرف، يفضل أن يكون ثمانية أحرف).
- يجب أن تكون كلمات السر معقدة (متكونة من أحرف وأرقام).
- حفظ كلمات السر القديمة في ملف تاريخي في قاعدة البيانات (مثال: كلمات السر الثلاثة الأخيرة)، وذلك لمنع إعادة إستخدام نفس الكلمات السابقة.

بالإضافة الى ذلك، يجب أن يتم لفت انتباه الموظفين من خلال برامج توجيهة أمنية الى الحاجة الى تغيير كلمات السر بشكل فوري في حال اصبحت معروفة من قبل الآخرين.

رد الادارة:

١٠. ضوابط الدخول المتزامن للنظام – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة متوسطة	إشراف وتوجيه

الملاحظة:

خلال مراجعتنا لنظامي الدينار العراقي والدولار الامريكي، لاحظنا أنه لا يوجد محددات للسيطرة على دخولهم الى النظام من خلال اكثر من حاسوب من قبل نفس المستخدم وفي نفس الوقت.

أن قدرة المستخدم على الدخول الى النظام من خلال اكثر من حاسوب وفي نفس الوقت من الممكن أن يزيد من خطورة مشاركة استخدام اسم المستخدم والذي يؤدي الى تعريض سلامة البيانات وسريتها الى الخطر.

التوصية:

على الإدارة منع مشاركة اسم المستخدم من قبل المستخدمين وكذلك منع فتح النظام بنفس اسم المستخدم من خلال اكثر من حاسوب في نفس الوقت الا في الحالات الضرورية التي يفرضها العمل.

رد الادارة:

١١. ضوابط الخروج التلقائي – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا للأنظمة، لاحظنا عدم وجود ضوابط للخروج التلقائي من الأنظمة في حال تركها من دون استخدام فتره معينه من الزمن.

أن عملية ترك النظام مفتوح وفعال من دون استخدام يمكن أن يؤدي الى استخدامه من قبل اشخاص غير مصرح لهم بالدخول الى معلومات النظام مما يعرض سرية المعلومات وسلامتها الى الخطر.

التوصية:

على الإدارة أن تضع ضوابط ملائمة على واجهات النظام، وهذه الضوابط يجب أن تتضمن انهاء تفعيل الواجهات الفعالة بعد فترة محددة من عدم الإستخدام (مثلا ٥ دقائق).

رد الادارة:

١٢. ضوابط اغلاق حساب مستخدم – نظام الدينار العراقي ونظام الدولار الامريكي	درجة المخاطرة متوسطة	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا لنظامي الدينار العراقي والدولار الامريكي، لاحظنا بأن حساب المستخدم لا يتم إيقافه بعد عدد محدد من المحاولات الغير ناجحة للدخول الى النظام.

في غياب عملية إغلاق حساب المستخدم بطريقة تلقائية بعد عدد من محاولات الدخول الغير ناجح للنظام، من الممكن أن يؤدي ذلك الى الدخول غير مسموح به الى الأنظمة.

التوصية:

يجب أن تسعى الإدارة الى التعاون مع قسم تكنولوجيا المعلومات على وضع ضوابط لإغلاق حسابات المستخدمين الذين تجاوزوا العدد المحدد من محاولات الدخول الغير ناجح الى النظام. ويجب أن يشمل هذا التحديد عدد المرات المسموحة للإدخال الخاطىء لكلمة السر (٣ مرات مثلا).

رد الادارة:

١٣. أمن نظام التشغيل – نظام السويفت	درجة المخاطرة متوسطة	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا لنظام التشغيل ويندوز ٢٠٠٣ الخاصة بنظام سويفت، لاحظنا عدم تغيير الحساب الرئيسي الافتراضي لنظام التشغيل ويندوز، وعلاوة على ذلك يتم استخدام هذا الحساب من قبل اثنين من موظفي قسم تقنية المعلومات.

إن استمرار تفعيل الحسابات الافتراضية، قد يؤدي الى تعريض المؤسسة الى المخاطر التالية:

- سهولة دخول الشخص الغير مصرح له للنظام.
- تعريض البيانات المالية الى التغيير بقصد أو بدون قصد.

وبالإضافة الى ذلك، لا تستطيع المؤسسة محاسبة الموظفين المخظئيين في حالة اشتراكهم في استخدام الحسابات الرئيسية الافتراضية.

التوصية:

ينبغي للإدارة النظر في الغاء أو ايقاف تفعيل الحسابات الرئيسية الافتراضية المحددة مسبقا من قبل المزود، وإذا كان ذلك غير ممكن بسبب قيود نظام التشغيل فينبغي إعادة تسمية تلك الحسابات.

رد الادارة:

١٤. مشاركة حساب المستخدم – نظام الدينار العراقي	درجة المخاطرة متوسطة	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا لنظام الدينار العراقي، لاحظنا وجود بعض المستخدمين الذين يتشاركون بنفس اسم المستخدم وكلمة السر. بدون وجود مسؤولية وملكية واضحة لحساب كل مستحدم للنظام فقد تجد الادارة صعوبة في مساءلة المستخدمين الغير مصرح لهم بالدخول.

التوصية:

من أجل إقامة المساءلة، ينبغي للإدارة إنشاء حسابات منفصلة لكل موظف بحاجة للإستخدام النظام.

رد الادارة:

١٥. أمن الدليل النشط (Active Directory) لنظام التشغيل ويندوز سيرفر – نظام سويفت	درجة المخاطرة عالية	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا للدليل النشط لنظام التشغيل ويندوز سيرفر، لاحظنا التالي فيما يتعلق بضوابط كلمة السر:

- خيار اجبار المستخدم على تغيير كلمة السر خلال الدخول الأول غير مفعل.
- خيار اجبار المستخدم على تغيير كلمة السر بشكل دوري غير مفعل.
- كلمة السر غير معقدة.
- لم يتم تحديد الحد الادنى لطول كلمة السر.
- خيار الاحتفاظ بأرشيف كلمات السر لمنع تكرار استخدم كلمة السر غير مفعل.
- لم يتم تحديد الحد الادنى لعمر كلمة السر.
- عدم توقيف الحساب الذي يقوم بعدد من المحاولات الفاشلة للدخول.

التوصية:

يجب أن تسعى الإدارة الى التعاون مع مزودي الأنظمة على تنفيذ ما يلي:

- إجبار المستخدمين على تغيير كلمات السر الإساسية عند دخولهم الأول الى النظام.
- عمر كلمات السر يجب أن يكون ملائما (شهر أو شهرين) وأن يكون هذا التحديد مقياس لكل المستخدمين.
- تحديد الحد الأدنى لطول كلمات السر (لا يقل عن ستة أحرف، يفضل أن يكون ثمانية أحرف).
- يجب أن تكون كلمات السر معقدة (متكونة من أحرف وأرقام).
- حفظ كلمات السر القديمة في ملف تاريخي في قاعدة البيانات (مثال: كلمات السر الثلاثة الأخيرة)، وذلك لمنع إعادة إستخدام نفس الكلمات السابقة.
- اقفال الحساب بعد محدد من المحاولات الفاشلة للدخول (على سبيل المثال ٣ محاولات).
- بالإضافة الى ذلك يجب أن يتم لفت انتباه الموظفين من خلال برامج توجيهة أمنية الى الحاجة الى تغيير كلمات السر بشكل فوري في حال اصبحت معروفة من قبل الآخرين.

رد الادارة:

١٦. برامج مكافحة الفايروسات – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة عالية	إشراف وتوجيه

الملاحظة:

فيما يتعلق ببرامج مكافحة الفيروسات، لاحظنا نقاط الضعف التالية:

- برنامج مكافحة الفيروسات المستخدمة غير مرخصة.
- يتم تحديث تعريفات الفيروسات "يدويا".
- برنامج مكافحة الفيروسات غير محدث بآخر التحديثات.
- جهاز الحاسوب الرئيسي الخاص بنظام سويفت غير محمي ببرنامج مكافحة الفيروسات.

استخدام البرامج غير مرخصة مع نظام التشغيل قد يعرض المؤسسة للمساءلة القانونية.

عدم تحديث برامج مكافحة الفيروسات في الحاسبات يجعل المؤسسة عرضة للاصابة بالفيروسات وبشكل سريع وغير متوقع.

التوصية:

ينبغي على قسم تكنولوجيا المعلومات شراء برامج مكافحة الفيروسات وجعل التحديث لهذه البرامج يتم بشكل تلقائي.

يجب وضع جدول زمني منتظم يتم بشكل تلقائي لتنفيذ فحص أجهزة الحاسبات وبشكل دوري.

رد الادارة:

١٧. الشبكات المحلية و الواسعة (LAN/WAN) – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة متوسطة	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا، لاحظنا عدم وجود شبكات محلية وواسعة لربط الأنظمة الخاصة بصندوق التنمية للعراق.

في غياب الشبكة المحلية والواسعة، سيؤدي ذلك الى التأخير في تنفيذ العمل بسبب الترحيل اليدوي للحركات المالية. بالإضافة الى ذلك، قد تواجه المؤسسة زيادة تكلفة نقل البيانات والمخاطرة بسرية البيانات بسبب الوضع الحالي في العراق.

التوصية:

ينبغي للإدارة أن تأخذ بنظر الاعتبار إنشاء شبكات محلية وواسعة لتوفير الاتصال بين دوائر المؤسسة وفروعها، حيث أن ذلك يساعد على تناقل المعلومات بصورة سريعة.

إن إنشاء هذه الشبكة سيزيد من فعالية عملية الرقابة والسيطرة وكذلك تقليل الوقت المستهلك لنقل وتجميع البيانات المالية.

رد الادارة:

١٨. إدارة النسخ الاحتياطية لتطبيقات – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة عالية	دليل إجراءات

الملاحظة:

عند فحص الضوابط لتي تحيط بعملية إجراء النسخ الاحتياطية من الأنظمة، لاحظنا ما يلي:

- لا يوجد إجراء رسمي موثق يتم إتباعة للقيام بعملية اجراء النسخ الاحتياطية.
- لا يوجد جدول زمني محدد للقيام بعملية عمل النسخ الاحتياطية.
- فيما يخص نطامي الدينار العراقي والدولار الامريكي، لا يتم نقل النسخ الاحتياطية الى مواقع خارجية وأمينة معتمدة من قبل الإدارة، وعوضا عن ذلك يتم حفظها على ذاكرات فلاش بحيث تبقى مع مستخدمي الأنظمة.
- فيما يخص نظام سويفت، يتم عمل النسخ الاحتياطية بشكل اسبوعي على قرص صلب بحيث يتم الاحتفاظ به مع الشركة التي طورت النظام..
- عدم الاحتفاظ بسجل تاريخي للنسخ الاحتياطية
- لا يتم تشفير بيانات النسخ الاحتياطية.

عدم وجود فحص دوري للنسخ الاحتياطية وذلك لضمان سلامة البيانات.

التوصية:

يجب على قسم تكنولوجيا المعلومات وضع سياسات وإجراءات موثقة بحيث تشتمل تعليمات عمل النسخ الاحتياطية بشكل دوري وبجدول زمني محدد، بالإضافة الى ما يلي:

- يجب أن يتم تخزين النسخ الاحتياطية في مكان آمن، ويجب أن يتم تخزين نسخة أخرى خارج المؤسسة الى منطقة آمنة ومعتمدة من قبل الادارة.
- عمل سجل تاريخي للنسخ الاحتياطية والاحتفاظ بها.
- التأكد من تشفير النسخ الاحتياطي.
- إجراء فحص دوري للنسخ الاحتياطية وذلك للتأكد من أن النسخ تم عملها بصورة صحيحة وسليمة.

رد الادارة:

١٩. واجهات أنظمة صندوق التنمية للعراق – انظمة الدينار العراقي والدولار الأمريكي والسويفت	درجة المخاطرة عالية	إشراف وتوجيه

الملاحظة:

من خلال مراجعتنا، لاحظنا عدم وجود وجهات تقوم بربط نظامي الدينار العراقي والدولار الامريكي مع نظام سوفيت.
المؤسسات المالية تميل إلى الاعتماد على واجهات الربط الآلي بين الأنظمة لتوفير التكامل التام بينها مع التقليل من التدخل اليدوي.
بدون وجود واجهات ربط الآلي ما بين الأنظمة، ربما تتعرض المؤسسة الى مخاطر الأخطاء البشرية الناجمة عن العمليات اليدوية.
وعلاوة على ذلك، سيؤدي ذلك الى زيادة الوقت اللازم لتنفيذ العمل والكلفة والشكوك حول دقة البيانات المدخلة.

التوصية:

ينبغي على المؤسسة أن تأخذ بعين الإعتبار تطوير واجهات ربط آلية وذلك لربط جميع الأنظمة وذلك للتقليل من مخاطر الخطأ البشري وتوفير الوقت والتكلفة وتحسين فعالية العمل.

رد الادارة:

إرنست ويونغ

خدمات التدقيق والضرائب والمعاملات والاستشارات

عن إرنست ويونغ

تعتبر إرنست ويونغ أحدى المؤسسات الرائدة على مستوى العالم في مجالات التدقيق والضرائب والمعاملات والاستشارات، حيث تضم إرنست ويونغ عدد كبير من الموظفين يصل الى ١٤٤.٠٠٠ تجمعهم مجموعة من القيم المشتركة والالتزام الشديد بالجودة.

تحدث إرنست ويونغ الفرق من خلال مساعدة كوادرها وعملائها والمجتمعات الأوسع نطاقا على تحقيق أهدافهم وصقل إمكاناتهم .

تعتبر إرنست ويونغ عضوا في مؤسسة إرنست ويونغ العالمية المحدودة، ولكل منهما كيانا قانونية منفصلا. ومؤسسة إرنست ويونغ العالمية المحدودة هي شركة محدودة بضمان وتعمل بالمملكة المتحدة ولا تقدم خدمات الى العملاء.لمزيد من المعلومات عن مؤسستنا يرجى زيارة موقعنا الالكتروني:www.ey.com.

تعود أعصال إرنست ويونغ في الشرق الأوسط إلى عام ١٩٢٣. على امتداد أكثر من ٨٥ سنة، نمت مؤسستنا وتطورت لتلبية الاحتياجات والتطورات القانونية والتجارية في المنطقة. لدينا عبر الشرق الأوسط أكثر من ٤.٢٠٠ فرد يتعاونون معا من خلال ٢٠ مكتبا في ١٥ دولة عربية، يتقاسمون ذات القيم والالتزام الشديد بالجودة. نحن نحدث الفارق من خلال مساعدة فريقنا وعملائنا ومجتمعاتنا في تحقيق وتوظيف إمكاناتهم.

لمزيد من المعلومات يرجى زيارة الموقع الالكتروني:www.ey.com/me

هكذا نحدث الفرق في إرنست ويونغ