سياسات / وزارة الصحة

دليل الإجراءات القياسية للأمن السيبراني الشامل (أمن المعلومات وضبط الأصول والأمن المادي وأمن الأفراد ودورة حياة البيانات)	رمز الوثيقة: MOH | SOP | D | IM | 16
عدد الصفحات : 23 صفحة	الطبعة: الأولى

الإعداد: قسم إدارة المخاطر والحوكمة السيبرانية		المعنيين بالوثيقة: كافة المنشآت التابعة لوزارة الصحة.
د. أمل الشافعي	التوقيع:	
م. ق داليا زياد	التوقيع:	
تاريخ الإعداد:	٢٠٢٤/٢/١٨	
التدقيق والمراجعة: مدير مديرية التحول الإلكتروني وتكنولوجيا المعلومات	التوقيع:	تاريخ التدقيق: ٢٠٢٤/٢/٢٢
التدقيق من ناحية ضبط الجودة: مديرية التطوير المؤسسي وضبط الجودة د. صفاء منير العوران	التوقيع:	تاريخ تدقيق ضبط الجودة: ٢٠٢٤/٢/٢٧
الاعتماد: الأمين العام للشؤون الإدارية والفنية	التوقيع:	تاريخ الاعتماد: ٢٠٢٤/٢/٢٩

وزارة الصحة
مديرية التطوير المؤسسي و ضبط الجودة
السياسات و الإجراءات
Policies & Procedures
ختم الإعتماد

Approved

تتم مراجعة الدليل كل سنتين على الأقل من تاريخ اعتماد آخر طبعة:

رقم الطبعة	تاريخ الاعتماد	مبررات مراجعة الدليل

ختم النسخة الاصلية

MASTER COPY

دليل الإجراءات القياسية للأمن السيبراني الشامل (أمن المعلومات وضبط الأصول والأمن المادي وأمن الأفراد ودورة حياة البيانات)	رمز الوثيقة: MOH SOP D IM 16
عدد الصفحات : 23 صفحة	الطبعة: الأولى

المقدمة

توفير إطار شامل لحماية الأصول المادية والرقمية وبيانات وزارة الصحة في كافة مراحلها، من الإنشاء وحتى الإتلاف. يعزز هذا الدليل تكامل الأمن المادي وأمن المعلومات وأمن الأفراد، مع ضبط الأصول وتطبيق دورة حياة البيانات لضمان سلامتها واستمرارية العمل وتقليل المخاطر.

الأهداف

1. حماية الأصول والبيانات من التهديدات المادية والرقمية.
2. ضمان سرية وسلامة وتوافر البيانات والأصول.
3. تطبيق تصنيفات الأصول والبيانات وضمان توافق الحماية مع حساسية المعلومات.
4. رفع وعي الموظفين بشأن حماية البيانات والأصول في كافة مراحل دورة حياتها.
5. تنفيذ أفضل الممارسات في إدارة أمن الأفراد وصلاحيات الدخول لمنع الوصول غير المصرح به إلى الأصول الحساسة.
6. تقليل المخاطر الناتجة عن التهديدات الداخلية من خلال تنفيذ سياسات أمن الأفراد بفعالية.

النطاق

يشمل هذا الدليل:

1. جميع الموظفين، المقاولين، والشركاء المتعاملين مع بيانات وأصول الوزارة.
2. جميع الأصول المادية مثل الأجهزة والمعدات والبنية التحتية.
3. البيانات الورقية والرقمية في كافة مراحل دورة حياتها.
4. الأنظمة والشبكات المرتبطة بوزارة الصحة.

MASTER COPY

دليل الإجراءات القياسية للأمن السيبراني الشامل (أمن المعلومات وضبط الأصول والأمن المادي وأمن الأفراد ودورة حياة البيانات)	رمز الوثيقة: MOH SOP D IM 16
عدد الصفحات : 23 صفحة	الطبعة: الأولى

التعريفات

1. **الأمن السيبراني:** الإجراءات المتخذة لحماية الأنظمة والشبكات المعلوماتية والبنى التحتية الحرجة من حوادث الأمن السيبراني والقدرة على استعادة عملها واستمراريتها سواء أكان الوصول إليها بدون تصريح أو سوء استخدام أو نتيجة الإخفاق في اتباع الإجراءات الأمنية أو التعرض للخداع الذي يؤدي لذلك. (قانون رقم 16 لسنة 2019، قانون الأمن السيبراني.)
2. **التهديد السيبراني:** أي نشاط أو حدث متعمد أو غير متعمد يهدد سرية، سلامة، أو توافر البيانات أو الأنظمة، بما يشمل الهجمات السيبرانية التقليدية والمتطورة مثل هجمات الفدية والهجمات التي تعتمد على الذكاء الاصطناعي.
3. **الحادث السيبراني** (Cyber Incident) أي حدث يؤدي إلى تأثير غير مقصود أو غير مصرح به على سرية، سلامة، أو توافر الأصول الرقمية أو الشبكات.
4. **الأمن المادي:** الإجراءات التي تهدف إلى حماية المواقع والمرافق المادية من الوصول غير المصرح به، بالإضافة إلى الحماية من التهديدات البيئية مثل الحرائق والكوارث الطبيعية أو أي مخاطر قد تؤثر على استمرارية العمل وسلامة الأصول.
5. **أمن الأفراد:** مجموعة السياسات والإجراءات القياسية التي تهدف إلى حماية الأصول من التهديدات الداخلية من خلال تعزيز النزاهة، الامتثال، وبناء ثقافة أمنية واعية بين جميع الأفراد المرتبطين بالوزارة، مع توضيح الجزاءات المترتبة على عدم الامتثال.
6. **أمن المعلومات:** مجموعة الإجراءات والسياسات التي تهدف إلى ضمان سرية، سلامة، وتوافر البيانات الرقمية والورقية أثناء معالجتها، تخزينها، ونقلها، بما يشمل الحماية من التهديدات السيبرانية التقليدية والمتطورة.
7. **دورة حياة البيانات:** المراحل التي تمر بها البيانات منذ إنشائها أو جمعها، مرورًا بالتخزين، الاستخدام، النقل، والمشاركة، وصولًا إلى الإتلاف الآمن، بما يضمن حماية البيانات طوال هذه الدورة وفق المعايير الأمنية المعتمدة.
8. **الأصول:** كل الممتلكات المادية، الرقمية، وغير الملموسة للوزارة، بما في ذلك الأجهزة، البيانات، البرمجيات، البنية التحتية السحابية، وأي موارد تقنية أخرى تُستخدم لتحقيق الأهداف المؤسسية.
9. **تصنيف البيانات:** تقسيم البيانات إلى مستويات حساسية بناءً على تأثير فقدانها أو اختراقها، مثل (سري للغاية، حساس، خاص، عام)، مع تطبيق المعايير الوطنية والدولية في التصنيف لضمان توفير الحماية المناسبة لكل مستوى.
10. **العلامات الوقائية:** علامات مادية أو رقم (Digital Tags) تستخدم لتحديد مستوى حساسية الأصول ومتطلبات الحماية الخاصة بها وفق التصنيف المعتمد، بهدف منع الوصول غير المصرح به أو الاستخدام الخاطئ.

11. **ضوابط تقييد الدخول:** الإجراءات التي تحدد وتقيّد دخول الأفراد (موظفين أو زائرين) إلى المواقع أو الأنظمة بناءً على الأدوار الوظيفية، متطلبات العمل، ومستوى الأمان المطبق، باستخدام وسائل مادية أو رقمية مثل الأقفال البيومترية وأنظمة التحكم في الوصول.
12. **المواقع الآمنة:** جميع المواقع التي تحتوي على بيانات أو أصول حساسة والتي يتم تقييد الوصول إليها بناءً على مستويات الأمان المطلوبة، مثل مراكز البيانات، مكاتب الإدارة العليا، أو مواقع تخزين الوثائق والأجهزة.
13. **التحكم في الوصول:** الإجراءات المتخذة لتقييد وتحكم الوصول إلى المواقع، الأصول، المعلومات، والأنظمة بناءً على أدوار وصلاحيات المستخدمين، بما يشمل تحديد من يمكنه الوصول إلى الموارد المختلفة وكيفية استخدام هذه الموارد بشكل آمن.
14. **الوسائل الدفاعية المتعمقة:** نهج متعدد الطبقات لتوفير حماية شاملة ضد الاختراقات والتهديدات السيبرانية باستخدام تقنيات الحماية المادية، التقنية، والإجرائية، بما يعزز قدرة الأنظمة على الصمود أمام الهجمات.
15. **الحوسبة السحابية** (Cloud Computing): نموذج لتوفير الخدمات الحاسوبية بما يشمل تخزين البيانات ومعالجتها عبر الإنترنت باستخدام موارد افتراضية آمنة وفق معايير الأمن السيبراني.
16. **التشفير** (Encryption): عملية تحويل البيانات إلى صيغة مشفرة لا يمكن قراءتها إلا بواسطة الأطراف المصرح لها باستخدام مفاتيح فك التشفير.
17. **إدارة الوصول** :(Access Management) مجموعة السياسات والأدوات المستخدمة لتحديد وضبط صلاحيات الأفراد للوصول إلى الأصول الرقمية والمادية بناءً على الحاجة الوظيفية.
18. **أنظمة كشف التسلل ومنعه** :(IDS/IPS) أدوات تقنية متخصصة لمراقبة الأنشطة المشبوهة على الشبكات والأنظمة مثل الجدران النارية (Firewall) وتنبيه الإدارة الأمنية أو اتخاذ إجراءات تلقائية لمنع الهجمات.

[redacted]

1. الأجهزة الإلكترونية.
2. كاميرات المراقبة.
3. رقم هاتف المفرزة الأمنية للتدخل السريع: [0782200192]
4. ماكينات تقطيع الوثائق.
5. أقفال رقمية وبيو مترية
6. نظام جرد الأصول (Asset management System)

MASTER COPY

7. Firewalls الجدران النارية
8. (WAF)

المسؤوليات

1. مدير إدارة / مدير المديرية:

1.1 تحديد المواقع الحساسة داخل بيئة العمل ووضع ضوابط واضحة للدخول إليها والعمل فيها، بالإضافة إلى تحديد الأفراد المصرح لهم بالدخول والعمل في تلك المواقع وفقًا لمستوى الأمان المطلوب.

1.2 مراقبة التزام الموظفين التابعين لأمرهم لتنفيذ ضوابط الدخول.

1.3 إجراء مراجعة دورية للمواقع لتقييم المخاطر الأمنية وضمان تحديث الضوابط.

2. مديرية التطوير المؤسسي وضبط الجودة /قسم إدارة المخاطر والحوكمة السيبرانية:

2.1 تطوير السياسات والإجراءات القياسية المتعلقة بالأمن السيبراني.

2.2 إجراء تقييم دوري للمخاطر التي تهدد البيانات والأصول.

2.3 تقديم برامج تدريبية لرفع وعي الموظفين.

2.4 مراجعة عمليات تصنيف الأصول وإجراء التحديثات اللازمة.

2.5 إجراء تدقيق على الامتثال لإجراءات حماية الشبكات والأنظمة.

3. مديرية التحول الالكتروني وتكنولوجيا المعلومات:

3.1 تحديد وضبط صلاحيات الدخول إلى الأنظمة والشبكات.

3.2 مراقبة وتحديث صلاحيات الدخول إلى غرفة مركز المعلومات بانتظام.

3.3 تطبيق ضوابط الأمان للشبكات مثل التشفير وجدران الحماية.

3.4 مراقبة النشاط الشبكي وتوثيق التغييرات.

3.5 حماية غرفة مركز المعلومات وغرفة المولدات الاحتياطية.

3.6 الاستجابة للحوادث السيبرانية وعمل تقارير الاستجابة والتنسيق مع الجهات ذات العلاقة.

3.7 تعريف الموردين بمعايير الأمن المطلوبة وتقييم التزامهم بها بانتظام.

3.8 مراقبة الظروف البيئية لحماية الأجهزة في المواقع الحساسة.

3.9 توفير منصات التخزين الآمنة.

3.10 تطوير إجراءات محو البيانات إلكترونيًا.

3.11 التحقق من تأمين الأصول أثناء النقل.

3.12 إعداد أنظمة المراقبة بالكاميرات.

3.13 تحديد المخاطر التي تتعلق بالشبكة والأنظمة الالكترونية لتكون أساسًا لتصميم اجراءات امنية تحمي البنية التحتية الالكترونية.

4. إدارة الخدمات:

4.1 تأمين المواقع المادية والمرافق المرتبطة بالأصول وجميع الأفراد.

4.2 تنفيذ جولات تفقدية دورية لضمان الامتثال للإجراءات الأمنية.

4.3 إدارة صلاحيات الدخول للمواقع الحساسة مثل مكتب الوزير ومكاتب الأمناء العامين والمستودعات.

4.4 توفير ماكينات تقطيع الوثائق.

4.5 مراقبة الظروف البيئية لحماية الأجهزة والمستندات.

4.6 تركيب وصيانة أنظمة الحماية المادية.

4.7 تأمين المحيط الخارجي للوزارة.

4.8 تنفيذ الجرد الميداني للأصول.

5. مديرية شؤون الموظفين:

5.1 التحقق من النزاهة الشخصية والخلفية الجنائية والتاريخ المهني قبل التوظيف.

5.2 التأكد من توقيع الموظفين الجدد على مدونة السلوك الوظيفي عند التعيين.

6. المفرزة الأمنية للتدخل السريع:

6.1 الاستجابة الفورية لأي حادث أمني مادي داخل مبنى الوزارة

6.2 التواصل مع معالي الوزير لإبلاغه بأسباب ونتائج التحقيق بالحادث الامني

7. الأفراد:

7.1 الالتزام بجميع السياسات والإجراءات الأمنية.

7.2 الإبلاغ عن أي حوادث أو مشكلات أمنية.

7.3 اتخاذ التدابير اللازمة لحماية البيانات والأصول التي في عهدتهم وتشمل:

7.3.1 استخدام الأنظمة والشبكات بشكل آمن يتوافق مع السياسات الأمنية المعتمدة.

7.3.2 التزام بسرية المعلومات وعدم إفشاء أو مشاركة أي معلومات حساسة مع غير المصرح لهم، سواء خلال فترة عملهم أو بعدها، حسب الالتزامات القانونية والسياسية للوزارة.

الإجراءات التي حسب الأمر السياسات الصادرة في هذه الوثيقة

تمتد إجراءات الأمن السيبراني في الوزارة على عدة محاور رئيسية، تهدف إلى ضمان حماية الأصول والمعلومات الحساسة والتحكم في الوصول إلى المواقع المختلفة. وفيما يلي تفاصيل هذه المحاور.

المحور الأول: الحوكمة وإدارة المخاطر والامتثال:

1. يقوم قسم إدارة المخاطر والحوكمة السيبرانية في مديرية التطوير المؤسسي وضبط الجودة بما يلي:

1.1 إعداد السياسات الخاصة بالحوكمة السيبرانية بالتعاون مع الجهات ذات العلاقة والتي يتم فيها تحديد الأدوار والمسؤوليات والمسائلة لكافة الفئات والمستويات ومن ثم واعتمادها من الأمين العام للشؤون الإدارية.

1.2 تعميم السياسات التي تم اعتمادها على كافة الإدارات والمديريات ورقيًا ونشرها الكترونيًا على موقع الوزارة.

1.3 تقديم برامج تدريبية دورية حول أمن المعلومات والتوعية بمتطلبات الإطار الوطني للأمن السيبراني وإدارة المخاطر السيبرانية.

2. إدارة المخاطر:

MASTER COPY

2.1 تحليل المخاطر المرتبطة بالبيانات والأصول كما هو موضح في خطة إدارة المخاطر والحوكمة السيبرانية.

2.2 وضع خطط لتخفيف المخاطر وتقييم فعاليتها بشكل دوري.

2.3 تحسين التدابير الأمنية بناءً على الحوادث السابقة.

3. التدقيق وضمان الامتثال:

المتابعة الدورية لتطبيق متطلبات الإطار الوطني للأمن السيبراني مع جميع المديريات وتسجيل نتائج درجة نضج الوزارة في الأمن السيبراني على المنصة المخصصة من المركز الوطني للأمن السيبراني.

4. الامتثال الدولي:

متابعة دورية لتطبيق المعايير الدولية لاستمرارية الأعمال (ISO22301) في مديرية التحول الالكتروني وتكنولوجيا المعلومات.

المحور الثاني: العلامات الوقائية وتوفير الموارد وضبط الأصول:

1. **العلامات الوقائية** : يتم تخصيص مستويات ملائمة من العلامات الوقائية للمعلومات والأصول الخاصة بوزارة الصحة لضمان أن تحظى تلك الأصول بتدابير الحماية المناسبة مثل وضع الخزنات بالأقفال للحماية الإضافية للأصول المالية والأجهزة الثمينة في الوزارة
2. **الحماية والافصاح:** يتم تصنيف الأصول لضمان الاستخدام الصحيح لهذه الأصول والبيانات المخزنة عليها كالتالي: وذلك لوضع الضوابط الأمنية والحماية الإضافية المناسبة.

العلامات	التوصيف
سري للغاية	
النطاق	المعلومات التي تُعتبر في غاية الحساسية والأهمية.
التأثير	هذا النوع من المعلومات يمكن أن يعرض أمن المؤسسة وخصوصيتها، وأمن من لهم صلة بها للخطر الشديد. وإفشاء المعلومات دونما تصريح قد يشكل خطرًا على حياة الأفراد، أو أن يحدث ضررًا ماديًا أو معنويًا للمؤسسة أو

	للجهات المرتبطة بها. كما أن إفشاء هذه المعلومات قد يعرض أمن البلاد للخطر.
أساليب الحماية	تحتاج الأصول فائقة السرية إلى درجة عالية من الضمان لحمايتها من كافة التهديدات. ولا بد من تحصين المؤسسة بكل الوسائل الممكنة ضد التهديدات العرضية أو المتعمدة، ويشمل ذلك توفير القدرة على صد الهجمات المتكررة والمتطورة. وغالبا ما يجب أن تتيح ضمانات الحماية إمكانية التعرف على المسؤولون عن إفشاء المعلومات.
سرية	
النطاق	المعلومات الحساسة المعّدة للاستخدام السري الرسمي.
التأثير	إذا تم إفشاء ذلك النوع من المعلومات فإن أمن المؤسسة وخصوصية أصولها ومن لهم صلة بها ستكون بالتأكيد عرضة للخطر. فمثلًا، قد تتضمن المعلومات السرية مناقصات لم تُطرح بعد، أو أي بيانات/معلومات يمكن أن تكون مفيدة لدول أجنبية.
أساليب الحماية	تتطلب المعلومات السرية أيضًا أقصى درجات ضمان الحماية من كافة التهديدات ولا بد من تحصين المؤسسة بكل الوسائل الممكنة ضد التهديدات العرضية أو المتعمدة، ويشمل ذلك توفير القدرة على صد الهجمات المتكررة والمتطورة، الداخلية والخارجية. وبالنسبة لجميع الأصول المصنفة بدرجة سري وما فوق، يجب تطبيق تدابير أمنية مشددة تتعلق بالأفراد.
محدودة	
النطاق	معلومات حساسة معدة للاستخدام الرسمي.
التأثير	إذا تم إفشاء ذلك النوع من المعلومات، فإن أمن الحكومة وخصوصيتها والقوات المسلحة أو الأفراد التابعين لتلك الجهات قد يتعرضون للخطر، أو قد يتسبب

	الإفشاء بإحداث أضرار محدودة. كما أن الإفشاء ربما يشكل خطرًا على أمن المؤسسة وخصوصيتها، أو على من لهم صلة بها، أو أن يلحق أضرارًا محدودة بمصالح المؤسسة. ومن شأن الإفشاء غير المصرح به أن يؤثر سلبًا على الثقة بالمؤسسة.
أساليب الحماية	يجب أن يخضع كافة الموظفين للتوعية والتدريب على ضمان الأمن، وذلك لضمان التعامل مع كافة أصول المؤسسة بالحذر الملائم. كما ينبغي أن تعكس الضوابط الأمنة أفضل الممارسات التجارية والدولية.
عادية وغير مصنفة	
النطاق	معلومات ذات حساسية دنيا.
التأثير	عادة ما تكون تلك المعلومات متاحة للنشر عن طريق وسائل التواصل وتبادل المعلومات إلكترونيًا، أو شفويًا، أو كتابيًا – كالمطبوعات والنشرات الإخبارية والمنشورات – والمواقع الإلكترونية. وإفشاء تلك المعلومات لن يؤثر على خصوصية المؤسسة أو أمنها، أو على أي ممن له صلة بها، كما أنه لن يلحق الضرر بمصالحها.
أساليب الحماية	ينبغي أن يخضع كافة الموظفين للتوعية والتدريب على ضمان الأمن للتأكد من أنهم يدركون الفارق بين الأصول غير المصنفة وتلك التي تحتاج إلى حماية.

كما يتم الإبلاغ عن أي عطل في هذه الأصول لأخذ الإجراءات اللازمة من قبل المعنيين

3. **إدارة الموارد:** يقوم مدراء الادارات والمديريات **وضع ضوابط للتعامل مع الموردين والشركاء** لإلزامهم في حماية أمن المعلومات من خلال:

3.1 توقيع اتفاقية عدم الافشاء(NDR) التي تتضمن بنود واضحة تتعلق بأمن المعلومات عند التعاقد مع الموردين والشركاء عند الاتفاق على مشروع جديد، أو عند تطوير برامج، أو إنشاء أنظمة إلكترونية، أو صيانتها وذلك قبل تبادل أي معلومات حساسة أو سرية.

3.2 إجراء تقييمات أولية ودورية للموردين والشركاء لضمان التزامهم بمعايير الأمن السيبراني.

3.3 استخدام أدوات وآليات لمراقبة الالتزام بمعايير أمن المعلومات من قبل الموردين والشركاء.

3.4 الالتزام بجميع القوانين واللوائح الوطنية والدولية المتعلقة بحماية البيانات وأمن المعلومات.

3.5 الالتزام بتطبيق سياسة شراء المنتجات السيبرانية

4. ضبط الأصول: تقوم إدارة الخدمات ومديرية التحول الالكتروني وتكنولوجيا المعلومات بما يلي كل حسب دوره:

4.1 **جرد الأصول:** ويشمل إنشاء سجل يشمل جميع الأصول مع تحديد المسؤوليات ومستويات الحماية وتحديثه بشكل دوري لضمان الامتثال.

4.2 **حماية الأصول:** ويشمل تطبيق الحماية المادية مثل الأقفال البيومترية وكاميرات المراقبة وإدارة الوصول لها بناءً على التصنيف الوظيفي واحتياجات العمل والتأكد من حجب صلاحية الدخول إلى البيانات عن الشخص الذي يتم نقله أو إنهاء خدماته.

4.3 **التعامل مع الأصول أثناء النقل:**

4.3.1 يقوم الموظف المعني بفحص الجهاز لتحديد حساسيته وقيمة البيانات المخزنة عليه.

4.3.2 تصنيف الجهاز بناءً على درجة الحماية المطلوبة (سري، حساس، عام).

4.3.3 حماية الأجهزة المادية أثناء النقل حيث يقوم موظفي الامن بما يلي:

4.3.3.1 مرافقة الأجهزة أثناء النقل واستلام نموذج السماح بإخراج الاجهزة من المبنى والاحتفاظ به في الملفات الخاصة.

4.3.3.2 التحقق من إجراءات الحماية أثناء مراحل النقل المختلفة.

4.3.3.3 اختيار وسائل نقل مناسبة (مثل مركبات مغلقة ومؤمنة).

4.3.3.4 توثيق العمليات المتعلقة بنقل الأصول الحساسة على النماذج المعتمدة.

4.4 **إزالة التصنيف أو تغييره** وذلك من خلال مراجعة مبررات تغيير تصنيف الأصول وتحديث السجلات بشكل دوري لضمان توافقها مع السياسات.

المحور الثالث: أمن الأفراد

أولًا: التدقيق الأمني: تقوم مديرية شؤون الموظفين بما يلي:

1. إجراء تدقيق أمني شامل يشمل التحقق من الخلفية الجنائية (وثيقة عدم المحكومية محدثة لا تتجاوز 6 أشهر) وكذلك التحقق من التاريخ المهني لكل موظف قبل التوظيف لضمان توافق الموظفين مع معايير الأمان المطلوبة.
2. التحقق من عدم وجود تضارب المصالح وتوقيع الموظف على النموذج الخاص بها.
3. توقيع كافة الموظفين على تعهد الالتزام بمدونة السلوك الوظيفي الذي ينص على الالتزام بأمن وسرية المعلومات وحمايتها.
4. تحديث التدقيق الأمني بشكل دوري لضمان الامتثال المستمر للمتطلبات الأمنية.

ثانيًا: إعطاء صلاحيات دخول للموظفين الجدد:

تقوم مديرية التحول الإلكتروني وتكنولوجيا المعلومات وبالتنسيق مع مدراء الادارات والمديريات المعنية بالعمل على أي نظام الالكتروني القيام بما يلي:

1. إعطاء صلاحيات دخول للموظفين الجدد بناءً على مستوى المعلومات التي يحتاجون الوصول إليها.
2. مراجعة صلاحيات الدخول بانتظام وتحديثها حسب الحاجة الوظيفية.

كما تقوم المنشأة الصحية التابعة لوزارة الصحة بمخاطبة شركة الحوسبة الصحية (حكيم) لإعطاء صلاحية دخول على نظام (حكيم) وتحديد صلاحياته على النظام حسب المهنة والمسمى الوظيفي

ثالثًا: إدارة صلاحيات الدخول: على المديريات المعنية باستخدام أي نظام الكتروني القيام بما يلي:

1. مخاطبة مديرية التحول الالكتروني لطلب إعطاء صلاحيات الدخول أو إلغائها للأشخاص المعنية باستخدام النظام بناءً على أدوارهم الوظيفية.
2. الاحتفاظ بصورة من الكتاب بملف الموظف الذي تم إعطائه الصلاحية على النظام.
3. مخاطبة مديرية التحول الالكتروني وتكنولوجيا المعلومات لإلغاء أو تعديل التصـــاريح الأمنية عند تغيير المناصب أو إنهاء الخدمة أو الانتقال إلى مكان عمل آخر أو الاستقالة أو التقاعد.
4. مراجعة دورية لصلاحيات الدخول والاطلاع بالتعاون مع مديرية التحول الالكتروني وتكنولوجيا المعلومات.

رابعًا: الإبلاغ عن الحوادث السيبرانية

1. يقوم قسم إدارة المخاطر والحوكمة السيبرانية بما يلي:

1.1 استقبال بلاغات الموظفين حول الحوادث الامنية السيبرانية وضمان امتثالهم للسياسات الأمنية.

1.2 اســـتلام تقارير الحوادث الأمنية من المديرية المعنية حســـب النموذج المعتمد المرفق في خطة ادار المخاطر السيبرانية لمراجعتها واستخلاص الدروس المستفادة منها

1.3 اعتماد نموذج موحد لتقارير الحوادث الأمنية يشمل نوع الحادث، تاريخ وقوعه، الإجراءات المتخذة، والنتائج.

1.4 حفظ التقارير المستلمة في ملف مركزي منظم، إما إلكترونيًا باستخدام برامج مثل Word أو ورقيًا.

1.5 تصنيف التقارير بناءً على نوع الحوادث أو التاريخ لتسهيل الوصول إليها وتحليلها.

1.6 إعداد تقرير شهري من قبل قسم إدارة المخاطر والحوكمة السيبرانية يلخص أهم الحوادث والإجراءات المتخذة وتقديمه للإدارة العليا.

1.7 عقد اجتماع شهري لمراجعة التقارير ومناقشة القضايا والتحسينات المطلوبة مع مديرية التحول الالكتروني وتكنولوجيا المعلومات.

1.8 تدريب موظفي القسم على التعامل مع تقارير الحوادث الأمنية وتحليلها باستخدام أدوات بسيطة مثل Excel

2. تقوم مديرية الرقابة والتدقيق الداخلي بما يلي:

2.1 تلقي تقارير الحوادث الأمنية المتعلقة بأمن الأفراد من المديرية أو المنشأة المتأثرة والقيام بالتحقيقات اللازمة.

2.2 الايعاز لمديرية الشؤون القانونية لاتخاذ الإجراءات القانونية بحق الموظفين الذين ينتهكون السياسات الأمنية.

3. تقوم مديرية الشؤون القانونية بما يلي:

3.1 اتخاذ الإجراءات القانونية بحق الموظفين الذين ينتهكون السياسات الأمنية (الموظف المتسبب بالتهديد السيبراني) استنادا إلى أحكام قانون الجرائم الإلكترونية وقانون حماية البيانات الشخصية.

3.2 تعريف الافراد بحق اعتراضهم على تسريب معلوماتهم الشخصية بمقتضى القانون (حماية البيانات الشخصية)

المحور الرابع: أمن وضبط المعلومات

يتمثل هذا المحور بضمان امن المعلومات والبيانات بكافة مراحلها، بالإضافة الى حماية الشبكات التي سيتم استخدامها لحفظ ونقل البيانات والمعلومات وكذلك حماية الأجهزة المستخدمة للعمل على هذه البيانات وتقع مسؤولية تنفيذ هذا المحور على مديرية التحول الإلكتروني وتكنولوجيا المعلومات بتطبيق ما يلي:

أولًا: تصنيف البيانات من خلال الالتزام بما يلي:

1. تصنيف البيانات إلى (متاح، غير متاح) بناءً على حساسيتها وتأثير فقدانها من خلال لجنة مشكلة من قبل الامين العام وحسب سياسة تصنيف البيانات وادارتها المعدة من قبل مديرية التحول الإلكتروني وتكنولوجيا المعلومات.
2. تطبيق الحماية المناسبة لكل تصنيف مثل الحماية البيومترية والتشفير والتخزين في خوادم ومنصات مؤمنة وكذلك تخزين نسخ احتياطية في أماكن جغرافية مختلفة.
3. تطبيق العلامات الوقائية (علامات تصنيف) لتوضيح التصنيف بواسطة:

1.3.1 استخدام ملصقات توضح التصنيف على الملفات الورقية.

1.3.2 إضافة وسوم رقمية (Digital Tags) للبيانات الإلكترونية.

ثانيًا: تصنيف الأصول المادية:

1. إعداد قائمة بالأصول التي تحتاج إلى تقييد.
2. جرد الاصول بواسطة استخدام (Asset Management Systems)
3. تصنيف الأصول حسب حساسية البيانات المخزنة فيها: (سري للغاية، حساس، خاص).
4. تحديد القيمة المالية للأصول وتأثير فقدانها.
5. استخدام العلامات الوقائية لتوضيح مستوى الحماية المطلوب لكل أصل وتشمل:

5.1 تأمين المواقع التي تحتوي على هذه الأصول الحساسة باستخدام أنظمة بيومترية وأقفال رقمية، وتحديد صلاحيات الدخول لها.

5.2 تركيب كاميرات مراقبة تعمل 24/7.

ثالثًا: تقييد الوصول الرقمي من خلال:

1. تحديد صلاحيات المستخدمين للأنظمة الالكترونية والأصول المختلفة بناءً على الوظيفة.
2. إنشاء سجلات بالوصول لكل أصل بهدف تتبع جميع الأنشطة المرتبطة بأصل معين (مادي أو رقمي)، وتشمل: (الاسم، نوع الاصل سواء كان مادي او رقمي، الموقع، المسؤول، التصنيف، سبب الدخول) ومثال ذلك الدخول إلى خادم يحتوي على بيانات طبية، فسجل الوصول سيشمل:

2.1 من دخل إلى الخادم (اسم المستخدم/التقني).

2.2 العمليات التي تم إجراؤها على الخادم (تحديث نظام التشغيل، نسخ بيانات).

2.3 الوقت والتاريخ لكل عملية.

2.4 اما بالنسبة للأصول الرقمية باستخدام أنظمة تسجيل النشاط (Log Management Systems) او أنظمة إدارة الأصول .(Access Management Systems)

2.5 توثيق الدخول والخروج من المواقع الحساسة بهدف تتبع حركة الأفراد داخل وخارج موقع معين بحيث تكون المعلومات الموثقة هي:

2.5.1 اسم الشخص الذي دخل أو خرج من الموقع.

2.5.2 وقت وتاريخ الدخول والخروج.

2.5.3 الغرض من التواجد داخل الموقع (زيارة، صيانة، تفتيش)

2.5.4 تسجيل ومتابعة أي تغييرات أو تعديلات على الأصول أو البيانات.

2.5.5 إعداد تقارير دورية تشمل جميع العمليات التي تمت على الأصول.

2.5.6 إنشاء قاعدة بيانات شاملة

2.5.7 تخزين السجلات في قاعدة بيانات مركزية

خامسًا: لضمان حماية البيانات في الوزارة منذ إنشائها إلى إتلافها يتم الالتزام بالإجراءات التالية طول دورة حياة البيانات حيث تتضمن دورة حياة البيانات أربع مراحل وتشمل:

1. مرحلة الإنشاء والجمع: يجب على جميع الموظفين اتباع الضوابط والتوصيات التالية:

يلتزم جميع الموظفين بالإجراءات التالية:

1.1 تسجيل الدخول للأجهزة باستخدام معرفات فريدة وكلمات مرور قوية تحدث دوريًا.

1.2 اخلاء سطح المكتب قبل المغادرة

1.3 تغطية لوحة الأرقام السرية عند إدخال رموز الدخول.

1.4 إغلاق شاشات الكمبيوتر عند التوقف عن استخدامه.

1.5 الامتناع عن مناقشة الأمور الحساسة خارج المواقع الحساسة أو أمام الزائرين وذلك لمنعهم من رؤية أو سماع أي شيء غير مصرح لهم بالاطلاع عليه.

1.6 تسجيل الخروج من الأجهزة المستخدمة أو بقفل أجهزة الكمبيوتر واللابتوب بنظام آلي لإقفال الشاشة عند وقف العمل أو مغادرة المكان لوقت قصير أو بانتهاء الدوام الرسمي.

1.7 تأمين الملفات الحساسة أو السرية بكلمات مرور أو عن طريق وضعها في مجلدات محمية بكلمات مرور أو تشفير كلمات المرور أثناء النقل والتخزين.

1.8 عدم تحميل أو استخدام برامج غير مرخصة (crack) تحتاج إلى تحميل لتشغيلها.

1.9 عدم حفظ كلمات المرور الخاصة بأي نظام محوسب بشكل تلقائي على أي من متصفحات الانترنت.

1.10 تنفيذ سياسات النسخ الاحتياطي المنتظم واستعادة البيانات.

1.11 حماية الملفات أو المعلومات الورقية المتوفرة في أماكن عملهم وحفظها في الأماكن المخصصة لها قبل مغادرة المكان والالتزام بإجراءات إخلاء سطح المكتب المذكورة أعلاه.

1.12 عدم دخول المواقع غير المصرح لهم بدخولها إلا بناءً على حاجة ومتطلبات العمل بناءً على سياسة (الدخول الى المواقع).

1.13 يقوم الأفراد المسؤولين عن إدارة صفحات مواقع التواصل الاجتماعي التابعة للوزارة من مديرية الاعلام والعلاقات العامة وخدمة الجمهور بتوثيق الصفحة الالكترونية المراد متابعتها من قبل وزارة الاقتصاد الرقمي والريادة ليتم متابعتها وفي حال حصل أي حادث سيبراني للصفحة يقوم مدير الصفحة بما يلي:

1.13.1 تبليغ قسم إدارة المخاطر والحوكمة السيبرانية في مديرية التطوير المؤسسي وضبط الجودة لتعبئة النموذج المعتمد للوزارة للتبليغ عن الحوادث السيبرانية.

1.13.2 تبليغ وحدة مكافحة الجرائم الالكترونية للمتابعة ان لزم الامر

2. تحديد قواعد انشاء واستخدام وتخزين كلمات السر للموظفين وتشمل ما يلي:

2.1 يمنع مشاركة الموظفين لكلمات السر فيما بينهم

2.2 يمنع الموظفين من كتابة كلمات السر خطيًا وتركها مكشوفة بالقرب من الأجهزة.

2.3 يجب ان تستوفي كلمة السر الحد الأدنى من صعوبتها بحيث يكون طولها محدد (12 خانة) وأن تشمل رموزًا خاصة وأعدادًا.

2.4 يمنع الموظفين من إعادة استخدام آخر كلمتي سر ككلمة سر جديدة.

2.5 ألا تحتوي كلمة السر على معلومات شخصية، وعدم تكرار حروف/ رموز فيها أو استخدام حروف/ أرقام متتالية.

2.6 ألا تحتوي كلمة السر فقط على كلمات شائعة مأخوذة من القاموس أو من لغات دارجة.

2.7 ألا تحتوي كلمة السر على عبارات مألوفة أو كلمات متلازمة منطقيًا.

2.8 ألا تتضمن كلمة السر مختصرات تتعلق بالوزارة مثل (MOH).

2.9 أن يكون لكلمة السر فترة صلاحية محددة وهي (42 يوم) وأن يتم تغييرها بالضرورة في حال وقوع حادث معين.

3. **مرحلة التخزين والحفظ:**

3.1 تخزين البيانات الحساسة على منصات معتمدة حكوميًا

3.2. تجزئة (Hashing) كلمات المرور المستخدمة أثناء تخزين البيانات باستخدام أدوات موثوقة لضمان عدم استرجاعها.

3.3 التأكد من عمل النسخ الاحتياطي (Back up) لكل البيانات من قبل الأشخاص المعنيين وحسب سياسة النسخ الاحتياطي

3.4 حماية مواقع التخزين المادية مثل مراكز البيانات باستخدام كاميرات وأقفال بيومترية وتحديد صلاحيات الدخول.

4. **مرحلة النقل والمشاركة:**

4.1 استخدام قنوات اتصال آمنة (HTTPS) .

4.2 منع استخدام البريد الإلكتروني غير المعتمد.

4.3 توثيق عمليات نقل البيانات بالكتب الرسمية لضمان عدم وجود خروقات.

5. **مرحلة الإتلاف:**

5.1 **لإتلاف البيانات الورقية الحساسة تقوم المديرية المعنية بإتباع الخطوات التالية:**

5.1.1 تشكيل لجنة لإتلاف البيانات الحساسة ومن ثم تسليم البيانات الورقية وملفات المرضى لشركة التدوير المتعاقد معها من قبل الوزارة لإتلافها حسب الأصول وحسب سياسة إتلاف الملفات الطبية.

5.1.2 استخدام تقنيات التقطيع الآلي للوثائق والتأكد من أن حجم القطع يتناسب مع معايير الأمن مثل DIN P-4 أو أعلى.

5.1.3 جمع الأوراق المتلفة في حاويات آمنة.

5.1.4 تسجيل تفاصيل الوثائق التي تم إتلافها وإعداد تقرير يتضمن توقيت الإتلاف، الكمية، والمسؤول عن التنفيذ.

5.2 **لإتلاف البيانات الرقمية تقوم مديرية التحول الإلكتروني وتكنولوجيا المعلومات بإتباع الخطوات التالية:**

التأكد من عمل شطب كامل (Format) للأجهزة قبل بيعها للجهات الخارجية إضافة إلى ذلك سحب الأقراص الصلبة التي تحتوي على بيانات حساسة ثم يتم اتلافها بشكل آمن بأحد الطرق التالية:

5.2.1 تطبيق الحقول المغناطيسية لمحو البيانات من الأجهزة.
5.2.2 تحطيم الأقراص الصلبة إلى أجزاء صغيرة لتجنب استعادة البيانات.
5.2.3 إزالة الأقراص الصلبة من الأجهزة والاحتفاظ بها في خزانة مغلقة.

سادسًا: الحماية التقنية تتم من خلال ضمان أمن الشبكة وادره التغيير وإدارة المخاطر الاستباقية والاستجابة للحوادث السيبرانية في حال حدوثها من خلال تطبيق الإجراءات التالية:

1. **أمن الشبكة: تقوم مديرية التحول الالكتروني وتكنولوجيا المعلومات بحماية الشبكة على عدة مستويات وهي:**

1.1 تحديد نطاق الشبكة العامة والخاصة، ونقاط التحكم وحفظ مخططات الشبكة.
1.2 مراقبة وفهم حركة دخول وخروج البيانات مع التركيز على نقاط الدخول.
1.3 تحديد التهديدات بالتعاون مع مديرية التطوير المؤسسي (قسم إدارة المخاطر والحوكمة السيبرانية) حيث يتم تحديد المخاطر الأمنية والجهات المستهدفة.
1.4 استخدام أدوات مثل جدران حماية متقدمة تحتوي على نظام كشف ومنع الدخلاء (IDS/IPS)، وبرامج الحماية من الفيروسات والبرامج الضارة، وفلترة المحتوى وفلترة بروتوكولات الويب (HTTP) والسماح فقط ل (HTTPS).
1.5 تحديث أنظمة الأمان والبرامج والأجهزة المستخدمة بشكل منتظم لسد الثغرات الأمنية.
1.6 إعداد التقارير الأمنية وتزويد مديرية التطوير المؤسسي وضبط الجودة (قسم إدارة المخاطر والحوكمة السيبرانية) بتقارير واضحة وبانتظام لتزويد المركز الوطني للأمن السيبراني بها.
1.7 مراقبة السجلات التقنية والأمن المادي للرد السريع على الحوادث.
1.8 اتخاذ الإجراءات الوقائية لربط الأجهزة بالشبكة الخاصة الافتراضية (virtual privet net-VPN).
1.9 إدارة الدخول اللاسلكي (WIFI) والتحكم بالدخول عن بُعد، حيث يتم منع استخدام تطبيقات التواصل الاجتماعي ومنصات مشاهدة الفيديوهات مثل: (U-tube)او السماح باستخدامها لفئة معينة في ساعة معينة ولفترة محدودة.
1.10 تطبيق اجراءات أمان صارمة على الشبكة تمنع الاتصال غير المصرح به
1.11 تشفير كلمات السر الخاصة للدخول للبيانات
1.12 إدارة التغييرات من خلال توثيق جميع التغييرات التي تتم على إعدادات الشبكة ومراجعة دورية لضمان تطابق الإعدادات مع معايير الأمان.

المحور الخامس: الأمن المادي

يتم تأمين الحماية المادية من قبل الادارة العليا وإدارة الخدمات ومديرية التحول الإلكتروني وتكنولوجيا المعلومات كل حسب مسؤوليته وعلى ثلاث مستويات (المحيط، المداخل، وفرق الاستجابة):

اولًا: لحماية المواقع الحساسة: تم تصنيف المواقع حسب حساسية البيانات والأصول الموجودة بها كالتالي:

1. أماكن مؤمنة بدرجة عالية بحيث يكون الدخول إليها محدود جدًا مثل (مراكز البيانات ومراكز العمليات الأمنية).
2. أماكن حساسة مخصصة فقط لموظفي الإدارة العليا ويكون الدخول اليها محدودًا مثل (مكتب معالي الوزير ومكاتب الأمناء العامين).
3. المواقع العامة المخصصة فقط للموظفين وتكون ضوابط الدخول إليها بالحد الأدنى مثل (الأقسام غير الحساسة).
4. أماكن العمل المفتوحة وتكون ضوابط الدخول إليها بالحد الأدنى مثل (قاعات الاجتماعات، المواقف الداخلية للمركبات).
5. المحيط الخارجي للمبنى وتكون عليه ضوابط دخول بسيطة.

ثانيًا: وسائل الحماية المستخدمة لحماية محيط المبنى والمداخل كما يلي:

1. إقامة أسوار وجدران محيطة بموقع الوزارة.
2. توفير بوابات مغلقة لمنع دخول غير المصرح لهم.
3. الحرص على عدم وجود نباتات تعيق رؤية الكاميرات أو توفر أماكن للاختباء.
4. دورية شرطة متجولة حول المبنى على مدار اليوم وخلال العطل الرسمية.
5. نشر رجال الأمن في كافة مرافق الوزارة.
6. منع دخول الباعة المتجولين والمتسولين إلى مبنى الوزارة.
7. استخدام كاميرات مراقبة تعمل على مدار الساعة وفي كافة مرافق المبنى.
8. تحسين مقاومة الأبواب والنوافذ والشبك والأقفال الخارجية لتأمين المبنى والغرف.
9. توفير خزائن صغيرة بأقفال لحفظ الوثائق وما شابه.
10. تخصيص خزائن مغلقة للتمديدات الكهربائية والأسلاك (الألياف).
11. تأمين خوادم البيانات في خزائن مقفلة بأماكن مخصصة لحمايتها.
12. مراقبة الظروف البيئية للبيانات الحساسة مثل مركز المعلومات ومستودعات تخزين الأجهزة لضمان سلامة الأجهزة والمعدات المخزنة وتجنب تعرضها لأي تلف بيئي.

13. توفير أنظمة إطفاء الحريق وتوفير الصيانة الدورية والتفقد اليومي لها.
14. فحص جاهزية المولدات الاحتياطية وغرفة أنظمة مزود الطاقة غير المنقطع (UPS) للعمل بشكل فوري عند انقطاع التيار الكهربائي، وذلك لضمان استمرارية العمل وحماية البيانات.

ثالثًا: تقوم إدارة الخدمات / مديرية الأبنية والصيانة بتأمين مداخل المواقع الحساسة عبر الوسائل التالية:

1. وضع حواجز وعوائق على الطرق المؤدية للموقع.
2. توفير بوابات خاصة لدخول وخروج الأفراد المهمين من الموظفين أو من غير الموظفين.
3. تكليف حرس داخلي أو مكتب استقبال لتأمين المناطق الحساسة مثل مكتب معالي الوزير ومكاتب الأمناء العامين.
4. استخدام أقفال بيومترية باستخدام بصمة الأصبع أو بصمة العين وأقفال من نوع مفتاح الرمز السري مثل غرف مراكز البيانات وغرف المراقبة ووحدة الأسرة والمصاعد، ليتيح الدخول للأشخاص المصرح لهم فقط.
5. حماية غرفة نظام مزود الطاقة غير المنقطع ((Uninterruptable Power Supply, (UPS) والتأكد من تحديث وصيانة البطاريات الاحتياطية داخل الغرفة بانتظام لضمان استمرار التشغيل في حالة انقطاع التيار الكهربائي.
6. إجراء فحص دوري لمستويات الأمان في مواقع العمل والمرافق، بما في ذلك التأكد من توفر الوقود اللازم (ديزل أو سولار) لتشغيل المولدات الكهربائية عند الحاجة.
7. منع دخول الزوار أو الموردين أو الشركاء إلى الأماكن الحساسة دون موافقات خطية ومرافقة.
8. منع إدخال أي أجهزة الكترونية محمولة أو أدوات تخزين بيانات إلى الأماكن الحساسة إلا إذا اقتضت طبيعة عمله ذلك.

المحور السادس: استمرارية العمل

1.الاستجابة للحوادث: تقوم مديرية التحول الإلكتروني وتكنولوجيا المعلومات بالاستجابة للحوادث السيبرانية:

MASTER COPY

تشكيل فريق الاستجابة لطوارئ الحاسوب للتحقيق في الحادث عن بعد أولًا ثم بالتواجد المادي ومن ثم، ضبط أصول الشبكة وفصلها وعزلها إما للحد من تأثيراتها الضارة أو لحماية الأدلة اللازمة في التحقيق ومن ثم كتابة تقرير الاستجابة وتشمل نسخة برنامج الكمبيوتر المتضرر وبيانات انتهاء صلاحيته، إن كان ذلك ينطبق ، والأصول المتضررة والتأثير المحتمل على سرية أو سلامة أو توفر البيانات أو النظام وتصحيحات أو تحديثات البرامج، أو حلول لمعالجة نقطة الضعف لتستند إليها عملية اتخاذ القرار حتى لو تطلب ذلك إدخال تغييرات كبيرة على البرامج أو الأنظمة ..

يتم تفعيل فرق الاستجابة السريعة عند وقوع حادث أمنى في محيط أو داخل مبنى الوزارة من خلال المفرزة الأمنية للتدخل السريع كالتالي:

1. الاستجابة الفورية لأي حادث أمني مادي داخل مبنى الوزارة. حيث أن أفراد المفرزة يكونوا على أهبة الاستعداد لتقديم الدعم اللازم للسيطرة على الموقف حتى وصول الدعم الإضافي إن لزم والتواصل المباشر مع معالي الوزير لغايات الإبلاغ وأخذ الإجراء المناسب حسب الحادث.
2. يتم تعميم رقم هاتف المفرزة الأمنية للتدخل السريع: [0782200192] على كافة الموظفين في الوزارة، لضمان إمكانية الوصول إليه في حالات الطوارئ.
3. **يتم الاستعانة برجال الأمن:** لردع الدخول المادي غير المصرح به والتنسيق مع المفرزة الأمنية للتحقيق واحتجاز الدخلاء عند الضرورة.

المؤشرات:

1. عدد الحوادث الأمنية قبل وبعد تطبيق السياسة
2. عدد المرات التي يتم فيها تحديث سجل الأصول مقارنة بالجدول الزمني المحدد.
3. نسبة البيانات التي تم إتلافها باستخدام الإجراءات المعتمدة.
4. نسبة الموظفين الذين أكملوا برامج التدريب على الأمن السيبراني.
5. عدد الحوادث العرضية الموثقة التي تتعلق بأمن الأفراد.

MASTER COPY

المراجع:

المراجع العربية:

1. الإطار الوطني للأمن السيبراني
2. قانون الأمن السيبراني رقم 16 لسنة 2019 المادة (4) فقرة (أ) واحكام المادة (8/ ب / 1)
3. قانون الجرائم الإلكترونية رقم 27 لسنة 2015
4. سياسة الوسائل الدفاعية المتعمقة الصادرة عن وزارة الاقتصاد الرقمي والريادة.
5. سياسة الحاويات والتخزين الصادرة عن وزارة الاقتصاد الرقمي والريادة.
6. سياسة الدخول الى المواقع الصادرة عن وزارة الاقتصاد الرقمي والريادة
7. سياسة أمن المعلوماتية من المركز الوطني للأمن السيبراني.
8. سياسة معايير أمن الأفراد من وزارة الاقتصاد الرقمي والريادة.
9. سياسة التصريح الأمني من وزارة الاقتصاد الرقمي والريادة.

المراجع الانجليزية:

10. -NIST Special Publication 800-53, National Institute of Standards and Technology
11. ISO/IEC 27001:2013 - Information Security Management.
12. NIST Cybersecurity Framework (CSF).
13. ISO/IEC 31000:2018 - Risk Management.
14. CIS Controls (Center for Internet Security).
15. Microsoft Security Documentation.
16. IBM Cybersecurity Solutions.
17. AWS Security Documentation.
18. "Cybersecurity Fundamentals" by Chuck Easttom.

المرفقات:

نموذج الإبلاغ عن الحادث السيبراني

MASTER COPY

وزارة الصحة

نموذج توثيق حادثة أمن سيبراني

- تاريخ الإبلاغ: _____
- وقت الإبلاغ: _____
- اسم المُبلغ: _____
- قسم/وحدة: _____
- موقع الحادث: _____
- نوع الحادث (مثل: فيروس، اختراق، تصيد، إلخ): _____

وصف الحادث: (بالاعتماد على مصفوفة حساب درجة الخطر)

_____

- تفاصيل الحادث (ما حدث، كيف تم اكتشاف الحادث): درجة الخطر

_____

_____

_____

- تأثير الحادث (الأنظمة المتأثرة، البيانات المتأثرة، تأثير الحادث على العمليات): درجة الخطر

_____

_____

_____

الاستجابة الأولية:

_____

_____

MASTER COPY

- الإجراءات المتخذة بعد اكتشاف الحادث:

- الأشخاص المبلغين والمستجيبين للحادث:

التحقيق والتحليل:

- نتائج التحقيق الأولي:

- الأسباب المحتملة للحادث:

MASTER COPY

الإجراءات التصحيحية والوقائية:

- الإجراءات المتخذة لاستعادة الأنظمة/البيانات:

- الإجراءات المتخذة لمنع تكرار الحادث:

<u>متابعة:</u>

- خطط المتابعة والمراقبة:

MASTER COPY