أنا الموظف /

من إدارة / قسم /

اطلعت على التالي :-

١- تعميم رقم٣٨٤٨٤٦٢٤ بتاريخ ١٤٣٨/٣/٢٠هـ عدد صفحات (٢)

٢- سياسة تنظيم استخدام الحاسب الآلي والشبكات الخاصة بأجهزة الإدارة العامة للتعليم عدد صفحات (٦)

٣- سياسة عدم افشاء المعلومات والبيانات عدد صفحات (٤)

٤-)Password Policy(سياسة كلمات المرور) وعدد الصفحات(٦)

٥- اتفاقية نظام نور و عدد الصفحات (١)

كما أني سأقوم بتغيير كلمة المرور الخاصة بحسابي على الشبكة بكلمة صعبة التخمين حسب السياسات التي تم الاطلاع عليها.

وعلى ذلك جرى التوقيع.

الاسم /

العمل الحالي /

رقم الجوال /

البريد الإلكتروني /

ختم الجهة الإدارية

ملاحظة : يتم التوقيع على كل ورقة على حدة

اتفاقية الاستخدام المقبول لنظام نور Acceptable Use agreement for Noor System

حماية لموثوقية المعلومات فإن جميع مستخدمي أنظمة المعلومات في وزارة التعليم والمستفيدين من خدماتها، ملزمين بشكل عام بسياسات تقنية المعلومات وسياسات أمن المعلومات، بالإضافة إلى ذلك تأكد هذه الاتفاقية على وجوب التزام مستخدمي نظام نور بالشروط التالية:

- استخدام انظمة المعلومات يجب ان يتوافق مع ما هو مصرح به حسب لوائح الوزارة واللوائح الحكومية.
- يتحمل المستخدم المسؤولية الكاملة عن جميع التعاملات الصادرة عن استخدام صلاحيات الدخول الممنوحة له.
- يتوجب عدم محاولة الدخول او الاستخدام الغير مصرح به الى مصادر وأنظمة المعلومات في الوزارة مالم تكن الصلاحيات المطلوبة ممنوحة نظام.
- يتوجب عدم إفشاء معلومات الحسابات أو مشاركة كلمات المرور أو الرموز السرية مهما كانت الاسباب، ويجب الابلاغ عن أي استخدام أو تغير مشكوك فيه يطرأ عليها.
- يجب على المستخدم التأكد من اختيار كلمات سر صعبة التخمين كأن تكون خليط من الحروف الكبيرة والصغير والارقام والا يقل طولها عن ٦ خانات.
- الالتزام بتسهيل مهام الحسابات الفرعية التي لها ارتباط جزئي او كلي بهذا الحساب.
- وجوب ابلاغ (الادارة العامة لأمن المعلومات) عن أي حالة استغلال غير مصرح به لأنظمة ومعلومات الوزارة أو حالات الاختراق مما يصل الى علم المستخدم.
- يحكم هذه الاتفاقية وتفسير بنودها وفقا لقوانين المملكة العربية والسعودية.

أنا الموقع أدناه، اتعهد وألتزم بالسياسة أعلاه بشأن الاستخدام المقبول لنظام نور، كما أعلم أن أي انتهاك للوائح المذكورة أعلاه يعتبر غير أخلاقي ويمكن أن يشكل جريمة جنائية، وفي حال ارتكبت أي مخالفة أو سوء استخدام متعمد للخدمات التي يقدمها النظام، سيتم اتخاذ الإجراءات القانونية المناسبة بحقي.

(تعميم)

للمساعدين ومديري ومديرات الإدارات

تجدون برفقه صورة من تعميم معالي وزير التعليم رقم ٣٨٤٨٤٦٢٤ في ١٤٣٨/٣/٢٠هـ المبني على برقية سعادة مدير عام المركز الوطني للوثائق والمحفوظات المكلف رقم ١/٢٢٤ في ١٤٣٨/٣/٨هـ المبني على القرار رقم ٥٥ في ١٤٣٧/١٠/١٥هـ بشأن الموافقة على اللائحة التنفيذية لنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها.

لذا نأمل الإحاطة والعمل بموجبه.

والسلام عليكم ورحمة الله وبركاته

المدير العام للتعليم بالمنطقة الشرقية

١٤٣٨/٣/٢٧

د. عبد الرحمن بن إبراهيم المديرس

الهاتف: ٨٢٧٣٦٦٦ (٣٠٢/٣٠١) المباشر/الفاكس: ٨٢٧٢٦٣١ البريد الإلكتروني: office15@edueast.gov.sa

المملكة العربية السعودية
وزارة التعليم

(٢٨٠)

وزارة التعليم
Ministry of Education

الادارة العامة للاتصالات الادارية
الرقم : ٣٨٤٨٤٦٢٤
التاريخ : ١٤٣٨/٠٣/٢٠
المرفقات : ٣

تعميم

لجميع الجامعات وقطاعات الوزارة (التعليم العام والتعليم الجامعي وإدارات التعليم بالمناطق والمحافظات)

معالي ..... وفقه الله

سعادة ..... وفقه الله

السلام عليكم ورحمة الله وبركاته.

تلقينا برقية سعادة مدير عام المركز الوطني للوثائق والمحفوظات المكلف رقم ١/٢٢٤ وتاريخ ١٤٣٨/٣/٨هـ (المرفق نسخة منها ومشفوعها) نسخة من القرار رقم (٥٥) وتاريخ ١٤٣٧/١٠/١٥هـ بشأن الموافقة على اللائحة التنفيذية لنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها.

آمل الاطلاع والتقيد به وإبلاغه لمن يلزم بالعمل بموجبه .

وتقبلوا أطيب تحياتي وتقديري ،،،

وزير التعليم

د. أحمد بن محمد العيسى

وزارة التربية والتعليم
صورة طبق الأصل
الإدارة العامة لمركز الاتصالات الإدارية

الإدارة العامة للاتصالات الإدارية
الرقم : ٣٨٤٨٤٦٢٤
التاريخ : ١٤٣٨/٠٣/٢٠
المرفقات : ٣

١/٢/٣٧

تعميم

لجميع الجامعات وقطاعات الوزارة (التعليم العام والتعليم الجامعي وإدارات التعليم بالمناطق والمحافظات)

معالي ..... وفقه الله

سعادة ..... وفقه الله

السلام عليكم ورحمة الله وبركاته.

تلقينا برقية سعادة مدير عام المركز الوطني للوثائق والمحفوظات المكلف رقم ١/٢٢٤ وتاريخ ١٤٣٨/٣/٨هـ (المرفق نسخة منها ومشفوعها) نسخة من القرار رقم (٥٥) وتاريخ ١٤٣٧/١٠/١٥هـ بشأن الموافقة على اللائحة التنفيذية لنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها.

آمل الاطلاع والتقيد به وإبلاغه لمن يلزم بالعمل بموجبه .

وتقبلوا أطيب تحياتي وتقديري ،،،

وزير التعليم

د. أحمد بن محمد العيسى

وزارة التربية والتعليم
صورة طبق الأصل
الإدارة العامة للاتصالات الإدارية والمالية
الرقم: 70840
التاريخ: 20 / 03 / 1438
المرفقات: لا توجد

صورة لمكتبنا .

صورة للإدارة العامة للشؤون القانونية مع الأساس .

٩- ٢٨١

الرقم: ٧٢١
التاريخ: ١٤٣٨/ ٢٨٩هـ

الديوان الملكي
المركز الوطني للوثائق و المحفوظات
رقم الصادر : ١/٢٢٤
تاريخ الصادر : ١٤٣٨/٠٣/٠٨
المرفقات :

بسم الله الرحمن الرحيم

المملكة العربية السعودية
الديوان الملكي
المركز الوطني للوثائق والمحفوظات

(٠٧٧)

الموضوع : تبليغ اللائحة التنفيذية لنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها.

معالي وزير التعليم **سلمه الله**

السلام عليكم ورحمة الله وبركاته،

تنفيذاً للمادة (١١) نظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها الصادر بالمرسوم الملكي رقم (م/٣٥) وتاريخ ١٤٣٢/٥/٨هـ، فقد أصدرت هيئة المركز الوطني للوثائق والمحفوظات قرارها رقم (٥٥) وتاريخ ١٤٣٧/١٠/١٥هـ، بالموافقة على **اللائحة التنفيذية لنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها.**

أبعث لكم نسخة من تلك اللائحة وقرار اعتمادها؛ لإبلاغ الجهات التابعة لكم أو المرتبطة بكم للعمل بموجبها.

ولمعاليكم خالص تحياتي وتقديري ،،،

مدير عام
المركز الوطني للوثائق والمحفوظات المكلف

د. فيصل بن عبدالعزيز التميمي

وزارة التعليم
Ministry of Education
الإدارة العامة لمكتب الوزير
الرقم: 70840
التاريخ: 1438/03/09
المرفقات: لا يوجد

بسم الله الرحمن الرحيم

المملكة العربية السعودية
الديوان الملكي

الرقم :
التاريخ :
المرفقات :

المركز الوطني للوثائق والمحفوظات

قرار رقم (٥٥) وتاريخ ١٥/ ١٠ / ١٤٣٧هـ

إن هيئة المركز الوطني للوثائق والمحفوظات بناءً على المادة (الرابعة/٣) من نظام المركز الوطني للوثائق والمحفوظات المتضمنة أن هيئة المركز تختص بإصدار اللوائح التنفيذية لنظام الوثائق والمحفوظات، وبناءً على المادة (١١) من نظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها التي تنص على أن يصدر المركز اللائحة التنفيذية للنظام، وبناءً على محضر هيئة المركز الوطني للوثائق والمحفوظات رقم (٤٨) وتاريخ ١٤٣٧/٥/٩هـ، الذي تمت فيه الموافقة على اللائحة التنفيذية لنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها.

وبناءً على مقتضيات المصلحة العامة.

تُقرر ما يلي:-

١- الموافقة على اللائحة التنفيذية لنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها.
٢- تبلغ الأجهزة الحكومية بنسخة من هذه اللائحة.
٣- على مدير عام المركز الوطني للوثائق والمحفوظات إنفاذ ذلك.

رئيس الديوان الملكي

رئيس هيئة المركز الوطني للوثائق والمحفوظات

خالد بن عبدالرحمن العيسى

بسم الله الرحمن الرحيم

المملكة العربية السعودية
الديوان الملكي

الرقم :
التاريخ :
المرفقات :

المركز الوطني للوثائق والمحفوظات

اللائحة التنفيذية لنظام عقوبات نشر الوثائق والمعلومات السرية وإفشائها

المادة الأولى : على كل موظف عام أو من في حكمه أسندت إليه مهمات متصلة بالوثائق السرية ثم نُقلت خدمته أو انتهت علاقته وظيفياً بالجهة التي يعمل بها أو انقطعت علاقته بتلك المهمات؛ أن يُسلم الجهة ما لديه من وثائق سرية بموجب نموذج يبين ذلك . وعلى الجهة ألا تخلي طرفه إلا بعد استلام تلك الوثائق.

المادة الثانية : مع عدم الإخلال بأحكام المساءلة التأديبية، يوقف أي موظف عام أو من في حكمه، يقوم أو يشتبه بقيامه بنشر وثيقة سرية أو إفشاء معلومة سرية متعلقة بعمله، عن مزاولة أي مهام تتعلق بالوثائق السرية، وذلك إلى حين استكمال إجراءات المساءلة التأديبية.

المادة الثالثة : عند فقدان أو تسريب وثيقة سرية أو ثبوت إفشاء معلومة سرية؛ تتخذ الجهة الإجراءات الآتية :

١- تحرير محضر بالواقعة يتضمن إيضاح يوم اكتشافها وتاريخه وساعته ومعلومات عنها وأي معلومة إيضاحية أخرى.
٢- إبلاغ جهة التحقيق المختصة نظاماً عن الواقعة خلال (٢٤) ساعة من تحرير المحضر.

المادة الرابعة : في حالة العثور على الوثيقة السرية المفقودة ، يحرر محضر بذلك وتعاد - بموجب محضر- إلى الجهة التي فقدت منها.

المادة الخامسة : تنشر هذه اللائحة في الجريدة الرسمية، وتصبح نافذة من تاريخ نشرها.

اتفاقيات

سياسة استخدام التجهيزات التقنية و التطبيقات

النسخة (١) -١٤٣٥هـ ، ٢٠١٤م

- لائحة تنظيم استخدام الحاسب الآلي والشبكات.
- سياسة عدم افشاء المعلومات و البيانات.
- سياسة المراسلات المباشرة(Instance Messaging IM) .
- سياسة الإجتماعات المرئية و عن بعد(Video Conferencing) .
- سياسة التواصل الاجتماعي (Social Networking).
- سياسة برامج رسائل الجوال القصيرة (SMS).
- سياسة كلمات المرور (Password Policy).
- أهمية استخدام سياسة كلمة مرور فعالة.

تاريخ بدء تطبيق الإتفاقية / / ١٤ هـ

تم اعتمادها من قبل: إدارة تقنية المعلومات – إدارة الشؤون القانونية – إدارة المتابعة- إدارة القضايا التربوية - ادارة الشؤون الإدارية و المالية.

سياسة تنظيم استخدام الحاسب الآلي والشبكات الخاصة بأجهزة الإدارة (العامة) للتربية والتعليم

آخر تحديث تم بتاريخ ١٤٣٥/٨/٢٨هـ الموافق ٢٠١٤/٦/٢٦م.

أولاً : أينما وردت العبارات التالية في هذه اللائحة فيقصد بها المعاني الموضحة أمام كل منها :

١/١ : الإدارة - الإدارة العامة للتربية والتعليم بالمنطقة الشرقية .

١/٢ : المستخدم – كل من يستخدم أجهزة أو معدات الحاسب الآلي والبرامج الحاسوبية التابعة للإدارة سواء داخل مباني الإدارة أو خارجها (مباني إدارية أو مدارس) ويشمل ذلك الموظفين وغيرهم ممن يعملون لحساب الإدارة بأجر أو بدون .

١/٣ : الحاسب الآلي – كل جهاز حاسب آلي قامت الإدارة بتوفيره في جميع المدارس والإدارات والأقسام والمكاتب داخل مبانيها ، ويشمل ذلك بالإضافة إلى الأجهزة :

١/١/٣ - برامج الحاسب الآلي ومدخلاتها : وهي المصنفات والأعمال العلمية والفنية والتنظيمية المنسوبة لمؤلفيها والمملوكة لهم والمحملة في أجهزة الحاسب الآلي أو الخوادم على الشبكة العنكبوتية او السحابة الرقمية لتسيير أعمال الموظفين والإدارات .

٢/١/٣ - ملحقات الحاسب الآلي : كل ما يتصل بالحاسب الآلي سواء كان بشكل مباشر أو غير مباشر مثل (توصيلات الكهرباء ، الشاشة ، لوحة المفاتيح ، الكاميرا ، مكبرات الصوت ، الماسح الضوئي ، الفأرة ، طابعات الأقراص المرفقة بالجهاز وغيرها ....) .

١/٤ : اللجنة – هي لجنة الفحص والتفتيش لأي من أجهزة الحاسب الآلي بالإدارة والمدارس .

١/٥ : البرامج الحاسوبية – جميع البرامج الإلكترونية المعتمدة من إدارة تقنية المعلومات .

١/٦ : التطبيقات الوزارية المركزية: التطبيقات و البرامج المعتمدة من المركز الوطني للمعلومات التربية

١/٧ : مدير ، موظف – عند ذكر " مدير " ، " موظف " في هذه اللائحة فيقصد به العنصر الرجالي والنسائي على حد سواء .

ثانياً : مهام إدارة تقنية المعلومات : (فيما يخص أجهزة الحاسب الآلي وبرامجها)

تكمن مهام إدارة تقنية المعلومات في تخطيط وتنفيذ كافة المهام المتعلقة بميكنة أعمال الإدارة والمدارس ويشمل ذلك :

٢/١ : توفير الحاسب الآلي لكافة الإدارات والموظفين والمدارس حسب حاجة العمل .

٢/٢ : تركيب وصيانة وإزالة وإضافة وتحميل جميع البرامج المتعلقة بالحاسب الآلي وملحقاته (لأجهزة الأعمال الإدارية).

٢/٣ : إعداد وتنفيذ البرامج التطبيقية للإدارات والأقسام والمدارس بالتنسيق مع كل إدارة .

٢/٤ : دراسة العقود مع الشركات المتخصصة للقيام بمهام التوريد والبرمجة والصيانة وذلك وفقاً للصلاحيات المخولة .

٢/٥ : إدارة تقنية المعلومات هي المرجع الوحيد لجميع مستخدمي الحاسب الآلي فيما يخص إدارة وتنظيم وحيازة أجهزة وبرامج الحاسب الآلي وملحقاته في جميع الإدارات والأقسام والمدارس .

٢/٦ : تنسيق التوريد لأجهزة المعامل المدرسية ودراسة وتنفيذ طلبات النقل والصيانة لها.

ثالثاً : حدود استخدامات الحاسب الآلي :

٣/١: لا يحق لأي مستخدم استخدام حاسبه الآلي وجميع الملحقات المرتبطة به لأغراض شخصية أو لأغراض تخرج عن نطاق اختصاص عمله .

٣/٢: على كل مستخدم استعمال الحاسب الآلي المسلّم له ، ولا يحق له اللجوء إلى أجهزة الآخرين إلا في حالة الضرورة التي تحددها احتياجات العمل وتكون بالتنسيق مع الرئيس المباشر .

رابعاً : إعدادات وتجهيزات الحاسب الآلي : (أجهزة الإدارات والأقسام فقط) :

لا يحق لأي مستخدم القيام بالتصرفات التالية إلا بعد الحصول على الموافقة الخطية من إدارة تقنية المعلومات :

٤/١ : إضافة أو تعديل أي من الإعدادات أو التجهيزات المحملة في الجهاز الخاص بكل مستخدم .

٤/٢ : فك أو نقل الحاسب الآلي أو جزء منه أو ملحقاته .

٤/٣ : القيام بأي تغيير في ملحقات الجهاز واستبدالها بأخرى سواء كانت من جهاز آخر في الإدارة أو من خارجها .

٤/٤ : إضافة أي ملحقات في الحاسب الآلي سواء داخله أو خارجه بغض النظر عن نوعها أو الهدف من أضافتها.

٤/٥ : التصرف أو تعديل أو إزالة كل ما يتعلق بتمديدات نقاط الشبكة .

خامساً : أنظمة وبرامج الحاسب الآلي :

٥/١ : لا يحق لأي مستخدم إزالة أي من الأنظمة أو البرامج أو الملفات الموجودة داخل جهازه والمثبتة أصلاً من قبل إدارة تقنية المعلومات بغض النظر عن الهدف من هذه الإزالة .

٥/٢ : في حالة وجود ملاحظات على أحد البرامج المعتمدة يلتزم المستخدم بإبلاغ إدارة تقنية المعلومات لإتخاذ الإجراءات المناسبة حيال ذلك .

٥/٣ : في حالة رغبة المستخدم إضافة أنظمة أو برامج يتطلبها العمل يتم ذلك من خلال تعبئة النموذج المخصص لذلك وتقديمه لإدارة تقنية المعلومات .

سادساً : المسئولية الكاملة عن الجهاز ومحتوياته من برامج وأنظمة وملفات :

٦/١ : يعد المستخدم مسئولاً مسئولية تامة عن جهاز الحاسب الآلي وملحقاته التي بحوزته وما تشتمل عليه من برامج وأنظمة وملفات.

٦/٢ : ليس لأي موظف التدخل في أجهزة زملائه المستخدمين الآخرين لأي سبب كان ، وفي حالة وجود عطل بجهازه فإنه يلتزم بإبلاغ إدارة تقنية المعلومات من خلال تعبئة النموذج المخصص لذلك حتى لا ينتج عن ذلك تعطيل

لعمل المستخدم وفي حالة الضرورة فإن إدارة تقنية المعلومات ستقوم وفق ما تراه بعمل الصيانة اللازمة للجهاز الخاص بالمستخدم .

٦/٣: تلتزم إدارة تقنية المعلومات بإصلاح أعطال أجهزة الحاسب الآلي فيما عدا ما يتبين أنه بسبب سوء الاستخدام .

٦/٤ : يلتزم كل مستخدم بالمحافظة على جميع كلمات المرور والأرقام السرية للدخول على الشبكة أو على البرامج التي يتعامل معها والخاصة به. ولا يجوز له أن يفشي بها أمام الغير ويتحمل لوحده المسئولية الكاملة الناتجة عن عدم التزامه بذلك والأضرار المترتبة عن ذلك .

٦/٥ : يحق لإدارة تقنية المعلومات إلغاء أو تغيير كلمة المرور والرقم السري لأي مستخدم في أي وقت حسب الضرورة وإبلاغ المستخدم ومديره المباشر بذلك .

٦/٦ : يلتزم المستخدم بعدم الدخول أو محاولة الدخول على قواعد ومصادر البيانات غير المصرح له بها أو استخدامها .

٦/٧ : يلتزم المستخدم بعدم تخزين أي ملفات على جهازه لا تتعلق بمصلحة العمل .

سابعاً : البرامج الحاسوبية (خاص بالمدارس) :

٧/١ : يعد مدير المدرسة المسئول الأول عن التطبيقات الوزارية المركزية و البرامج الحاسوبية وفي حالة تفويض الصلاحية لأحد الموظفين بالمدرسة أو آخر مساعد له يتم تسليمهم العمل بخطاب رسمي. وهذا لا يعفي المدير من المسئولية .

٧/٢ : يلتزم مدير المدرسة بإدخال واستكمال جميع البيانات في التطبيقات الوزارية المركزية و البرامج الحاسوبية أولاً بأول والخاصة بالمدرسة وجميع العاملين والطلاب خلال الشهر الأول من بدء العام الدراسي.

٧/٣ : يلتزم مدير المدرسة بالتأكد من تدقيق وصحة جميع البيانات المدخلة في التطبيقات الوزارية المركزية و البرامج الحاسوبية.

٧/٤ : يلتزم مدير المدرسة بإجراء أي تعديلات تتم على البيانات المدخلة في البرامج الحاسوبية أولاً بأول بدون تأخير.

ثامناً : خدمة مشاركة الملفات (أجهزة الإدارات والأقسام فقط) :

٨/١: يلتزم المستخدم بتعبئة النموذج المخصص للحصول على خدمة المشاركة على جهازه وتقديمه لإدارة تقنية المعلومات .

٨/٢: عند إنشاء مشاركة يتم تحديد أسماء الأشخاص المصرح لهم بالدخول عليها ، مع وضع الصلاحيات المناسبة لكل منهم .

٨/٣: عند اكتشاف مشاركة مفتوحة للجميع (Every One) يتحمل منشئها المسئولية الناتجة عن ذلك (حيث هي من الأسباب الرئيسية لانتشار الفيروسات) .

٨/٤: تستخدم المشاركة لتبادل الملفات الخاصة بالعمل ولا يسمح باستخدامها للأغراض الشخصية .

٨/٥: عند الانتهاء من الحاجة التي أدت إلى فتح المشاركة يتم إزالتها .

٨/٦: يحق لإدارة تقنية المعلومات إلغاء أي مشاركة لا تنطبق عليها الضوابط المذكورة.

تاسعاً : خدمة البريد الإلكتروني والانترنت :

٩/١: تقتصر خدمة البريد الإلكتروني على تبادل المعلومات والخطابات وكافة المعاملات الخاصة بأعمال الإدارة .

٩/٢: كل مدير إدارة أو رئيس قسم أو مدير مدرسة أو موظف مسئول عن البريد الإلكتروني الخاص بالإدارة أو القسم أو المدرسة بالإضافة إلى بريده الخاص (إن وجد) و يتحمل كامل المسئولية عن أي رسالة تصدر منه ، ولا يجوز تداول الرسائل المخالفة للأنظمة الرسمية أو المخلة بالآداب أو التي تخدش الحياء العام ، كما لا يجوز تداول أي رسائل ليس لها صلة بالعمل وتؤدي إلى تعطيله .

٩/٣: تقدم إدارة تقنية المعلومات خدمة الإنترنت للجهات والأشخاص الذين يتطلب عملهم ذلك وفق ضوابط ومعايير محددة .

٩/٤: يحاسب أي مستخدم عند الدخول أو محاولة الدخول على الإنترنت من خلال جهازه بطريقة غير نظامية ، وسيتم إزالة أي أجهزة خاصة بالربط على الإنترنت من جهاز المستخدم.

٩/٥: يحق لإدارة تقنية المعلومات القيام بمراقبة عمليات دخول المستخدمين إلى الإنترنت من خلال نظام إلكتروني خاص والرفع لإدارة المتابعة عن من يتجاوز التعليمات المنظمة لذلك .

٩/٦: يلتزم مستخدمو الإنترنت المصرح لهم بذلك بعدم الدخول على المواقع المحظورة أو التي تحتوي على ما يخالف العادات والتقاليد والأنظمة السائدة بالمملكة .

عاشراً : ملكية البرامج :

١٠/١ : كل مستخدم قام بأي إضافة أو تعديل في البرامج الأصلية أو المرخصة للإدارة والمدارس أو نسخها أو قلدها أو باعها أو أجرها أو وزعها يعتبر مخالفاً لما نص عليه نظام حماية حقوق المؤلف ويتحمل ما سوف يتخذ بشأنه سواء من الشركة المالكة أو من الإدارة بما في ذلك أي مسئولياتٍ تحمّل على الإدارة نظاماً .

١٠/٢ : كل مستخدم قام بنسخ أي برنامج تم تطويره في الإدارة ، أو باعه أو أجره أو وزعه في أي بلد كان يعتبر مخالفاً لما نص عليه نظام حماية حقوق المؤلف ويتحمل ما سوف يتخذ بشأنه من قبل الإدارة بناءاً على الضرر اللاحق بها .

١٠/٣ : تكون كافة برامج الحاسب الآلي التي يتم تصميمها أو تطويرها في الإدارة ملكاً للإدارة ولا يجوز التصرف بهذه البرامج أو جزء منها بأي شكل من الأشكال سواء بالبيع أو الإهداء أو النسخ .

١٠/٤: يلتزم كافة مستخدمي الحاسب الآلي بالإدارة والمدارس بالمحافظة على كافة الأسرار والمعلومات المتعلقة بالبرامج المستخدمة داخل الإدارة ولا يجوز تسريبها للغير حتى بعد انتهاء علاقة المستخدم بالإدارة أو المدرسة ويتحمل من يخالف ذلك مسئولية تعويض الإدارة عن أي أضرار تصيبها نتيجة لذلك .

١١/٤ : تكون كافة برامج الحاسب الآلي التي يتم تصميمها أو تطويرها في الإدارة من قبل أحد موظفيها ملكاً للإدارة العامة ويستثنى من هذه القاعدة الحالات التي يتم التنسيق فيها بين الإدارة التابع لها الموظف ومركز الحاسب الآلي والمعلومات ، على أن يراعى في جميع الأحوال تسليم النسخة النهائية المفتوحة من البرنامج Open Source .

١٢/٤ : تكون كافة برامج الحاسب الآلي التي يتم تصميمها أو تطويرها بشكل كامل للإدارة من قبل الشركات ملكاً للإدارة العامة ، على أن تقوم الجهات الإدارية بالتنسيق مع مركز الحاسب الآلي والمعلومات حيال الأمور الفنية لقواعد البيانات وتسليم النسخة النهائية المفتوحة من البرنامج وتوثيقها لديهم .

١٣/٤ : تكون كافة برامج الحاسب الآلي التي تملكها الشركات ثم يتم تطويرها لتتناسب مع عمل الإدارة من قبل تلك الشركات ملكاً للإدارة العامة للعمل عليها خلال مدة الترخيص المتفق عليه مع الشركة داخل المنطقة ، على أن يكون التنسيق مع مركز الحاسب الآلي والمعلومات حيال الأمور الفنية لقواعد البيانات وتسليم نسخ البرامج وتوثيقها لديهم .

حادي عشر : ملكية أجهزة الحاسب الآلي :

١١/١ : تعتبر جميع أجهزة الحاسب الآلي وملحقاته والبرامج المرخصة ملكاً للإدارة ، ولا يجوز التصرف فيها إلا بعد أخذ الموافقة الخطية من إدارة تقنية المعلومات .

١١/٢ : لا يتم إتلاف أي جهاز حاسب آلي أو ملحقاته لا يعمل بشكل صحيح إلا بعد التنسيق مع إدارة تقنية المعلومات ، حتى تتمكن الإدارة من تعويض الإدارة أو القسم أو المدرسة بجهاز حاسب آلي آخر .

ثاني عشر : فحص وتفتيش الحاسب الآلي :

١٢/١ : تكوّن لجنة لفحص وتفتيش أجهزة الحاسب الآلي برئاسة مدير إدارة تقنية المعلومات أو من يمثله وعضوية ممثل من إدارة المتابعة.

١٢/٢ : لمديري الإدارات ورؤساء الأقسام ومديري المدارس حق التقدم بطلب إجراء عملية الفحص والتفتيش على أجهزة أي من موظفيهم عند الحاجة .

١٢/٣ : لمدير إدارة تقنية المعلومات الحق في تكليف اللجنة بفحص وتفتيش أي من أجهزة الإدارة أو المدارس عند الحاجة .

١١/٤ : تتم عملية الفحص والتفتيش بحضور المستخدم المعني بالجهاز ، ويحرر محضر يدون به الوقائع والنتائج الخاصة بعملية الفحص والتفتيش ويوقع عليه رئيس وأعضاء اللجنة والمستخدم على أن تحفظ صورة من المحضر في ملف خدمته وذلك في حالة ثبوت مخالفة لأحكام هذه اللائحة ويزود مساعد المدير العام للخدمات المساندة بصورة من المحضر لاتخاذ اللازم .

ثالث عشر : الإجراءات :

يعاقب كل موظف يخالف هذه اللائحة وفقاً للائحة الجزاءات المعمول بها في الإدارة عن طريق إدارة المتابعة بناءً على المادة (١١) فقرة (ج) والمادة (١٥) من نظام الخدمة المدنية – الواجبات . حيث تعتبر مخالفات إدارية يعرض المخالف نفسه للمسائلة التحريرية والمجازاة وفق المادة (٣٢/أولاً/٣,٢,١) من نظام تأديب الموظفين وهذه المجازاة تشمل الآتي : إما -

١ : الإنذار .

٢ : اللوم .

٣ : الحسم .

بالإضافة إلى محاسبة الشخص المستخدم للجهاز مما يتطلب معه نقله من الجهة التابع لها إلى جهة أخرى وذلك بعد التحقيق معه وإثبات المخالفة من قبل لجنة فحص وتفتيش والحاسب الآلي.

سياسة عدم افشاء المعلومات و البيانات

آخر تحديث تم بتاريخ ١٤٣٣/٢/١٥هـ الموافق ٢٠١٢/١/٩م.

ملخص

إن سياسة عدم افشاء المعلومات و البيانات تحمي معلومات الإدارة العامة للتربية و التعليم بالمنطقة الشرقية السرية من كشفها لأشخاص من خارج أو داخل الإدارة العامة للتربية و التعليم بالمنطقة الشرقية والذين من المحتمل – بقصد أو بغير قصد – أن يستخدموا تلك المعلومات بطريقة قد تكون ضارة للإدارة العامة. وسوف يتم التعبير في هذه الوثيقة عن مثل تلك المعلومات بـ "المعلومات السرية".

وتقوم سياسة عدم افشاء المعلومات و البيانات أيضا بحماية الأشخاص المرخص لهم في الوصول الى المعلومات السرية وذلك بتوضيح وتحديد واجباتهم والتزاماتهم فيما يتعلق بحماية المعلومات السرية.

• الهدف

هذه السياسة سوف توجز الإجراءات المتخذة من الإدارة العامة للتربية و التعليم بالمنطقة الشرقية لضمان حماية المعلومات السرية، بما في ذلك فرض التزام تعاقدي على شكل اتفاق عدم الكشف.

• الأشخاص المعنيين

يجب على جميع الموظفين و الموظفات والمتعاقدين المستقلين للإدارة العامة للتربية و التعليم بالمنطقة الشرقية أن يكونوا على إلمام بالمتطلبات للالتزام بهذه السياسة.

• الاستثناءات

لا يوجد .

• تفاصيل السياسة

في أثناء تأدية عملهم، يمكن للموظفين و الموظفات والمتعاقدين المستقلين أن يستقبلوا، يشاهدوا أو يتعاملوا مع معلومات تضم معلومات سرية خاصة بالإدارة العامة للتربية و التعليم بالمنطقة الشرقية. إن كشف المعلومات السرية الى أطراف غير مصرح لها قد يؤدي الى ضرر لا يمكن إصلاحه ، ولذلك فمن مصلحة الإدارة العامة للتربية و التعليم بالمنطقة الشرقية أن تضع ضوابط محددة للأشخاص الذين يتلقون، و يطلعون، ويستمعون الى، أو يستخدمون المعلومات السرية وأن تتطلب من أولئك الأشخاص تنفيذ اتفاق تعاقدي يشعر بنية الامتثال بتلك الضوابط.

• المعلومات المشمولة في سياسة عدم افشاء المعلومات و البيانات

المعلومات السرية قد تشتمل على أسرار المهنة، الملكية الفكرية، وبيانات أخرى خاصة تم تطويرها، إنشائها، تجميعها، أو استخدامها في سياق ممارسة نشاط العمل. المعلومات السرية تشمل – ولكن ليس مقصورا على –المعلومات الخاصة بالمالية، والمبيعات، و التسويق، والقانونية، والتشغيلية، والشخصية والإنتاجية.

المعلومات السرية تشير الى كل وأي من المعلومات التقنية وغير التقنية، بما يشمل براءات الاختراع، الحقوق الفكرية، سر المهنة، والمعلومات الملكية، التقنيات، المخططات، رسوم، نماذج، اختراعات، مهارة، عمليات، معدات، أدوات، خوارزميات، برامج، وثائق مصدر البرامج، والصيغ المتعلقة بالمنتجات والخدمات الحالية والمستقبلية و المقترحة لكل من الأطراف ويشمل على، دون تحديد، معلوماتهم الخاصة بالبحوث، العمل التجريبي، التطوير، تفاصيل التخطيط و المواصفات، الهندسة، معلومات المالية، الاحتياجات الشرائية، التصنيع، قوائم العملاء، توقعات العمل، المبيعات و التجارة، والخطط والمعلومات التسويقية.

وتشمل المعلومات السرية أيضا على المعلومات السرية والملكية لأي طرف ثالث والتي قد تكشف عن مثل تلك المعلومات لأي من الطرفين في سياق عمل الطرف الآخر.

قد يتم نقل المعلومات السرية بشكل كتابي، كلامي، رسومي، تصويري، سمعي أو أي شكل آخر ويمكن أن تقدم أو تخزن على ورق، بشكل مغناطيسي أو الكتروني، نموذج مجسم، أو على هيئة أخرى.

- ## الأشخاص المشمولين في سياسة عدم افشاء المعلومات و البيانات

تنطبق سياسة عدم افشاء المعلومات و البيانات على أي موظف أو موظفة أو مقاول مستقل ممن تكشف له المعلومات السرية التي تمتلكها الإدارة العامة للتربية و التعليم بالمنطقة الشرقية في سياق ممارسة العمل. وكذلك على الموظفين و الموظفات بعد ترك الخدمة بناء على ما ورد في الفقرة (هـ) من المادة (١٢) من نظام الخدمة المدنية – الواجبات (يحضر على الموظف إفشاء الأسرار التي يطلع عليها بحكم وظيفته حتى بعد ترك الخدمة).

- ## الأعمال المحظورة والمطلوبة

يحظر على الأشخاص الذين يتلقون المعلومات السرية من استغلال، نشر، أو الكشف بأي طريقة لأي معلومات سرية لأي شخص، أو شركة، أو نشاط تجاري، باستثناء الحد الضروري للقيام بالعمل لمصلحة الإدارة العامة للتربية و التعليم بالمنطقة الشرقية وبإذن منها.

إذا كان الشخص المتلقي للمعلومات السرية مقاول مستقل أو طرف ثالث، فيحظر عليه كشف المعلومات السرية لأي شخص، أو شركة، أو نشاط تجاري، أو منظمة باستثناء موظفيه الذين هم بحاجة للإطلاع على تلك المعلومات والذين سبق لهم الموافقة، إما كشرط وظيفي أو لغرض الحصول على المعلومات السرية، على أن يكونوا ملتزمين ببنود وشروط مماثلة الى حد كبير لتلك الموجودة في هذه الاتفاقية.

يحظر على الأشخاص المتلقين للمعلومات السرية من نسخ أو عمل هندسة انعكاسية للمعلومات السرية من دون إذن صريح من الإدارة العامة للتربية و التعليم بالمنطقة الشرقية.

يلزم الأشخاص المتلقين للمعلومات السرية أن يبقوا المعلومات السرية للإدارة العامة للتربية و التعليم بالمنطقة الشرقية بشكل آمن وأن يأخذوا كافة التدابير المعقولة لحماية المعلومات السرية.

على الأشخاص المتلقين للمعلومات السرية أن يقوموا بإشعار الإدارة العامة للتربية و التعليم بالمنطقة الشرقية مباشرة عند حصول أي استخدام غير مصرح به أو كشف للمعلومات السرية، والموافقة على مساعدة الإدارة العامة للتربية و التعليم بالمنطقة الشرقية في معالجة أي استخدام غير مصرح به أو كشف للمعلومات السرية.

- ## متطلبات اتفاق سياسة عدم افشاء المعلومات و البيانات

تعزيزا لأهداف سياسة عدم افشاء المعلومات و البيانات، يطلب من الأشخاص المتلقين للمعلومات السرية، أو الأشخاص الذين هم في موضع لتلقي المعلومات السرية، أن يقوموا بتنفيذ اتفاق عدم الكشف رسميا، والذي سوف يصبح ساري المفعول مباشرة فور التوقيع وسوف يبقى ساري المفعول الى الأبد حتى أو مالم تقوم الإدارة العامة للتربية و التعليم بالمنطقة الشرقية بتقديم إشعار يفيد بأن الاتفاق لم يعد ساري المفعول. إن إنهاء الالتزام سوف يكون مقصورا فقط على تلك المعلومات السرية المحددة في إشعار الإنهاء. و يجب أن يكون الإشعار خطيا وموقعا من قبل ممثل مفوض من الإدارة العامة للتربية و التعليم بالمنطقة الشرقية.

- ## عقوبات الانتهاك

إن المخالفة لسياسة عدم افشاء المعلومات و البيانات هذه من قبل موظف او موظفة بالإدارة العامة للتربية و التعليم بالمنطقة الشرقية سيؤدي الى إجراء تأديبي وفق الأنظمة المقررة. وفي حالة ثبوت المخالفة يكون الموظف/الموظفة عرضة للعقوبة المقررة وفقا لنظام تأديب الموظفين و عقوبات نشر الوثائق السرية وإفشائها الصادر بالمرسوم الملكي رقم ٣٥ و تاريخ ١٤٣٢/٥/٨ هـ.

تعد المخالفة لسياسة عدم افشاء المعلومات و البيانات هذه من قبل مقاول مستقل خرقا للعقد وقد تؤدي الى إنهاء فوري لاتفاق العمل مقابل الاستئجار وتصبح التزامات الإدارة العامة للتربية و التعليم بالمنطقة الشرقية المنصوص عليها في العقد لاغية وباطلة.

من حق الإدارة العامة للتربية و التعليم بالمنطقة الشرقية الحصول على تعويض كامل بما هو مناسب بموجب القانون عن الأضرار المستمرة التي قد تلحق بالإدارة العامة للتربية و التعليم بالمنطقة الشرقية و عملياتها، و إنتاجها، و سمعتها وقدرتها على القيام بعملها.

- ## إقرار بسياسة عدم افشاء المعلومات و البيانات

هذا النموذج يستخدم للإقرار باستلام والامتثال لسياسة عدم افشاء المعلومات و البيانات الخاصة بالشركة.

- ## الإجراء

أكمل الخطوات التالية:

١. اقرأ سياسة عدم افشاء المعلومات و البيانات.
٢. قم بالتوقيع وتدوين التاريخ في الأماكن المخصصة لذلك.
٣. قم بإرجاع نسخة من هذه الوثيقة الموقعة الى إدارة تقنية المعلومات.

- **التوقيع**

بالتوقيع أدناه، فإني أوافق عل الشروط التالية:

١. لقد استلمت وقرأت نسخة من سياسة عدم افشاء المعلومات و البيانات وأفهم وأوافق عليها.
٢. أفهم و أوافق على أن أي برامج وأجهزة تقدم الي من قبل الإدارة العامة للتربية و التعليم بالمنطقة الشرقية تبقى من ملكية الإدارة العامة للتربية و التعليم بالمنطقة الشرقية.
٣. أفهم و أوافق على أن لا أقوم بتغيير، تعديل، أو تحديث لأي برامج أو أجهزة يتم تزويدي بها من قبل الإدارة العامة للتربية و التعليم بالمنطقة الشرقية بدون الحصول على إذن من إدارة تقنية المعلومات.
٤. أفهم و أوافق على أنه في حالة مغادرة الإدارة العامة للتربية و التعليم بالمنطقة الشرقية لأي سبب كان، يجب أن أقوم مباشرة بإعادة النسخ الأصلية والمنسوخة لكل البرامج، و مواد الحاسب أو معداته الى الإدارة العامة للتربية و التعليم بالمنطقة الشرقية والتي استلمتها من الإدارة العامة للتربية و التعليم بالمنطقة الشرقية والتي إما أن تكون في حيازتي أو بشكل مباشر أو غير مباشر تحت سيطرتي.
٥. أفهم و أوافق على أنه يتوجب علي المحافظة على جميع البرامج المقدمة من الإدارة العامة للتربية و التعليم بالمنطقة الشرقية والأجهزة من السرقة والأضرار المادية.

للتنويه: هذه السياسة ليست بديلا عن المشورة القانونية. إذا كان لديك تساؤلات حول هذه السياسة، قم بمراجعة محام.

سياسة كلمات المرور (Password Policy)

آخر تحديث تم بتاريخ ١٤٣٣/٢/١٥هـ الموافق ٢٠١٢/١/٩م.

مصطلحات:

- الإدارة العامة : الإدارة العامة للتربية و التعليم بالمنطقة الشرقية.

مقدمة

إن أخطر الثغرات الأمنية لأي منظمة تكمن في مدى قوة و ضعف كلمات المرور. تعتبر كلمات المرور البسيطة أو المشتركة غير فعالة وتساعد القراصنة وغيرهم في محاولاتهم الغير مشروعة للوصول الى البيانات الحساسة ، والسرية الخاصة بالإدارة العامة. إن حماية الأجهزة والأنظمة والبيانات والاتصالات للإدارة العامة يعتبر ذا أهمية قصوى؛ كلمات المرور القوية تلعب دورا مهما في هذه العملية.

الهدف

إن الهدف من هذه السياسة هو التأكد من أن كل موظف أو موظفة ، مقاول ، عامل أو عاملة مؤقت أو متطوع في الإدارة العامة يفهم ويوافق على الالتزام بالإرشادات الخاصة بإنشاء وإدارة والمحافظة على كلمات المرور.

النطاق

تطبق سياسة كلمة المرور للإدارة العامة على جميع الموظفين و الموظفات ، المقاولين ، العاملين المؤقتين، المتطوعين وكل من يعمل على أجهزة الحاسب المقدمة من المنظمة أو يستخدم خدمات الإنترنت أو البريد الإلكتروني المقدمة من الإدارة العامة. إن أي استخدام لحسابات المستخدم الخاصة بالإدارة العامة ، أجهزة الحاسب المكتبية والمحمولة، الخوادم، خدمات الإنترنت والاتصالات الإلكترونية يجب أن يتوافق مع الإرشادات الواردة في هذه السياسة.

إدارة كلمات المرور

إن كلمات المرور لكل الأنظمة يجب أن لا يتم البوح بها لأي أحد أبدا ، وهي تخضع للقواعد التالية:

- لا يتم التحدث بكلمات المرور أو كتابتها أو إرسالها بالبريد الإلكتروني أو التلميح بها أو مشاركتها أو أن تعرف لأي شخص غير المستخدم المعني بذلك.
- لا يتم تشارك كلمات المرور لأجل "تغطية" لشخص آخر خارج المكتب أو متغيب لسبب مرضي. بدلا من ذلك، اتصل بإدارة تقنية المعلومات للحصول على حساب مؤقت.

- كلمات المرور يجب أن لا تكتب على الورق أبدا أو أن يتم كتابتها وإخفائها بالقرب من محطة العمل.
- يجب أن تستخدم جميع أجهزة الحاسب والخوادم خاصية شاشة التوقف والتي تتطلب إدخال اسم المستخدم وكلمة المرور لمعاودة الوصول عند ترك النظام خاملا لأي فترة أطول من ثلاث دقائق.
- يفضل و بشكل كبير جدا تغيير كلمات المرور كل ٩٠ يوما.
- يجب أن لايتم إعادة استخدام كلمات المرور أبدا.

- **تعقيد كلمة المرور**

يجب أن تتطابق كلمات المرور الخاصة بأنظمة المستخدمين مع المعايير التالية:

- كلمات المرور يجب أن تكون بطول ثمانية أحرف على الأقل.
- كلمات المرور يجب أن تحتوي على كل من حروف وأرقام.
- كلمات المرور ينبغي أن تحتوي على رموز(مثلا !، @، #، $، %، ^، &، ❖) متى ماأمكن ذلك.
- كلمات المرور ينبغي أن تحتوي على أحرف صغيرة وكبيرة.
- كلمات المرور يجب أن لا تحتوي على جزأ من اسمك، العنوان، تاريخ الولادة، رقم الضمان الإجتماعي، اللقب، العائلة، اسم المستخدم، اسم فريق رياضي أو كلمة واردة في القاموس أو مكتوبة بالعكس.
- أي من الأعلى مسبوقا أو متبوعا برقم.

يجب أن تتطابق كلمات المرور الخاصة بالأنظمة الإدارية والمالية مع المعايير التالية:

- كلمات المرور يجب أن تكون بطول عشرة أحرف على الأقل.
- كلمات المرور يجب أن تحتوي على كل من حروف وأرقام.
- كلمات المرور يجب أن تحتوي على أحرف صغيرة وكبيرة.
- كلمات المرور يجب أن تشمل على الأقل ثلاثة رموز غير أبجدية: (مثلا !، @، #، $، %، ^، &، ❖، .،).
- كلمات المرور يجب أن لا تحتوي على جزأ من اسمك، العنوان، تاريخ الولادة، رقم الضمان الإجتماعي، اللقب، العائلة، اسم المستخدم، اسم فريق رياضي أو كلمة واردة في القاموس أو مكتوبة بالعكس.
- أي من الأعلى مسبوقا أو متبوعا برقم.

- **الأنظمة المشمولة**

إن الإرشادات الخاصة بسياسة كلمات المرور تطبق على كل الموظفين و الموظفات ، مقاولين ، عمال مؤقتين ، متطوعين أو آخرين ممن يعمل على الحسابات، المعدات والخدمات المقدمة من الإدارة العامة ، بما يشمل التالي:

- حسابات مستخدم أنظمة التشغيل والشبكة الداخلية.
- حسابات الانترنت.
- حسابات جماعية.
- حسابات البريد الالكتروني.
- أنظمة تخطيط موارد المؤسسات (ERP).
- منصات إدارة علاقة العملاء(CRM).
- خدمات الشبكة الخاصة الإفتراضية (VPN).
- كلمات السر للحاسب (BIOS).

- المخالفات والعقوبات

في حالة مخالفة الأنظمة في هذه الإتفاقية فإن الموظف أو الموظفة سيكونون عرضة للمساءلة القانونية من قبل الإدارات ذات العلاقة في الإدارة العامة للتربية و التعليم بالمنطقة الشرقية، وللجهات ذات العلاقة أو الأطراف المتضررة رفعها للجهات القضائية المختصة.

وفي حالة ثبوت المخالفة يكون الموظف/الموظفة عرضة للعقوبة المقررة وفقا لنظام تأديب الموظفين و عقوبات نشر الوثائق السرية وإفشائها الصادر بالمرسوم الملكي رقم ٣٥ و تاريخ ١٤٣٢/٥/٨ هـ.

إقرار بسياسة كلمة المرور

هذا النموذج يستخدم للإقرار باستلام والإمتثال لسياسة كلمة المرور الخاصة بالإدارة العامة.

- الإجراء

أكمل الخطوات التالية:

٤. إقرأ سياسة كلمة المرور
٥. قم بالتوقيع وتدوين التاريخ في الأماكن المخصصة لذلك.
٦. قم بإرجاع نسخة من هذه الوثيقة الموقعة الى إدارة تقنية المعلومات.

- التوقيع

إن توقيعك يشهد بموافقتك على الشروط التالية:

i. لقد استلمت وقرأت نسخة من سياسة كلمة المرور و أفهم وأوافق عليها.

ii. أفهم بأن خرق سياسة كلمة المرور قد يؤدي الى اتخاذ إجراء قانوني ضدي.

للتنويه: هذه السياسة ليست بديلا عن المشورة القانونية. اذا كان لديك تساؤلات حول هذه السياسة، قم بمراجعة محام.

أهمية استخدام سياسة كلمة مرور فعالة

بواسطة: Brien M. Posey

إن الحاجة لسياسة كلمة مرور فعالة أمر في غاية الوضوح، لدرجة أني أعترف أني أشعر بسئ من الغرابة أن أكتب مقالا حول هذا الموضوع. في الحقيقة، أستطيع وبكل سهولة أن أجمع الضرورة لسياسة كلمة مرور فعالة في جملة واحدة. أنت بحاجة لسياسة كلمة مرور فعالة لكي تمنع تخمين أو اختراق كلمات المرور. وبالرغم من ذلك، توجد بعض المنظمات والتي لا تتعاطى مع أمن كلمات المرور بجدية. في هذا المقال، سوف أشرح لماذا يعتبر وجود سياسة فعالة لكلمة المرور أمر في غاية الأهمية حتى بالنسبة للشركات الصغيرة ذات الحد الأدنى من المتطلبات الأمنية.

لقد قمت مرة بعمل استشاري لشركة صغيرة ذات سياسة كلمة مرور مسلية. ألزم موظفوا تقنية المعلومات المستخدمين باستخدام كلمات مرور، ولكن لم يضعوا أي قيود على كلمات المرور تلك. لم يكن هناك حد أدنى لطول كلمات المرور أو متطلبات التعقيد، وكلمات المرور لم تكن لتنقضي فعاليتها أبدا. لم أكن أريد الإساءة، ولكن كان علي سؤال الشخص المسؤول عن فقدان الأمن لكلمات المرور. وكانت اجابته بأن أمن كلمات المرور لم يكن حقيقة مهما لأن المستخدمين لم يكن لديهم صلاحيات لعمل شيء.

في ذلك الوقت، تركت الموضوع لأني لم أكن هناك للعمل على قضايا أمنية. على كل حال، أريد أن أغتنم الفرصة الآن لشرح لماذا عدم وجود سياسة لكلمة المرور يعتبر فكرة سيئة، حتى عندما يكون للمستخدمين أدنى الصلاحيات.

أول سبب لأهمية أمن كلمة المرور هو أن المستخدمين يوجد لديهم صلاحيات لشيء ما. فكر في ذلك للحظة. لا حاجة لوجود حسابات للمستخدمين اذا لم يكونوا بحاجة للوصول الى شيء ما. مهما كانت الموارد التي يصل اليها المستخدمين، لابد من حمايتها.

لمعرفة لماذا هذا الأمر في غاية الأهمية، دعنا ننظر الى أبسط نموذج عمل يمكنني التفكير فيه، نظام عمل بريد صغير. في عمل مثل ذلك، الطلبات سوف تأتي عن طريق الويب أو بالهاتف أو بالفاكس. المستخدمون لديك سوف يكونون مسؤولين عن إدخال الطلبات الى النظام بحيث يكون بالإمكان شحن طلب العميل.

اذا كان المستخدم يقوم فقط بإدخال الطلب، قد لا تظهر أهمية أن يكون لديهم كلمة مرور قوية. ومع ذلك تخيل ما كان ليحدث لو أن كلمة مرور المستخدم سقطت في أيدي أشخاص آخرين. لو أن كلمة المرور حصل عليها أحد المخربين، مجموعة من الطلبات المزيفة ربما يتم إدخالها فقط للخبطة القائمة لديك. وربما أسوأ من ذلك، قد يتم حذف قاعدة بيانات العملاء بالكامل، أو نشرها على الإنترنت. إذا حصل منافسوك على كلمة مرور المستخدم، ربما يقوموا بسرقة قائمة العميل لديك. ولو أن سارقا

كان ليحصل على كلمة مرور المستخدم، ربما يقوم بوضع طلبات مزيفة في محاولة لسرقة القائمة. وبالمثل، فمن المحتمل أن يقوم السارق بسرقة أرقام البطاقات الائتمانية لعملائك. إن النقطة هنا أن هذا الحساب الذي قد يبدو بريئًا قد يستخدم في العديد من الأغراض السيئة.

ولمصلحة النقاش دعنا نفترض أنك قمت بإغلاق نظام طلب الإدخال في محاولة لتقليل الخطر الذي من الممكن أن يسببه مستخدم واحد. حتى في وضع مثل ذلك، يبقى من الأهمية أن يكون لديك سياسة كلمة مرور جيدة لأن الهاكر يستطيع أن يستخدم (وغالبا ما يفعل) حسابا مخترقا كخطوة أولية نحو السيطرة على أنظمة أخرى.

لا أريد تحويل هذه المقالة الى دورة مكثفة عن لقرصنة، ولكن دعونا نتظاهر للحظة أن شركتنا الوهمية تتطلب كلمات مرور، ولكن ليس لديها أي متطلبات أخرى نحوها. لو كان على الهاكر أن يخترق أو يخمن كلمة المرور لحساب ما، حتى لو كان حسابا "غير مهما"، سوف يدركون أن سياسة كلمة المرور للمنظمة عبارة عن أضحوكة. حينها من المحتمل أن يقوموا باختراق كلمات المرور لحسابات أخرى. حتى لو لم يكن لحساب واحد القدرة للقيام بأي ضرر حقيقي، فالاستخدام الجماعي لعدة حسابات قد يكون مدمرا.

سبب واحد أخير لماذا يعتبر وجود سياسة كلمة مرور جيدة أمرا ضروريا، حتى في المنظمات الصغيرة هو أنه لو قام شخص بتسجيل الدخول بحساب ليس له، قد يسبب هذا كل أنواع المشاكل للمستخدم الذي تم اختراق حسابه. على سبيل المثال، لو قام الهاكر باختراق حساب لمستخدم ما ثم استخدم ذلك الحساب لشن هجوم ضد أجزاء أخرى من النظام، حينها سوف تقوم آليات التدقيق والمراقبة في الشبكة لديك باتهام بطريق الخطأ المستخدم لذلك الحساب بشن الهجوم.

دعنا نرجع للوراء للمثال الأول عن شركة نظام البريد الوهمية للحظة. افترض ان الهاكر قام بتسجيل الدخول كمستخدم والذي يكون عادة مسؤول عن ادخال الطلب وبدأ بالعبث مع نظام ادخال الطلب. اذا تم حذف الطلبات، فمن المحتمل أن المستخدم الذي تم اختراق حسابه سوف يحاسب على تلك الطلبات المحذوفة. ناهيك عن حقيقة أنه سوف يكون لديك بعض العملاء المستائين اذا "فقدت" طلباتهم.

وكما ترى، فإن وجود سياسة فعالة لكمة المرور أمر في غاية الأهمية، حتى للشركات الصغيرة. في هذا المقال، قمت بإعطائك عدة أمثلة على الضرر الذي يمكن أن يحدث اذا تم اختراق حساب مستخدم حتى لو بدا أنه غير مهم.

الإدارة / المكتب :			
م	الاســـــم الرباعي	التوقيع	التاريخ
١			
٢			
٣			
٤			
٥			
٦			
٧			
٨			
٩			
١٠			
١١			
١٢			
١٣			
١٤			
١٥			
١٦			
للاستخدام الرسمي فقط:			