***دليل إرشادات أمن المعلومات***

النسخة الثانية

 2013©

إعــــداد:

***قسم أمن المعلومات***

المديرية العامة لتقنية المعلومات

**المقدمة:**

إن الهدف من وضع دليل الإرشادات الأمنية في نسخته الثانية، هو أن يكون كل فرد على علم ودراية بمسؤوليته تجاه حماية المعلومات الخاصة بالوزارة، وإدراكه التام لأهمية أمن المعلومات في الوزارة ومعرفته للأخطار المترتبة على أي من التجاوزات الأمنية. إن أمن المعلومات لهي تنمية وتعزيز للمسؤولية الفردية والفهم الكامل بأهمية تطبيق القواعد الأمنية الموضوعة من قبل الجهات العليا والحرص على عدم تجاوزها.

سوف يتم تزويد جميع موظفي الوزارة ومستخدمي جهاز الحاسوب بنسخة من هذا الدليل، وعلى مديري الدوائر أن يزودوا بهذا الدليل أي موظف/ـة يتم تعيينه حديثاً أو أي موظف/ـة يعمل من خلال شبكة الوزارة. كما أنه تم وضع نسخة رقمية من هذا الديل على موقع الوزارة الإلكتروني بوابة سلطنة عمان التعليمية [www.moe.gov.om](http://www.moe.gov.om).

**الباب الأول: أمـــــــن المعلومات**

**تعريف أمن المعلومات:**

توجد المعلومات بأشكال مختلفة فهي يمكن أن تكون على الورق أو محفوظة إلكترونياً أو تتناقل على الألسنة. هذه المعلومات على درجة عالية من الأهمية لدى المؤسسات والأفراد حيث أنها تعد من أصول الممتلكات، وعليه يجب حمايتها وحماية البنية التحتية التي تساندها مثلها مثل بقية الأشياء الثمينة و هذا ببساطة هو هدف أمن المعلومات.

**تصنيف سرية المعلومات:**

**سري للغاية:** يعتبر هذا التصنيف أعلى درجات التصنيف الأمنيى ويستعمل لحماية المعلومات البالغة الأهمية سواء كانت تعليمية، أو المالية أو ذات طابع أمني والتي سيؤدي إفشاؤها إلى إلحاق ضرر خطيـــــــــــــــــر للغاية بالمؤسسة.

**سري:** يستعمل هذا التصنيف لحماية المعلومات التعليمية أو المالية أو ذات الطبيعة الأمنية التي سيؤدي التصريح بها من غير إذن إلى إلحاق ضرر بالغ بمصالح المؤسسة.

**مقيد:** يحمي هذا التصنيف تلك المعلومات التي لا يجب تضمينها في فئتي سري للغاية أو سري والتي تعمم على نطاق أوسع ضمن دوائر المؤسسة، ولكن مع مراعاة عدم الإفشاء بها للأشخاص الغير مصرح لهم.

**غير مصنف:** يستخدم هذا التصنيف لحماية المعلومات الشخصية الخاصة بالموظفين لحجبها عن الإطلاع لغير المخول.

حرصا من وزارة التربية و التعليم و على رأسها معالي الوزيرة الموقرة على التطوير و الرقي بالمستوى والفعالية المهنية وتوفير الوقت و الجهد وزيادة الإنتاج و رفع كفاءة الموظف فإن الوزارة تدرك مدى الحاجة لوجود نظام أمني فعّال لحماية المعلومات الرسمية المتداولة بين دوائر هذه الوزارة. ونتيجة لسعي الوزارة الحثيث لتزويد جميع الموظفين بأحدث الأجهزة و المعلومات الرقمية و الأنظمة كأدوات مساعدة لإنجاز الأعمال المتعلقة بمجالات العمل كان لزاما علينا حماية المعلومات وأصولها من الأخطار التي تهددها.

**من أخطاء المستخدمين التي تخل بأمن المعلومات:**

1. كتابة كلمات المرور في مكان معروف.
2. أختيار كلمات مرور ضعيفة.
3. فتح مرفقات البريد الإلكتروني المرسل من قبل الغرباء.
4. ترك أجهزة الحاسب دون أية حماية.
5. إدخال أو تخزين البيانات بصورة غير صحيحة.
6. نشر الفيروسات بوسائل التخزين المتنقلة.
7. توصيل الأجهزة بالكهرباء بدون حماية.
8. الثرثرة بمعلومات هامة في الأماكن العامة.
9. عدم الإبلاغ عن إنتهاكات أمن المعلومات.

**إنتبـــــــــــــــــــــــــه:**

أمن المعلومات ليست مسؤولية فرد وإنما مسؤولية الجميع.

**الباب الثاني: كلمة المرور**

تعد كلمات المرور من المقومات الأساسية في أمن المعلومات، إذ يتم من خلالها التحقق من الهوية، حيث أن معرفة كلمات المرور هي الهدف الأول للمخترقين للحصول على البيانات أو التلاعب بها.

**وتكتب كلمة المرور القوية على النحو التالي:**

1. استخدم ثمانية رموز على الأقل.
2. امزج بها ثلاثة من العناصر التالية:
	1. الأحرف الكبيرة (A-Z).
	2. الأحرف الصغيرة (a-z).
	3. الأرقام (0-9).
	4. علامات الترقيم (-+=\_()\*&^%$#@!)
3. أدخل أخطاء إملائية متعمدة لكل كلمة معجمية تستخدمها.
4. مثال على كلمة مرور قوية: P@ss0rd

**ومن أهم مزايا كلمة المرور القوية أن:**

1. يسهل تذكرها ولا تحتاج أن تدوّن.
2. تتشكل من أحرف وأرقام وعلامات ترقيم.
3. ليست بأسماء ولا تواريخ ولا كلمات معجمية.

ومن المهم ذكره هنا أنه يجب أن يتم تغيير كلمة المرور بين فترة وأخرى لإنه ربما يكون هناك شخص قد استولى على كلمة المرور الخاصة بك.

**إنتبـــــــــــــــــــــــــه:**

اختيارك لكلمة مرور قوية تقيك من التعرض لإختراق حساباتك الوظيفية و الشخصية.

**الباب الثالث: البريد الإلكتروني**

البريد الإلكتروني هو الوسيلة الأساسية للإتصال داخل المؤسسة حيث أنه يستخدم لنقل وتبادل الرسائل عبر الأنترنت، وبما أن عملية نقل البيانات عملية حساسة جداً لذلك فإن سلامة هذه البيانات من الأمور المهمة. وقد انشأت وزارة التربية و التعليم ممثلة في المديرية العامة لتقنية المعلومات نظاماً خاصاً للبريد الإلكتروني ضمن النطاق (moe.om) ومن حق جميع منتسبي الوزارة الحصول على بريد إلكتروني خاص بهم لمساعدتهم في تسهيل أمور العمل بالوزارة.

**وتتمثل مصادر الضرر في رسائل البريد الإلكتروني على النحو التالي:**

1. الملفات المرفقة: رسائل البريد الإلكتروني هي أكثر الطرق أستخداماً من قبل المخربين، لذا تفادى فتح الملفات المرفقة إن لم تعلم مصدرها و تفحصها بمضاد الفيروسات؛ لأنها قد تكون ضاره، لاسيما إن كانت من ملفات التنفيذ أو البرامج مجهولة الصيغ.
2. الرسائل المزعجة: هي ما يكون مصدرها عادة مؤسسات و مواقع تحصل على عنوان بريدك الإلكتروني فتقوم بتبادل هذه العناوين فيما بينها أو تقوم ببيع هذه العناوين بغرض التسويق.
3. الرسائل المتسلسلة: هذه الرسائل تحمل أخباراً مغلوطة وقصصاً مختلقة تطالبك بإرسالها لمن تعرف، ومثال على ذلك كتلك الرسائل التي تحوي في آخرها مقولة أنشر ولك الأجر أو من فضلك اعد إرسال الرسالة.
4. التصيد الإحتيالي: هو أستدراج مستخدمي شبكة الإنترنت إلى مواقع وهمية بإستخدام البريد الإلكتروني في محاولة لسرقة كلمات المرور أو معلومات الحسابات المصرفية أو غيرها من البيانات الحساسة.

**ويجب عند إرسال رسالة بريد إلكتروني أن:**

1. تجعل رسائلك واضحة سهل الفهم.
2. يجب أن تكون واثقاً في الشخص الذي تراسله حتى لا تكون عرضة لتسريب المعلومات.
3. لا تستخدم بريد العمل في إرسال الرسائل الخاصة.
4. لا تستخدم غير البريد الإلكتروني الرسمي لإرسال رسائل أو وثائق رسمية.
5. مسح جميع الرسائل التي يشك في مصدرها أو في محتواها أو في مرفقاتها، وعليه أن يبلغ شعبة أمن المعلومات بالمديرية العامة لتقنية المعلومات عن مرسلها في حالة التكرار.

**إنتبـــــــــــــــــــــــــه:**

1. يمكن استخدام البريد الإلكتروني كبينة أمام القضاء.
2. البريد الإلكتروني وسيلة اتصال رسمية بين المؤسسات.
3. يحسن أن يرفق بكل رسالة بريد رسمية ملاحظة إخلاء مسؤولية.
4. أن لا تستخدم بريدك الألكتروني الرسمي في التسجيل في مواقع الدردشة أو المواقع الإجتماعية.

**الباب الرابع: فيروسات الحاسب الآلي**

الفيروسات هي برامج صغيرة مصممة للإنتقال من جهاز إلى آخر لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات، ويمكن أن تنتشر هذه الفيروسات عبر نظام البريد الإلكتروني كمرفق بريدي أو من خلال أجهزة التخزين المتنقلة أو أجهزة الهواتف الذكية، كما تقوم وزارة التربية و التعليم ممثلة بقسم أمن المعلومات بتوفير برنامج مضاد الفيروسات لجميع موظفي الوزارة وذلك حفاظاً على أمن وسرية البيانات المودعة بأجهزة الوزارة.

**من أهم أعمال الفيروسات**

1. تدمير البيانات.
2. تدمير برامج التشغيل.
3. إنشاء رسائل مزعجة.
4. تشغيل برامج غير مطلوبة.
5. تبطئة سرعة عمل الجهاز.
6. سرقة البيانات كأرقام الحسابات وكلمات المرور أو أرقام بطاقات الائتمان.

**أنواع الفيروسات:**

1. الفيروس: هو برنامج مستنسخ لنفسه، عادة ما يكون قادراً على إحداث ضرر كبير بالملفات والبرامج. لا يستطيع الانتقال ذاتياً، وإنما ينتشر عبر البريد ووسائل التخزين الخارجية.
2. الدودة: هي برنامج مستنسخ لنفسه، تستخدم الشبكة للإنتشار حيث يمكنها الانتقال دون تدخل المستخدم، وتؤدي إلى إشغال موارد الجهاز والشبكة.
3. حصان طروادة: هي شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج المحملة، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته.
4. برامج التجسس: هي برامج تنتشر عند إنزال برامج من الأنترنت وتقوم بجمع معلومات من على حاسبك دون علمك.

**طرق الحماية من الفيروسات:**

1. لا تستخدم برامج مجهولة المصدر.
2. لا تفتح مرفقات بريد مجهول.
3. استخدم برامج الحماية (مضاد الفيروسات) الموثوقة والمحدثة.
4. تحميل الملفات والبرامج من المواقع الموثوق بها فقط.
5. عمل نسخ احتياطية من البيانات دوريًا لأنها قد تساعدك في أستعادة بياناتك في حالة تعرضها للتلف.

**إنتبــــــــــــــــــــــــــــــــــــه:** إن عدم استخدام برامج مضاده للفيروسات قد تعرض جهازك للخطر من قبل الفيروسات التي قد تصيب جهازك، كما ان الحماية من الفيروسات التي تقدمها بعض مواقع الخدمات عبر الأنترنت لا توقف الفيروسات بشكل تام.

**الباب الخامس: النسخ الإحتياطي**

النسخ الاحتياطي هو نقل نسخ مطابقة من الملفات وقواعد البيانات بشكل دوري بهدف حمايتها إن وقعت كارثة، أو لتفادي خسران البيانات في حالة تلفها لأي سبب من الأسباب، وهو يجب ان يكون إجراء روتيني لا يحسن إغفاله حتى على مستوى الاستخدام الشخصي.

**من الأمور التي يمكن أن تؤدي إلى فقدان البيانات :**

* 1. تعطل الأجهزة أو أنظمة التشغيل.
	2. تلف الملفات
	3. حذف الملفات عن طريق خطأ
	4. الإصابة بالفيروسات وأشباهها
	5. سرقة جهاز الحاسب الآلي
	6. الكوارث الطبيعية.

**طريقة عمل النسخ الاحتياطي:**

1. قم بإجراء النسخ الاحتياطي الكامل للجهاز شهرياً.
2. لا تنسخ على أحدث نسخة احتياطية لديك.
3. انسخ ثلاث نسخ احتياطية وعلى وسائط مختلفة، أمثلة " ذاكرة التخزين المتنقلة (فلاش ميموري أو هارديسك).
4. كرر عملية النسخ الاحتياطي الجزئي للبيانات المهمة دورياً.
5. قم بتصنيف وتسمية النسخ الاحتياطية.
6. ضع النسخ الاحتياطية في مكان آمن.
7. احم النسخ الاحتياطية بكلمة مرور متى أمكن ذلك.

**كيف تحدد ما يجب نسخه احتياطا:**

1. قبل أن تبدأ، اعمل قائمة بالملفات التي يجب نسخها، وهذا سيعينك في تحديد ما يجب نسخه ويعطيك قائمة مرجعية عند الحاجة لاستعادة ملف منسوخ.
2. كل ملف مهم ولا يمكن تعويضه بسهولة يجب أن يكون على رأس قائمة النسخ.

**انتبـــــــــــــــــــــــــه:** يعتمد تكرار عملية النسخ الاحتياطي والطريقة التي تستخدمها على أهمية البيانات التي تريد حمايتها.

**الباب السادس: أمن الهواتف الذكية**

في الآونة الأخيرة انتشر استخدام الهواتف الذكية بشكل ملحوظ, وذلك بسبب سهولة حملها و التقنيات الحديثة التي أضيفت للهواتف والتي لم تكن تتواجد إلا في الحاسب الشخصي. فأصبحت تستخدم لتصفح الانترنت,وتخزين ونقل البيانات,والدخول للبريد الالكتروني, ومع هذا التطور فإن المخاطر التي يمكن أن تتعرض لها الهواتف الذكية كثيرة ومنها سرقة أو ضياع الهاتف, أو تعرضه لعمليات الإحتيال الإلكتروني و بالتالي يمكن أن تتسبب في خسائر هائلة.

**من أهم مخاطر الأمان في الهواتف الذكيـــة:**

1. بما أن الهواتف الذكية خفيفة الوزن وغالية الثمن فهي معرضة بشكل كبير للسرقة أو الضياع.
2. يمكن للهواتف الذكية أن تتعرض للفيروسات عن طريق تحميل الملفات من مواقع الانترنت غير الموثوق فيها أو عن طريق البريد الالكتروني.
3. يمكن للهواتف الذكية أن تتعرض للتجسس و التتبع من قبل برامج سرية.
4. يمكن لبرامج الدردشة و التواصل الإجتماعي من إفشاء معلومات وملفات الخصوصية لدى المستخدم.

**طرق حماية مخاطر الهواتف الذكية:**

1. عدم ترك الهاتف في الأماكن العامة ولو كانت الفترة قصيرة.
2. تجنب حفظ أي معلومات حساسة على الهواتف ككلمات المرور أو معلومات عن الحسابات البنكية.
3. فإن كان لابد من ذلك فيجب وضع كلمة مرور قوية لا يمكن تخمينها وتشفير البيانات المهمة.
4. يجب تفعيل البرامج التي تمكن المستخدم من إقفال الجهاز و مسح البيانات و تحديد موقعه وتتبعه عن بعد في حالة ضياعه أو سرقته.
5. تحميل برامج مكافحة الفيروسات و التجسس .
6. يجب على المستخدمين من قراءة سياسة الخصوصية لأي برنامج قبل تثبيه وذلك لتفادي مخاطر تسريب بيانات الخصوصية.

**انتبــــــــــــه:** تتزايد شعبية الهواتف الذكية يوما بعد يوم,
وتزايدت المخاطر حولها فأصبح من الضروري الإلتزام بمعايير الأمان.

**الباب السابع: الهندسة الإجتماعية**

الهندسة الإجتماعية او ما يعرف بفن اختراق العقول هي عبارة عن مجموعة من التقنيات المستخدمة لجعل الناس يقومون بعمل ما أو يفضون بمعلومات سرية. ويتستخدم المهاجم فيها مهاراته الإجتماعية الكلامية مع أشخاص عاملين داخل مؤسسة يملكون الصلاحيات التي تسهل عليه الدخول إلى النظام الخاص بالمؤسسة.

**طرق الإختراق بالهندسة الإجتماعية:**

1. يعمدُ المخترق إلى حيلة سهلة وذلك بأن يسأل أسئلة بسيطة عن طريق الهاتف أو البريد الإلكتروني منتحلا شخصية يمكن الوثوق بها.
2. التصيدُ ويكون بأن يرسل لك بالبريد تنبيهاً من مصرفك مثلاً بأن عليك تغيير كلمة المرور لسبب ما ويعطيك وصلةً مزيفة لموقع المصرف، وعند النقر على الوصلة تجد أن الواجهة هي نفس واجهة المصرف الذي تتعامل معه تماما لكن الذي تجهله أن العنوان مزيف.
3. البحث في القمامة، وهي إحدى طرق الهندسة الإجتماعية والتي تسعى لجمع المعلومات من خلال صناديق القمامة بحثا عن فواتير أو أي مستند به معلومات شخصية أو مصرفية مفيدة.

**طرق الحماية من الهندسة الإجتماعية:**

1. إيجاد سياسة أمنية سليمة لدى المؤسسات لعدم إفشاء البيانات.
2. تقديم عددٍ كافٍ من الدورات التثقيفية للموظفين.
3. على الموظف عدم التردد أبداّ بالسؤال عن هوية طالب المعلومة.
4. عدم الإفصاح عن المعلومات الشخصية أو المالية من خلال البريد الالكتروني إلا عند التأكد من سلامة الأمر.
5. عدم الضغط على أي رابط ببريد الكتروني بقصد تحديث بيانات شخصية.
6. التخلص من الأوراق فور الانتهاء منها باستخدام آلة تقطيع الورق.

**انتبـــــــــــــــــــــــه:** ما نود التنبيه إليه هنا هو أن الاختراق لا يتم بالضرورة باستغلال ثغرات التقنية في نظامك، بل قد يكون باستغلال ثغرات بشرية.

**الباب الثامن: قانون مكافحة جرائم تقنية المعلومات**

**\*\*رابط مرفق للقانون\*\***