الدليل الإسترشادي الخاص بالضوابط الأساسية لأمن المعلومات

قطاع الحوكمة والمعايير

التوثيق والتوزيع

	الاسم	البريد الالكتروني	تاريخ الإصدار
صادر من	قطاع الحوكمة والمعايير	standards@ita.gov.om	2017/7/30
تدقيق	قطاع أمن المعلومات		
معتمد من	**اللجنة التوجيهية**		

قائمة التوزيع	
1. 1	هيئة تقنية المعلومات
.2	كافة الجهات الحكومية المعنية
.3	النشر الالكتروني

تاريخ مراجعة الوثيقة

رقم النسخة	التاريخ	المؤلف	ملاحظات
1.0	2017/7/30	قطاع الحوكمة والمعايير	إعداد الوثيقة

1 قائمة المحتويات

2 المصطلحات

ضوابط التحكم في الدخول	الموافقة على أو رفض الطلبات المتعلقة بـالتالي: (1) الحصول على واستخدام المعلومات والخدمات المرتبطة بمعالجة المعلومات (2) الدخول إلى مرافق مادية معينة (مثل المباني الحكومية ، المؤسسات العسكرية، النقاط الحدودية)
التدقيق	عملية مراجعة مستقلة وفحص للسجلات والأنشطة لتقييم كفاءة ضوابط التحكم في هذه الأنظمة والتأكد من أنها وفق سياسات وإجراءات التشغيل الموضوعة وتتضمن عملية التدقيق تقديم التوصيات بالتغييرات اللازمة في ضوابط التحكم والسياسات والإجراءات.
التهيئة الأساسية	مجموعة من المواصفات للأنظمة وأداة التهيئة ضمن نظام تم مراجعته بشكل رسمي والاتفاق عليه في نقطة معينة من الزمن والذي يمكن تغييره فقط من خلال إجراءات التحكم في التغيير. يتم استخدام عملية التهيئة الأساسية كأساس للبناء عليها في المستقبل وأساس لأي إصدارات أخرى و/أو أي تغييرات تتم.
رفض الخدمة	منع الدخول المصرح به أو تأخير في زمن إنجاز العمليات الحيوي (زمن إنجاز العمليات الحيوية ربما تكون أجزاء من الثانية أو ساعات ويعتمد ذلك على نوعية الخدمة المقدمة)
البرمجيات الخبيثة	برنامج موجود داخل نظام، في الغالب مخفي، الغرض منه التأثير على سرية ومتانة هذا النظام أو الحيلولة دون توفر البيانات أو التطبيقات أو نظام التشغيل للضحية أو التسبب في إزعاج أو تعطيل عمل الضحية
الحادثة	مخالفة أو تهديد وشيك لسياسات أمن الحاسب الآلي، السياسات المتعلقة بالاستخدام المقبول أو ممارسات الأمن القياسية.
خطة الاستجابة للحادثة	مجموعة التعليمات أو الإجراءات المعتمدة لاكتشاف وللاستجابة إلى والحد من تبعات الهجمات السيبرانية الخبيثة على نظام/أنظمة المعلومات لدى المؤسسة
وضع علامات مميزة	معلومات قابلة للقراءة ملحقة بمكونات نظم المعلومات ووسائط التخزين القابلة للمسح أو المخرجات التي تشير إلى القيود على التوزيع ، التعامل مع التحذيرات والعلامات المميزة للأمن المطبقة.

تجميد وسائط التخزين	مصطلح يشير إلى الإجراءات التي تم اتخاذها لجعل البيانات التي تم كتابتها على وسائط تخزين غير قابلة للاسترداد باستخدام الوسائل الاعتيادية وغير الاعتيادية
إدارة التحديثات	الإبلاغ، التعريف، النشر ، التركيب والتدقيق المنتظم على أنظمة التشغيل وإجراء مراجعات لرموز برمجيات التطبيقات . تعتبر هذه المراجعات عمليات تحديث، معالجات سريعة أو جزء من إجراءات الصيانة لهذه الأنظمة.
خطة إصلاح	خطة إصلاح لواحد أو أكثر من التهديدات أو المخاطر التي تواجه أنظمة المؤسسة. تشمل الخطة بشكل أساسي التخلص من التهديدات أو المخاطر وتحديد الأولويات في اتخاذ الإجراءات الإصلاحية
إدارة المخاطر	عملية إدارة المخاطر المتعلقة بالعمليات التنظيمية (بما في ذلك المهمة، الوظائف، الصورة الذهنية أو السمعة)، الأصول التنظيمية أو الفردية التي تنشأ من تشغيل نظام معلومات ويشمل ذلك: 1- القيام بتقييم للمخاطر 2- تنفيذ استراتيجية التخفيف من المخاطر و 3- توظيف التقنيات والإجراءات الخاصة بالمراقبة المستمرة لوضع الأمن في نظام المعلومات.
تحيل الأثر الأمني	التحليل الذي تم القيام به من جانب المسؤول التنظيمي لتحديد مدى تأثير التغيرات في أنظمة المعلومات على الوضع الأمني للنظام.
القابلية للمخاطر	ضعف في النظام، التطبيقات أو الشبكة التي تخضع للاستغلال أو إساءة الاستخدام.

الوثائق المتعلقة

تم استخدام هذه الوثيقة وفقا لقائمة الوثائق المبينة أدناه :

- إطار التصميم المؤسسي لأمن الشبكات الحكومية
- إطار التصميم المؤسسي لأمن الخدمات الالكترونية والتطبيقات الحكومية
- إطار التهيئة وتصميم أمن الأجهزة الذكية والنقاط الطرفية
- دليل سياسة أمن المعلومات – هيئة تقنية المعلومات.

3 الغرض

الغرض من هذه الوثيقة تحديد قواعد الأمن الأساسية التي تضمن توفير إجراءات أمن مناسبة لحماية أصول المعلومات القيمة بالمؤسسات الحكومية في سلطنة عمان. تتضمن هذه الوثيقة قائمة بضوابط التحكم التي يتم استخدامها في نطاقات محددة والتي تعتبر من العناصر الأساسية لوجود برنامج أمن مكتمل لدى المؤسسة الحكومية.

4 الفئة المستهدفة

تم تصميم هذه القواعد الإرشادية لمساعدة المتخصصين في أمن المعلومات بما في ذلك المسؤولين عن أمن المعلومات، العاملين في عمليات أمن تقنية المعلومات، المتخصصين في تقييم وتدقيق الأمن. كما تعتبر هذه القواعد دليل إرشادي للقائمين على تصميم وتطوير الحلول حيث تحدد لهم عناصر الأمن الأساسية التي يجب أن تتوفر عند تصميم منتجاتهم.

5 ضوابط الأمن الأساسية

يجب أن تكون الجهات الحكومية قادرة على توفير الحد الأدنى من ضوابط التحكم في الأمن للوصول إلى مستوى حماية شامل. يجب الإشارة إلى أن التركيز على الضوابط الفنية وحدها لا يضمن الوقاية بشكل فاعل من التهديدات الأمنية ولهذا فإن هذه القواعد تغطي مجموعة كبيرة من الجوانب المتعلقة بالأمن بما يضمن تغطية كافة الجوانب المرتبطة بهذا النطاق. هناك اثني عشر منطقة تعتبر جوهرية وبالتالي قمنا بوضع الخطوط العريضة التي يجب تنفيذها والالتزام بالمحافظة على توافرها بشكل مستمر في المؤسسات الحكومية. تم وضع قائمة بالعديد من الضوابط تحت كل منطقة من هذه المناطق بما يضمن التأكد من توفير الحد الأدنى من مستويات الحماية (تم تلخيصها في قائمة الفحص المذكورة في المرفق).

5.1 التحكم في الدخول

يجب أن يتم التحكم في كافة المستويات بما يسمح بالدخول المصرح به لموارد المؤسسة. يجب تحديد السياسات والإجراءات وصيانتها وإدارة حسابات الأنظمة والمستخدمين ومراقبتها بشكل جيد كما يجب تفعيل إجراءات معينة لضمان الوصول إلى وتدفق المعلومات بشكل فاعل .يجب كذلك أن تكون هناك إجراءات معينة للتأكد من الفصل في المهام مع إعطاء المستخدمين المستوى الأدنى من صلاحيات الدخول بحساباتهم للقيام بالواجبات المطلوبة منهم. يجب كذلك تفعيل واستخدام الإشعارات الخاصة باستخدام الأنظمة بغرض مراقبة الاستخدام. يجب كذلك تنفيذ إجراءات معينة للتأكد من أن الاتصالات التي تتم من خلال التوصيلات عن بعد، واللاسلكية آمنة. يجب التحكم في استخدام الأجهزة المتنقلة في شبكة المؤسسة من خلال تحديد الاستخدام المقبول عند الدخول بالوسائل اللاسلكية.

5.2 التوعية والتدريب

يجب على المؤسسات الحكومية أن تطور سياسات أمن للمستخدم تصف الاستخدام الآمن والمقبول لأنظمة تقنية المعلومات والاتصالات داخل المؤسسة ويجب الموافقة عليها بشكل رسمي في شروط وأحكام عقد العمل. يجب تدريب كافة المستخدمين بشكل منتظم على التعامل مع مخاطر الأمن التي قد تواجههم سواء كأفراد أو موظفين. هناك بعض الوظائف المتعلقة بالأمن (مثل المسؤولين عن النظام ، أعضاء فريق إدارة حوادث تقنية المعلومات والمحققين القانونيين) التي تحتاج إلى تدريب متخصص.

5.3 إدارة الحوادث

يجب أن تتوفر لدى المؤسسة الإمكانات والقدرات للتعامل مع والتعافي من الكوارث والحوادث التي يمكن أن تحدث. يجب اختبار خطة إدارة الحوادث (بما في ذلك خطة استمرارية الأعمال والتعافي من الحوادث) بشكل منتظم. يحتاج فريق الاستجابة للحادثة إلى تدريب متخصص على مختلف الجوانب الفنية وغير الفنية. يجب تحديد آلية الإبلاغ عن الحوادث واتباعها في مختلف

التخصصات بما يسمح باتخاذ الإجراءات التصحيحية والعلاجية وكذلك المساعدة في الالمام بأنماط التهديدات بما يساعد في تحديد خطة الاستجابة المطلوبة للحادثة.

5.4 حماية وسائط التخزين

يجب تحديد وتنفيذ السياسات الخاصة بوسائط التخزين القابلة للإزالة والتي تتحكم في استخدام وسائط التخزين القابلة للإزالة في جلب ونشر المعلومات. عندما يكون ليس هناك مفر من استخدام وسائط تخزين قابلة للإزالة فإنه يجب تحديد نوعية وسائط التخزين القابلة للإزالة التي يمكن استخدامها مع المستخدمين والأنظمة ونوعية المعلومات التي يمكن نقلها. يجب عمل مسح لكافة وسائط التخزين باستخدام ماسح لوسائط التخزين لاكتشاف أي فيروسات خبيثة قبل تنزيل أي بيانات على نظام المؤسسة. يجب وضع علامات مميزة على كافة وسائط التخزين ويجب حفظها ونقلها بشكل آمن بما يضمن حماية المعلومات التي يتم نقلها عبرها. عندما لا تكون هناك حاجة للبيانات الموجودة داخل وسائط التخزين، يجب استخدام طرق فاعلة للتخلص منها.

5.5 إدارة التهيئة

يجب على الشركات أن تقوم بإعداد وتوثيق وصيانة عمليات التهيئة الأساسية الحالية التي تغطي كافة أنظمة المعلومات وأجهزة الشبكة. يجب توضيح العمليات المتعلقة بإدارة التغيير وتحديد الخطوات لاعتماد هذه التغييرات كما يجب تحليل الأثر الأمني لأي تغيير يتم للحد من المخاطر المرتبطة بتنفيذ أي تغيرات.

5.6 تقييم المخاطر

الجهات الحكومية هي المسؤولة عن تقييم المخاطر المتعلقة بأصول المعلومات بنفس المستوى الذي تقيم به المخاطر التشغيلية أو المالية أو التنظيمية. لتحقيق ذلك، يجب على هذه الجهات وضع نظام لإدارة مخاطر المعلومات في المؤسسة يحظى بدعم من مجلس الإدارة والإدارة العليا إلى جانب وضع تصميم فاعل لجودة المعلومات. يجب على المؤسسة أن تدرس إمكانية تعميم سياسة إدارة المخاطر على العاملين في المؤسسة للتأكد من أن الموظفين والمقاولين والموردين على علم

بحدود الإدارة المتعلقة بالمخاطر التشغيلية. يجب عليهم كذلك إجراء عمليات تقييم للأمن بشكل منتظم والقيام بمسح للثغرات الموجودة في مواعيد محددة لمراقبة حالة ضوابط التحكم الفنية. يجب أن تغطي عمليات التقييم التي يتم القيام بها عمل تصنيف للجوانب المتعلقة بالأمن بحيث تبرز الاكتشافات الرئيسية التي يجب التعامل معها عند إعداد التقرير.

5.7 أمن شبكة المعلومات

يجب على المؤسسات المختلفة أن تتبع المبادئ المعتمدة لتصميم الشبكة والمبينة في " إطار التصميم المؤسسي لأمن الشبكة الحكومية" الذي أعدته هيئة تقنية المعلومات عندما قامت بتهيئة قطاعات حدود الشبكة الداخلية ويجب على هذه الجهات التأكد من أن كافة أجهزة الشبكة مهيئة لتوفير متطلبات الأمن الأساسية التي تم إعدادها. كما يجب أن تقوم المؤسسة بفرز (فلترة) الحركة التي تتم في حدود الشبكة بحيث يُسمح فقط بالأنشطة التي تدعم عمل المؤسسة ويجب عليها مراقبة هذه الحركة بشكل مستمر لاكتشاف أي نشاط غير معتاد أو خبيث داخل إلى إو خارج من الشبكة والذي ربما يؤشر على وجود هجوم (أو محاولة هجوم).

5.8 حماية الأنظمة والاتصالات

يجب أن يكون لدى الجهات سياسة محددة لتنفيذ الضوابط الأمنية التي تحمي النظم والاتصالات في هذه المؤسسة ويجب أن يكون لديها كذلك خريطة واضحة ومحددة المعالم لحدودها بما يضمن تحديد كافة ضوابط التحكم والمراقبة لحماية أي اتصالات واردة من الأطراف الخارجية على أنظمتها الداخلية الأساسية. يجب أن تقوم هذه الجهات بفصل البيئة الداخلية لها من الشبكة العامة وعليها تنفيذ ضوابط رقابة فاعلة للحد من أو خفض أثر أي هجوم لمنع الخدمة يمكن أن يؤدي إلى تعطيل الأنظمة. يمكن للمؤسسات الحكومية أن تلجأ إلى التشفير لدعم حلول الأمن المختلفة بما في ذلك (حماية المعلومات المحظورة والسرية، توفير التوقيعات الالكترونية وتصنيف المعلومات عندما يكون لدى الأشخاص المصرح لهم التصاريح اللازمة للاطلاع على هذه المعلومات ولكن لا تتوفر لهم الموافقات الرسمية للولوج إلى المعلومات).

يجب على الجهات المعنية أن تتأكد من توفير ضوابط فاعلة لإدارة التحديث لكافة الأنظمة والأجهزة الموجودة لديها بما يضمن تحديث الأنظمة الموجودة لديها بشكل مستمر وعلى هذه الجهات تنفيذ الحماية اللازمة ضد الفيروسات الخبيثة على كافة أجهزة الحاسب الآلي أو الأجهزة الأخرى المعرضة لها أيضا. يمكن للجهات المعنية أن تسترشد بـ " End Point Security Framework " الذي أعدته الهيئة لمعرفة مزيد من التفاصيل حول حماية الأنظمة.

5.9 التقييم الأمني والتفويض

يجب على المؤسسة الحكومية أن يكون لديها سياسة محددة لتقييم الأمن وتفويض الصلاحيات بما يغطي الغرض والمجال والادوار والمسؤوليات والتزامات الإدارة والتنسيق بين الجهات التنظيمية والالتزام. على هذه الجهات إما أن يكون لديها سياسة مستقلة خاصة بها أو أن تكون هذه السياسة موجودة ضمن السياسة العامة للأمن في هذه الجهات. يجب على هذه الجهات أيضا أن تنفذ ضوابط التفويض المطلوبة لإجراء تقييم للأمن.

يجب تنفيذ عمليات تقييم مستوى الأمن بشكل منتظم بما يضمن تقييم المكونات المختلفة لنظام تقنية المعلومات وفق الإجراءات المبينة في التعميم الوزاري رقم 2017/1. يجب أيضا تحديد ضوابط التحكم في التفويض لإجراء الاختبارات المطلوبة جنبا إلى جنب مع هذه العمليات كما يجب إجراء اختبارات تدقيق لمتابعة تنفيذ خطة العلاج.

5.10 الحماية البيئية والمادية

يجب عل المؤسسات الحكومية أن تحدد السياسة والإجراءات الخاصة بالحماية المادية والبيئية ويجب عليها تنفيذ ضوابط التحكم المطلوبة للتأكد من أن الدخول مصرح به وأنه آمن مع المراقبة الفاعلية للعمليات التي تتم. يجب على المؤسسات تنصيب أنظمة منع ووقاية مثل نظام الوقاية من الحريق، الأنوار الطارئة، ضوابط التحكم في درجة الحرارة والرطوبة.

5.11 أمن الأفراد

يجب أن يكون لدى الجهات المعنية سياسة وإجراءات خاصة بالتعامل مع موظفي الأمن. يجب تنفيذ إجراءات التحكم في الأمن في كافة مراحل التوظيف التي تشمل فرز الموظفين، إكمال الإجراءات، إنهاء خدمات الموظفين، النقل من وحدة إلى أخرى داخل المؤسسة. يجب التحقق من ضوابط التحكم في دخول الموظفين عند أي تغيير في الوضع الوظيفي للموظف. يجب أن يغطي أمن الموظفين ضوابط التحكم المرتبطة بموظفي الأطراف الخارجية الذين يتطلبون اعتبارات مختلفة خاصة.

5.12 التدقيق والمسائلة

يجب على مختلف الجهات أن يكون لديها سياسة وإجراءات محددة للتدقيق والمسائلة كما يجب إجراء التدقيق بشكل منتظم على كافة الجوانب التي تغطيها سياسات الأمن لديها. يجب أن يتم وضع تقارير التدقيق بشكل مسبق حيث أنه يجب تمكين كافة سجلات التدقيق على كافة الأنظمة والأجهزة المزودة بآليات لإعداد التقارير للحصول على فعاليات وسجلات التدقيق المطلوبة. يجب حماية معلومات التدقيق وإتاحتها للمراجعة والتحليل. يجب أن يتم إبلاغ نتائج التقارير وعمليات التدقيق لتعزيز مستويات السلامة والإلمام بها.

6 المرفقات

6.1 قائمة فحص ضوابط الأمن الأساسية

ضوابط التحكم	التحكم في الدخول	الوضع الحالي
AC.1	سياسة وإجراءات التحكم في الدخول	
AC.2	إدارة الحساب	
AC.3	إنفاذ الدخول	
AC.4	إنفاذ تدفق المعلومات	
AC.5	فصل المهام	
AC.6	امتيازات وصول أقل	
AC.7	الإشعار باستخدام النظام	
AC.8	عن بعد	
AC.9	دخول لاسلكي	
AC.10	التحكم في الدخول من خلال الأجهزة النقالة	
AC.11	استخدام أنظمة المعلومات الخارجية	
هوية التحكم	**التدريب والوعي الأمني**	
SAT.1	سياسة وإجراءات الوعي الأمني والتدريب	
SAT.2	التدريب الخاص بالوعي الأمني	
SAT.3	التدريب الأمني المبني على الأدوار	
هوية التحكم	**التدقيق والمساءلة**	
AA.1	سياسة وإجراءات التدقيق والمساءلة	
AA.2	وقائع لتدقق	
AA.3	محتوى سجلات التدقيق	
AA.4	التدقيق على سعة التخزين	
AA.5	الاستجابة لأوجه القصور في عمليات التدقيق	
AA.6	إعداد التقرير والتحليلات المراجعة للتدقيق	
AA.7	أختام الوقت	
AA.8	حماية معلومات التدقيق	
AA.9	إنشاء التدقيق	
هوية التحكم	**تفويض وتقييم الأمن**	
SAA.1	سياسات وإجراءات تقييم وتفويض الأمن	
SAA.2	عمليات تقييم الأمن	

SAA.3	الربط البيني بين الأنظمة	
هوية التحكم	**إدارة التهيئة**	
CM.1	سياسة وإجراءات إدارة التهيئة	
CM.2	التهيئة الأساسية	
CM.3	التحكم في تهيئة التغيير	
CM.4	تحليل الأثر الأمني	
CM.5	إعدادات التهيئة	
CM.6	أقل مستوى من العمليات	
CM.7	جرد مكونات نظم المعلومات	
CM.8	القيود على استخدام البرمجيات	
هوية التحكم	**الاستجابة للحادثة**	
IR.1	سياسة وإجراءات الاستجابة للحادثة	
IR.2	التدريب على الاستجابة للحادثة	
IR.3	التعامل مع الحادثة	
IR.4	مراقبة الحادثة	
IR.5	الإبلاغ عن الحادثة	
IR.6	المساعدة في الاستجابة للحادثة	
IR.7	خطة الاستجابة للحادثة	
هوية التحكم	**حماية وسائط التخزين**	
MP.1	سياسة وإجراءات حماية وسائط التخزين القابلة للإزالة	
MP.2	الدخول إلى وسائط التخزين القابلة للإزالة	
MP.3	وضع علامات على وسائط التخزين القابلة للإزالة	
MP.4	حفظ وسائط التخزين القابلة للإزالة	
MP.5	نقل وسائط التخزين القابلة للإزالة	
MP.6	التخلص من وسائط التخزين القابلة للإزالة	
MP.7	استخدام وسائط التخزين القابلة للإزالة	
التحكم في الهوية	**الحماية البيئية والمادية**	
PEP.1	سياسة وإجراءات الحماية البيئية والمادية	
PEP.2	عمليات التفويض للدخول المادي	
PEP.3	التحكم في الدخول المادي	
PEP.4	مراقبة الدخول المادي	

PEP.5	الإضاءة في حالة الطوارئ	
PEP.6	الوقاية من الحريق	
PEP.7	ضوابط التحكم في درجة الحرارة والرطوبة	
PEP.8	الوقاية من حدوث تلف بسبب المياه	
PEP.9	التوصيل والإزالة	
هوية التحكم	**أمن الموظفين**	
PS.1	سياسة وإجراءات أمن الموظفين	
PS.2	فرز الموظفين	
PS.3	إنهاء خدمات الموظفين	
PS.4	نقل الموظفين	
PS.5	اتفاقيات الدخول	
PS.6	الأمن الخاص بموظفي الأطراف الخارجية	
هوية التحكم	**تقييم المخاطر**	
RA.1	سياسة وإجراءات تقييم المخاطر	
RA.2	تصنيف الأمن	
RA.3	تقييم المخاطر	
RA.4	مسح لنقاط الضعف	
هوية التحكم	**حماية الأنظمة والاتصالات**	
SCP.1	سياسة وإجراءات حماية الأنظمة والاتصالات	
SCP.2	حماية الحدود	
SCP.3	الحماية ضد منع الخدمة	
SCP.4	شهادات البنية الأساسية الرئيسية العامة	
SCP.5	الحماية من البرمجيات الخبيثة	
SCP.6	إدارة التحديثات	

7 المراجع

1. التعميم الوزاري رقم 1/2017 حول ضرورة إجراء التقييم الامني للتطبيقات والخدمات الإلكترونية

2. كيسي، آر، "معجم مصطلحات أمن المعلومات الرئيسية"، نيستير 7298، المراجعة الثانية، 2013.