سياسة إدارة أمن المعلومات

الفهرس

مقدمة

يعتبر تنفيذ خطة عُمان الرقمية جزءاً من مسؤوليات وزارة التقنية والاتصالات حسب المرسوم السلطاني رقم 52/2006 ، إلى جانب دورها القيادي للمؤسسات الحكومية في المجال الرقمي

لقد أصبحت "المعلومات" ركيزة أساسية لنجاح المؤسسات في أي قطاع، ولحماية هذه المعلومات يجب اتخاذ التدابير الاحترازية اللازمة للحفاظ على أمن هذه المعلومات.

وتعرّف المعلومات بأنها البيانات المصاغة على شكل حقائق أو أفكار أو المعرفة التي يمكن تناقلها بشكل عام.

وعليه يعرّف أمن المعلومات بأنه حماية المعلومات وأنظمة المعلومات من العمليات الغير مصرحة مثل الوصول والاستخدام والكشف والعرقلة والتعديل والإتلاف، من أجل ضمان سرية وسلامة وتوفر هذه المعلومات.

مع الأخذ بالاعتبار ما سبق ذكره، تقوم وزارة التقنية والاتصالات بنشر "سياسة أمن المعلومات" ليتم استخدامها في مختلف وحدات الجهاز الإداري للدولة ولتساعد في تحقيق الاستخدام الآمن للمعلومات.

الهدف من الوثيقة

الهدف من هذه الوثيقة هو توحيد الاتجاهات وتوجيه وحدات الجهاز الإداري للدولة لإتباع أهم الممارسات الإدارية والتنظيمية في مجال إدارة برنامج أمن المعلومات الخاص بها.

نطاق العمل

تنطبق هذه الوثيقة على جميع وحدات الجهاز الاداري للدولة كونها القائمة على رعاية هذه البيانات باسم سلطنة عُمان.

المصطلحات

تستند سياسة أمن المعلومات على المبادئ التالية:

توفر المعلومات: إمكانية الوصول إلى المعلومات واستخدامها من الجهات المخوّلة.

سلامة المعلومات: حماية المعلومات من حيث الدقة والاكتمال.

سرية المعلومات: الحفاظ على عدم الكشف أو توفير المعلومات إلى الجهات والأفراد والعمليات الغير مخوّلة.

نسبية المعلومات: مدى ارتباط التدابير الأمنية مع المخاطر المتعلقة بعدم توفر المعلومات أو سلامتها أو سريتها.

البيانات التعريفية

5.1. حوكمة أمن المعلومات

يجب على وحدات الجهاز الإداري للدولة تشكيل لجنة أمن المعلومات مكونة من أعضاء من الإدارة العليا، أو تكليف إحدى لجان الإدارة العليا الحالية للقيام بهذا الدور.
ويجب أن يرأس هذه اللجنة الرئيس التنفيذي أو رئيس المؤسسة أو وكيل الوزارة وأن تتضمن ممثلين عن الإدارات العليا من الأقسام المختلفة من المالية والموارد البشرية والمدراء التنفيذيين والإداريين ومدراء تقنية المعلومات.
تتحمل هذه اللجنة مسؤولية تحديد "سياسة أمن المعلومات"*[1] ضمن المؤسسة*[2] بالإضافة للمسؤوليات التالية:

- إدارة التطوير والتغييرات في برنامج أمن المعلومات
- إدارة تنفيذ برنامج أمن المعلومات
- إسناد المسؤوليات المتعلقة بالبرنامج إلى الموظفين حسب اختصاصاتهم:
  - تعيين مسؤول أمن المعلومات
  - تعيين تبعية مسؤول أمن المعلومات بشكل مباشر إلى رئيس المؤسسة
- التحكم بتغيرات وتنفيذ خطة التواصل الخاصة بأمن المعلومات في المؤسسة
- عقد الاجتماعات اللازمة لمراجعة فعالية برنامج أمن المعلومات مع مسؤول أمن المعلومات والفريق الأمني على الأقل بشكل ربع سنوي.

5.2. إدارة المخاطر

يجب وحدات الجهاز الإداري بالدولة القيام بتقييم المخاطر الأمنية*[3] بشكل دوري وتنفيذ المعالجة المناسبة والمتناسبة مع مستوى المخاطر المحددة. كما يجب على وحدات الجهاز الإداري للدولة تحديد المخاطر وحجمها وأولوياتها حسب معيار قبول المخاطر الذي يتم تحديده من قبل اللجنة التوجيهية، وتطبيق الضوابط المناسبة للحماية من هذه المخاطر.

---

*1. يجب تحديد سياسة أمن المعلومات في وحدات الجهاز الإداري للدولة كل على حدة بما يتوافق مع المتطلبات الأمنية المرتبطة بالأهداف الخاصة بهذه المؤسسة.
*2. قصد بالمؤسسة هنا جميع الجهات الحكومية والوزارات الحكومية والهيئات والوحدات الحكومية المحلية.
*3. يمكن الرجوع إلى "إطار عمل إدارة مخاطر تقنية المعلومات", هيئة تقنية المعلومات.

5.3. تصنيف البيانات

يجب على وحدات الجهاز الإداري للدولة القيام بتطبيق التصنيفات المناسبة للبيانات:

- تطبيق تصنيفات أمن المعلومات *[4]
- التحكم بالوصول المادي لأصول المعلومات
- التحكم باستخدام تقنية المعلومات والاتصالات

5.4. التدريب والتوعية

يجب على وحدات الجهاز الإداري للدولة التأكد من إلمام الموظفين بالمهام والمسؤوليات الموكلة إليهم فيما يخص جوانب أمن المعلومات المختلفة من خلال:

- تحقيق المستوى التدريبي المناسب لمسؤول أمن المعلومات والفرق الأخرى المعنية بتطبيق الضوابط الأمنية.
- المحافظة والإستمرار على تنفيذ خطط التوعية والتواصل مع الموظفين حسب مسؤولياتهم اتجاه اتباع الممارسات التي تسنها السياسات الخاصة ببرنامج أمن المعلومات داخل المؤسسة.

---

*4. تصنيفات أمن المعلومات حسب:

1. المرسوم السلطاني 2011/118 "قانون تصنيف البيانات"
2. 2015/42 – تعديل قانون تصنيف البيانات
3. 2019/26 – تعديل قانون تصنيف البيانات
4. ترابط تصنيفات أمن أنظمة البيانات والمعلومات – هيئة تقنية المعلومات

5.5. إدارة الحوادث

يجب على الجهات الحكومية التأكد من وجود منهجية منظمة لإدارة حوادث أمن المعلومات ودعم أهداف البرنامج الأمني:

- يجب على المؤسسات تنفيذ الضوابط الملائمة والمحافظة عليها من أجل تقليل المخاطر المحددة من خلال عمليات إدارة الحوادث الأمنية وتقييم المخاطر.

5.6. إدارة استمرارية البيانات

لابد من وجود منهجية منظمة تستند إلى تقييم مخاطر أمن المعلومات لإدارة استمرارية تقنية المعلومات وضمان توافر الموارد الهامة دون انقطاع من أجل دعم الأنشطة الأساسية للمؤسسة.

- يجب على كل مؤسسة تنفيذ ودعم الضوابط الإدارية لاستمرارية تقنية المعلومات والتي تحقق المتطلبات التي يحددها اتقييم الخاص لمخاطر أمن المعلومات.

6. المهام والمسؤوليات

6.1 إدارة وثيقة السياسة

1. يتم إصدار هذه السياسة من قبل وزارة التقنية والاتصالات
2. تعود ملكية ومراجعة سياسة حوكمة تقنية المعلومات الى وزارة التقنية والاتصالات.

6.2 تنفيذ السياسة

1. يتحمل رئيس الوحدة مسؤولية تنفيذ سياسة أمن المعلومات والالتزام ببرنامج التنفيذ المذكور في الجدول المدرج تحت قسم برنامج التنفيذ (القسم التالي رقم 7).
2. وزارة التقنية والاتصالات بعملية التدقيق للتحقق من الالتزام بسياسة أمن المعلومات ورفع تقارير التحسينات اللازم إجراؤها في حوكمة تقنية المعلومات والترتيبات الإدارية إلى مجلس الوزراء.

7. برنامج التنفيذ

1. توزيع المهام والمسؤوليات من خلال المخاطبات الرسمية (أول 3 أشهر).
2. تحديد سياسة أمن المعلومات الخاصة بكل وحدة حكومية (أول 3 أشهر).
3. إعداد وتأسيس برنامج أمن المعلومات (6 أشهر).

أعمال المؤسسة	تاريخ الإنجاز (ابتداءً من تاريخ نشر هذه الوثيقة)
1. توزيع المهام والمسؤوليات من خلال المخاطبات الرسمية	3 أشهر
2. تحديد سياسة أمن المعلومات لكل مؤسسة على حدة *[5]	3 أشهر
3. وضع برنامج أمن المعلومات	6 أشهر

*5. تعميم هيئة تقنية المعلومات: 3-2015 "السياسة العامة لأمن المعلومات"
تعميم هيئة تقنية المعلومات: 1-2017 "تقييم أمن التطبيقات والخدمات الإلكترونية"

8. الإصدارات ذات الصلة

1- المرسوم السلطاني 2011\118 "قانون تصنيف البيانات"
2- 2015/42 – تعديل قانون تصنيف البيانات
3- 2019/26 – تعديل قانون تصنيف البيانات
4- سياسة حوكمة تقنية المعلومات - هيئة تقنية المعلومات (ITA) سابقاً، وزارة التقنية والاتصالات حاليا
5- الدليل الارشاي لتنفيذ سياسة حوكمة تقنية المعلومات - هيئة تقنية المعلومات (ITA) سابقاً، وزارة التقنية والاتصالات حاليا
6- إطار عمل إدارة أمن المعلومات - هيئة تقنية المعلومات (ITA) سابقاً، وزارة التقنية والاتصالات حاليا
7- إطار عمل استمرارية خدمات تقنية المعلومات - هيئة تقنية المعلومات (ITA) سابقاً، وزارة التقنية والاتصالات حاليا
8- ترابط تصنيفات أمن أنظمة البيانات والمعلومات – هيئة تقنية المعلومات (ITA) سابقاً، وزارة التقنية والاتصالات حاليا
9- تعميم هيئة تقنية المعلومات: 3-2015 "السياسة العامة لأمن المعلومات"
10- تعميم هيئة تقنية المعلومات: 1-2017 "تقييم أمن التطبيقات والخدمات الإلكترونية"