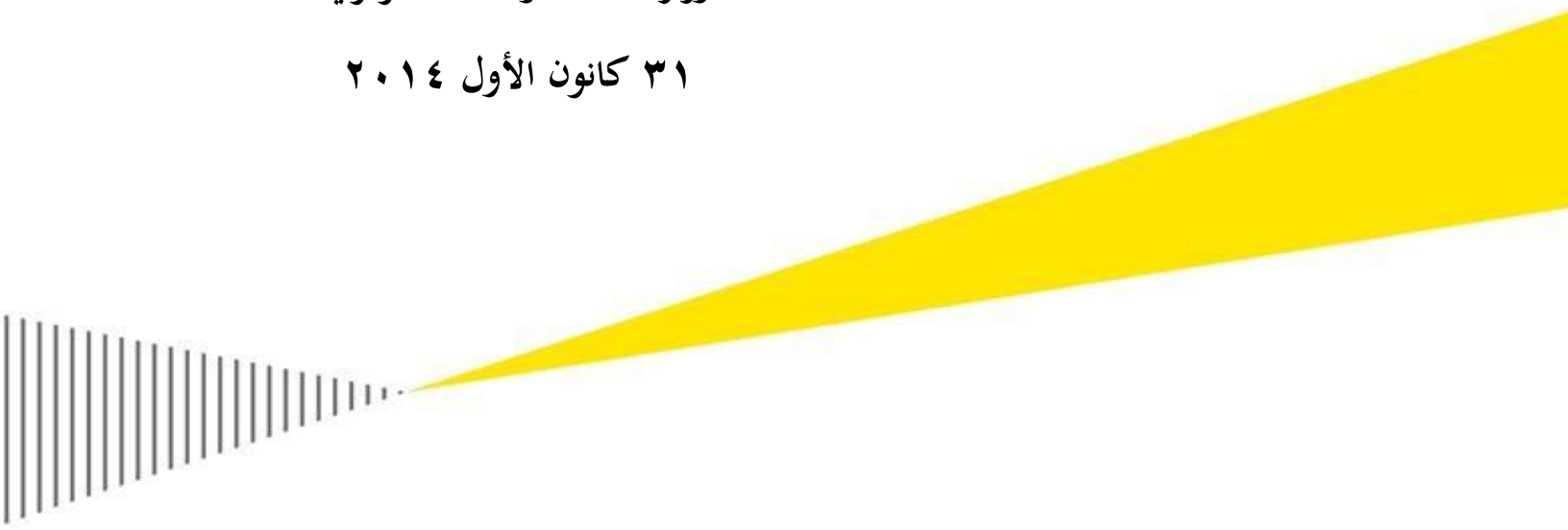
صندوق التنمية للعراق والحساب اللاحق

مذكرة الأمور الظاهرة من عملية تدقيق نظام المعلومات

(الملاحظات الجديدة)

وزارة المالية والبنك المركزي

٣١ كانون الأول ٢٠١٤



EY

نبني عالماً أفضل للعمل

إرنست و يونغ
صندوق بريد ٦٠٠٤
منزل ٢٣، شارع ٣ (شارع الأميرات) حي ٦٠٩،
حي المنصور، بغداد، العراق

هاتف: ٠٣٥٧ ٥٤٣ ١ ٩٦٤+
فاكس: ٩٨٥٨ ٥٤٣ ١ ٩٦٤+
baghdad.iraq@iq.ey.com
ey.com/mena

١٥ كانون الأول ٢٠١٥

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

تحية طيبة وبعد،

لقد قمنا بتدقيق نظام المعلومات في وزارة المالية والمؤسسات التابعة لها. ويسرنا أن 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 والحساب اللاحق سواء كانت إيرادات أو 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 والحساب اللاحق.
٢. **نظام الدولار الأمريكي**: وقد تم تطويره بإستخدام برنامج مايكروسوفت أكسس، ويستخدم لتسجيل جميع الحركات المالية التي تتم بالدولار الأمريكي الخاصة بصندوق التنمية للعراق والحساب اللاحق.

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

المذكرة المرفقة تتضمن اقتراحات لتحسين تكنولوجيا المعلومات ومحددات السرية المتعلقة بها والتي لفتت إنتباهنا أثناء مراجعتنا لنظم المعلومات المختارة والمتعلقة بصندوق التنمية للعراق والحساب اللاحق للسنة المنتهية في ٣١ كانون الأول ٢٠١٤.
إن مراجعتنا للأنظمة التي قمنا بإختيارها يهدف إلى 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 أن تشمل جميع التحسينات الممكنة لكافة نقاط الضعف القائمة.

سيكون من دواعي سرورنا أن نقوم بمناقشة هذه التوصيات معكم و كذلك مساعدتكم في تنفيذها.

ختاماً، 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 ، ، ، ،

Ernst + Young

إرنست ويونغ/ العراق

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 إتخاذ إجراءات معالجة فورية.
درجة المخاطرة متوسطة	تتعلق الملاحظة بالأمور متوسطة الخطورة و التي قد تؤدي إلى ضعف في نظام الرقابة الداخلي و/أو كفاءة الأنشطة التشغيلية والتي يجب أن يتم 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 التشغيلية، ولكن يجب الإهتمام بها من قبل الإدارة. نوصي بإتخاذ إجراءات معالجة خلال فترة معقولة.

رقم الصفحة	المؤسسة	الملاحظة	درجة المخاطرة
٢	وزارة المالية/ البنك المركزي	تقنية شبكة تكنولوجيا المعلومات – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	**درجة المخاطرة عالية**
٣	البنك المركزي	دعم خدمات نظام التشغيل – نظام السويفت	**درجة المخاطرة عالية**
٤	وزارة المالية/ البنك المركزي	الضوابط البيئية والمادية في غرف السيرفرات – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	**درجة المخاطرة عالية**
٦	البنك المركزي	سرية قاعدة البيانات – نظام المدفوعات والمقبوضات	**درجة المخاطرة عالية**
٧	البنك المركزي	ضوابط الدخول المتزامن للنظام – نظام المدفوعات والمقبوضات	**درجة المخاطرة متوسطة**
٨	البنك المركزي	مشاركة حساب المستخدم – نظام المدفوعات والمقبوضات	**درجة المخاطرة عالية**
٩	وزارة المالية/ البنك المركزي	ضوابط كلمة السر لنظام التشغيل ويندوز – أنظمة الدينار العراقي، والدولار الامريكي، والمدفوعات والمقبوضات، سويفت	**درجة المخاطرة عالية**

الملاحظات

١. تقنية شبكة تكنولوجيا المعلومات – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية

الملاحظة:

لقد لاحظنا أن كل الحواسيب مرتبطة بالسيرفر عن طريق تقنية شبكة مجموعة العمل (Workgroup Network Technology) بدلاً من إستخدام تقنية وحدة التحكم بالشبكة (Domain Controller Technology) للسيطرة وإدارة المستخدمين المخولين والحواسيب المرتبطة بالسيرفر من خلال بناء وتفعيل الدليل النشط (Active Directory).

الإدارة قد تجد صعوبة في تطبيق السياسات الأمنية على الأجهزة المرتبطة بالشبكة، مثل سياسة كلمة المرور وسياسة تدقيق حواسيب المستخدمين بسبب إستخدام تقنية شبكة مجموعة العمل اللامركزية (Workgroup Network Technology).

وعلاوة على ذلك، قد تجد الإدارة صعوبة في تتبع ومعرفة الأنشطة الغير مصرح بها وذلك لأن تقنية شبكة مجموعة العمل (Workgroup Network Technology) ليس لديها سيرفر مخصص لها لتتبع أنشطة المستخدمين وأي عمل يتم عبر جهاز المستخدم بواسطة الشبكة المحلية (LAN)، وهذا يشمل مشاركة الملفات وسجلات الدخول للمستخدمين.

التوصية:

يجب على الإدارة ضمان عدم تشغيل الحواسيب والسيرفرات في بيئة شبكة مجموعة العمل (Workgroup Network)، والعمل على تطبيق تقنية وحدة التحكم بالشبكة (Domain Controller Technology) وذلك لإدارة جميع الحواسيب السيرفرات وحسابات المستخدمين بشكل فعال.

رد الإدارة:

٢. دعم خدمات نظام التشغيل – نظام السويفت	درجة المخاطرة عالية

الملاحظة:

استناداً إلى مراجعتنا لحواسيب نظام سويفت، لاحظنا أن هذه الحواسيب تعمل على نظام التشغيل ويندوز اكس بي المنتهي الصلاحية (Windows XP)، والذي هو حالياً خارج الدعم من قبل شركة مايكروسوفت ولا يتم تسويقه.

لا يمكن للمؤسسة الحصول على دعم من أي موزع لمايكروسوفت في السوق في حالة حدوث مشاكل فنية في نظام التشغيل. وعلاوة على ذلك، قد تتعرض المؤسسة إلى مخاطر إستغلال الثغرات الأمنية المعروفة في الأنظمة الغير محمية بشكل كاف من خلال تحديث وتصحيح نظام التشغيل أو الأنظمة الغير محمية.

التوصية:

ينبغي على قسم تكنولوجيا المعلومات التوقف عن إستخدام تقنيات غير معتمدة أو منتهية الصلاحية تسويقياً. أيضا، يجب على قسم تكنولوجيا المعلومات التأكد من تحديث أنظمتهم بأحدث الإصدارات.

رد الإدارة:

٣. الضوابط البيئية والمادية في غرف السيرفرات – انظمة الدينار العراقي، والدولار الأمريكي، المدفوعات والمقبوضات، والسويفت	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا لغرف السيرفرات المخصصة لأنظمة صندوق التنمية للعراق، لاحظنا الأمور التالية:

- فيما يتعلق بنظامي الدينار العراقي والدولار الأمريكي:
  - السيرفرات موضوعة في غرف مكاتب الموظفين، حيث أن الوصول إليها متاح من قبل أي موظف أو زائر.

- فيما يتعلق بنظام المدفوعات والمقبوضات:
  - لا يوجد أي دليل على اختبارات دورية تجرى على مطافئ الحريق.
  - عدم وجود جهاز الكشف عن النار والماء والرطوبة.
  - لا توجد إنارة احتياطية في حالات الطوارئ.
  - عدم وجود كاميرات لمراقبة غرفة السيرفرات.
  - هناك جهاز دخول عن طريق المسح الضوئي لبصمة المستخدم المخول أو البطاقة التعريفية للمستخدم مثبت على بوابة غرفة السيرفرات، لكن لاحظنا عدم الالتزام بالدخول عن طريق الماسح الضوئي أو البطاقة التعريفية، حيث يتم ترك الباب مفتوحاً لدخول أي من الموظفين، علما بأن الباب كان مفتوحاً أثناء زيارتنا.
  - لا يتم الاحتفاظ بسجلات الدخول للزوار.
  - غرفة السيرفرات محاطة بالنوافذ الزجاجية.
  - لا يوجد مكيف هواء احتياطي مرتبط بالطاقة الكهربائية الاحتياطية للحالات الطارئة.

- فيما يتعلق بتطبيق سويفت:
  - أرضية غرفة السيرفرات غير مرتفعة.
  - طفايات الحريق منتهية الصلاحية وتحتاج الى تعبئة وصيانة دورية، بالإضافة إلى عدم وجود دليل على وجود اختبارات دورية تتم عليها.
  - لا توجد إنارة احتياطية في حالات الطوارئ.
  - عدم وجود كاميرات لمراقبة غرفة السيرفر.
  - لا يتم الإحتفاظ بسجلات الدخول للزوار.
  - عدم وجود بطاقة دخول أو مفتاح للدخول إلى غرفة السيرفرات.
  - لا يوجد مكيف هواء احتياطي مرتبط بالطاقة الكهربائية الاحتياطية للحالات الطارئة.

إن وجود السيرفرات على نفس المستوى من الأرض تزيد من إحتمالية تعطلها في حال حدوث فيضانات أو تسريب مياه.
إن عدم وجود أنظمة كشف الحرائق داخل مركز البيانات تزيد من خطورة الإصابة التي قد يتعرض لها الأفراد في الداخل وبالإضافة الى الخطورة على أجهزة الحاسوب.
قد لا تكون الإدارة قادرة على التأكد من أن طفايات الحريق ستعمل بصورة صحيحة في حال عدم اجراء فحص دوري عليها.
في حال عدم وجود كاميرات متصلة في غرفة السيرفرات، فإن الإدارة لن تكون قادرة على مراقبة وتسجيل أي حركات مشبوه أو أضرار قد تحدث على موجودات غرفة السيرفرات.
في حال عدم وجود ضوابط للسيطرة على دخول الزوار إلى مركز البيانات، قد يحدث دخول غير مصرح به إلى أنظمة المؤسسة، بالإضافة إلى احتمالية حدوث عمليات احتيال وعبث في بيانات ومعلومات سرية.
عدم وجود جهاز كشف تسرب المياه قد يؤدي إلى تعطل وتلف الاجهزة الموجودة في غرفة السيرفرات.

التوصية:

ينبغي على الإدارة تعزيز الضوابط المادية والبيئية في مركز البيانات وأن تأخذ بعين الاعتبار توفير الأمور التالية:

- التأكد من أن أرضية غرفة السيرفرات مرتفعة بشكل صحيح.
- تركيب الإضاءة الاحتياطية.
- تركيب جهاز كشف الحرائق وأنظمة اخماد الحريق.
- عمل فحص دوري لطفايات الحريق.
- تركيب كاميرات مراقبة داخل غرفة السيرفرات.
- عمل سجل دخول لمركز البيانات بحيث يتم تسجيل جميع الزيارات التي تتم للمركز. وينبغي الإحتفاظ السجل ومراجعته بشكل دوري.
- تركيب جهاز تسرب المياه.
- ضمان عدم وجود أي شبابيك زجاجية في غرفة السيرفرات.
- يجب أن تكون وحدة الطاقة الاحتياطية (UPS) كافية لإعطاء الوقت اللازم لإغلاق الأجهزة بشكل سليم في حال حدوث انقطاع في التيار الكهربائي.
- التأكد من نظام التكييف الهوائي يعمل في جميع الأوقات وذلك للحفاظ على درجة حرارة مناسبة في غرفة السيرفرات.

رد الإدارة:

٤. سرية قاعدة البيانات – نظام المدفوعات والمقبوضات	درجة المخاطرة عالية

الملاحظة:

خلال عملية مراجعتنا لمحددات قاعدة بيانات نظام المدفوعات والمقبوضات، لاحظنا بأن الـ "Database Listener" غير محمية بكلمة سر، وكذلك الرقم الأساسي الأولي الخاص بالـ "Listener Port" لم يتم تغييره، حيث أن ذلك من الممكن أن يؤدي إلى تعريض قاعدة بيانات إلى الإختراق والخطر.

التوصية:

نوصي بأن يتم حماية الـ "Database Listener" وذلك بأن يتم عليها تطبيق كلمة سر وتشفيرها وكذلك تغيير الرقم الأساسي الخاص بالـ "Listener Port".

رد الإدارة:

٥. ضوابط الدخول المتزامن للنظام – نظام المدفوعات والمقبوضات	درجة المخاطرة متوسطة

الملاحظة:

خلال مراجعتنا لنظام المدفوعات والمقبوضات، لاحظنا أنه لا يوجد محددات للسيطرة على دخولهم الى النظام من خلال أكثر من حاسوب من قبل نفس المستخدم وفي نفس الوقت.

إن 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 إلى 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 أكثر من حاسوب في نفس الوقت إلا في الحالات الضرورية التي يفرضها العمل.

رد الإدارة:

٦. مشاركة حساب المستخدم – نظام المدفوعات والمقبوضات	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا لنظام المدفوعات والمقبوضات، لاحظنا وجود بعض المستخدمين الذين يتشاركون بنفس اسم المستخدم وكلمة السر للدخول للعمل على النظام.

بدون وجود مسؤولية وملكية واضحة لحساب كل مستخدم للنظام فقد تجد الإدارة صعوبة في مساءلة المستخدمين الغير مصرح لهم بالدخول.

التوصية:

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

رد الإدارة:

٧. ضوابط كلمة السر لنظام التشغيل ويندوز – أنظمة الدينار العراقي، والدولار الأمريكي، والمدفوعات والمقبوضات، سويفت	درجة المخاطرة عالية

الملاحظة:

من خلال مراجعتنا لأنظمة التشغيل ويندوز والخاصة بالحواسيب المتعلقة بأنظمة صندوق التنمية للعراق، لاحظنا الأمور التالية فيما يتعلق بضوابط كلمة السر:

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

التوصية:

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

- إجبار المستخدمين على تغيير كلمات السر الأساسية عند دخولهم الأول إلى النظام.
- عمر كلمات السر يجب أن يكون ملائماً (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.
- إقفال الحساب بعد محدد من المحاولات الفاشلة للدخول (على سبيل المثال ٣ محاولات).
- بالإضافة إلى ذلك يجب أن يتم لفت انتباه الموظفين من خلال برامج توجيهة أمنية إلى الحاجة إلى تغيير كلمات السر بشكل فوري في حال اصبحت معروفة من قبل الآخرين.

رد الإدارة:

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 إلى ١٩٠,٠٠٠ تجمعهم مجموعة من القيم المشتركة والالتزام الشديد بالجودة.

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

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

تعود أعمال 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 معاً من خلال ٢٠ مكتباً 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