المركز الوطني للأمن السيبراني

إطار سياسة أمن المعلوماتية

18 تشرين الأول 2018

الوثيقة الأساسية لإطار سياسة أمن المعلوماتية

النسخة 1.3

عدد الصفحات شاملا صفحة الغلاف 21

تاريخ الوثيقة

النسخة	التاريخ	الملاحظات والمراجعات
0.1	18 شباط 2018	المسودة الأولى
0.2	4 حزيران 2018	تعديلات ما قبل الإصدار
0.3	12 حزيران 2018	تعديلات أولية بعد الإصدار – تطبيق نموذج الوثيقة
1.0	15 حزيران 2018	النسخة النهائية
1.1	19 حزيران 2018	التعديل السابق لقبول الوثيقة الذي تم إدخاله في التمهيد
1.2	26 تموز 2018	تحديث قائمة المصطلحات
1.3	18 تشرين الأول 2018	تحديث بعض الفقرات على ضوء ملاحظات إيه سي

جدول المحتويات

الأشكال

1 تمهيد

تلتزم حكومة الأردن بضمان الإدارة الفعالة للتدابير المتعلقة بأمن المعلوماتية الوقائي في مؤسسات الحكومة، وبناء الثقة في تعاملاتها مع قطاع الأعمال والجامعات والمواطنين والشركاء الدوليين.

السياسة الفعالة لأمن المعلوماتية تضع السياسات والمعايير، وتقدم المشورة في نفس الوقت بشأن التوجيهات حول أفضل الممارسات الأمنية، وكذلك بشأن السبل لضمان الامتثال لها بالشكل الملائم. وتحدد تلك السياسة المبادئ المتعلقة بحماية الأصول – سواء الأفراد أو الممتلكات أو المعلومات – ومنهجا لتطبيق إطار أمني متين.

والإطار المتين لأمن المعلومات يدعم تقديم الخدمات العامة الأساسية، واستقرار ونمو النشاط الاقتصادي والتجاري، كما ينشّط أعمال البحث والتطوير والجهود الأكاديمية. وفوق هذا وذاك، فإن وجود سياسة واضحة المعالم لأمن المعلوماتية يشجع اتباع منهج موحد، وفي نفس الوقت تحفيز الثقة بالحكومة.

ولكي تنجح سياسة أمن المعلوماتية هذه، ستسعى الحكومة لضمان التزام كافة موظفيها، والمتعاقدين معها، وكافة الأطراف الأخرى التي تستخدم معلومات الحكومة وأنظمتها المعلوماتية التي تدعم أعمال حكومة الأردن وتحمي أصولها.

وتتطلب الحكومة من رؤساء المؤسسات أن يكون لديهم تدابير فعالة للأمن الوقائي للمعلوماتية لضمان كل مما يلي:

- قدرة مؤسسة كل منهم على أداء مهامها؛
- سلامة الموظفين لكي يؤدوا مهام وظائفهم الحكومية، وسلامة عملاء الخدمات الحكومية؛
- حماية الموارد والمعلومات الرسمية التي تؤتمن عليها المؤسسة الحكومية، سواء كان مصدرها عامة الناس أو كانت تتعلق بهم، وكذلك المعلومات السرية التي تقدمها دول ووكالات ومنظمات أخرى.

لتحقيق تلك الغاية، يتعين على رؤساء المؤسسات تطبيق السياسات التي يحددها إطار سياسة أمن المعلوماتية وتشجيع الأمن الوقائي للمعلوماتية كجزء من الثقافة السائدة في مؤسساتهم. حيث إن تبنّي منهج أمني قائم على التدرج والمشاركة من شأنه أن يعزز الابتكار، الأمر الذي يؤدي إلى زيادة حماية وإنتاجية غايات المؤسسة.

وستواصل الحكومة إعداد وصقل سياسة أمن وقائي للمعلوماتية تشجع أكثر السبل كفاءة وفعالية لضمان استمرار سير أعمال الحكومة.

وقد أنشأت حكومة الأردن إطارا لسياسة أمن المعلوماتية كوسيلة لتأسيس مخرجات أمنية رئيسية تتحقق عن طريق نهج لإدارة المخاطر يستند إلى الدراية بالتهديدات، ويركز على نقاط الضعف، ويدفعه السعي لتحقيق الأثر المرجوّ.

1.1 الهدف

الهدف العام لإطار سياسة أمن المعلوماتية هو إرساء نهج وطني موحد إزاء أمن المعلوماتية.

2.1 التحول في أمن المعلومات

الاستراتيجية الوطنية لأمن المعلوماتية تحدد سبل دعم أمن المعلوماتية لأمن المعلومات، والذي يتم تقديمه على شكل نموذج العمل المُستهدف (Target Operating Mode - TOM). وعادة ما يكون التركيز على الأفراد والنهج والتكنولوجيا، كما هو مبين في الشكل رقم 1.

الشكل 1 - النهج التقليدي في نموذج العمل المُستهدف TOM

العناصر الثلاثة للتحول الناجح في أمن المعلوماتية هي:

3.1 الأفراد

الأفراد - ما هي المسائل الأساسية: من هي الجهة التي بيدها النهج، ومن هم المشاركون، وما هي أدوارهم، وهل هم ملتزمون بتحسين النهج ويعملون معا. ومن ناحية أهم، هل هم مستعدون لإنجاز العمل من أجل حل المشكلة.

4.1 النهج (العملية)

النهج - يدعم الأفراد عن طريق تحديد المهام والخطوات اللازمة لضمان التعامل مع أمن المعلومات بطريقة ثابتة ومُحكمة ومتناسبة، بغض النظر عن المؤسسة التي يعمل الأفراد بها.

5.1 التكنولوجيا

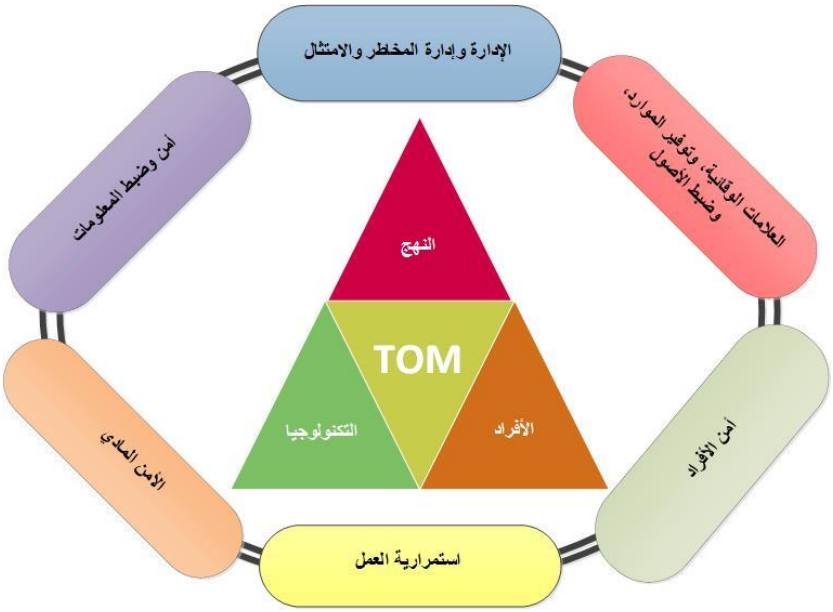
والآن، بعد اتفاق الأفراد على النهج وتطويره وتوضيحه، يمكن تطبيق التكنولوجيا لضمان استمرار تطبيق النهج، وتوفير الإرشادات التوجيهية الدقيقة لإبقاء النهج على المسار الصحيح - لجعل اتباعه أسهل من التخلي عنه.

6.1 أمثلة أخرى على نموذج العمل المستهدف

إن مثال نموذج العمل المستهدف (TOM) الذي يشمل الأفراد والنهج والتكنولوجيا هو تفريع أولي. ولتحقيق درجة أعلى من التحكم، لا بد من مقاربة أوسع نطاقا من أجل إعطاء المزيد من الاهتمام للمورّدين أو للمواقع والبنية التحتية للمباني، والذي هو أكثر صلة بالأمن المادي. وأحد الأمثلة على ذلك هو ما يُعرف بعبارة PISTOL - النهج، وأنظمة المعلومات، والمورّدون، والشركاء في العمل، والتكنولوجيا، والمؤسسة والأفراد، والمواقع والمباني - ويمكن استخدامه حين تطلب المؤسسة درجة أعلى من التقسيم.

2 مقدمة لإطار سياسة أمن المعلوماتية

إن الأمن الوقائي للمعلوماتية، بما في ذلك الأمن المادي وأمن الموظفين والمعلومات، هو من متطلب أساسي ومساند لضمان أمن المؤسسة ولجعلها تعمل بصورة أفضل. ولا بد من إدارة مخاطر أمن المعلوماتية بكفاءة وبجهد جماعي وبأسلوب متناسب من أجل خلق بيئة عمل آمنة وواثقة. ولضمان اتباع نهج متماسك لحماية نموذج العمل المستهدف (TOM) الأولي ومكوناته الفرعية من أفراد ونهج وتكنولوجيا، كما سبق تبيانه في الجزء 1، ينبغي تحديد مجالات الأمن الأساسية والسياسات التي ترتكز عليها من أجل "تسويرها"[1] أمنيا وتوفير التوجيهات الصائبة، والمتطلبات الرئيسية والإدارة والامتثال، كما هو مبين في الشكل رقم 2. وتشكل مجالات الأمن الأساسية هذه القاعدة والعمود الفقري لإطار سياسة أمن المعلوماتية.



الشكل 2 – المجالات الأساسية لإطار سياسة أمن المعلوماتية التي تدور حول نموذج العمل المستهدف (TOM)

1.2 المجالات الأساسية لإطار السياسة الأمنية

تعبير "الأمن الوقائي للمعلوماتية" في هذا السياق يصف سياسات إطار سياسة أمن المعلوماتية، والتدابير التي يتوجب على المؤسسات تطبيقها وإدارتها كوسيلة للتصدي للتهديدات السائدة للأفراد والممتلكات والمعلومات. ويتم ذلك عن طريق التعرف على المخاطر وتقييمها ومراجعتها، وتطبيق إجراءات الأمن وإدارتها على امتداد ستة مجالات أساسية وهي:

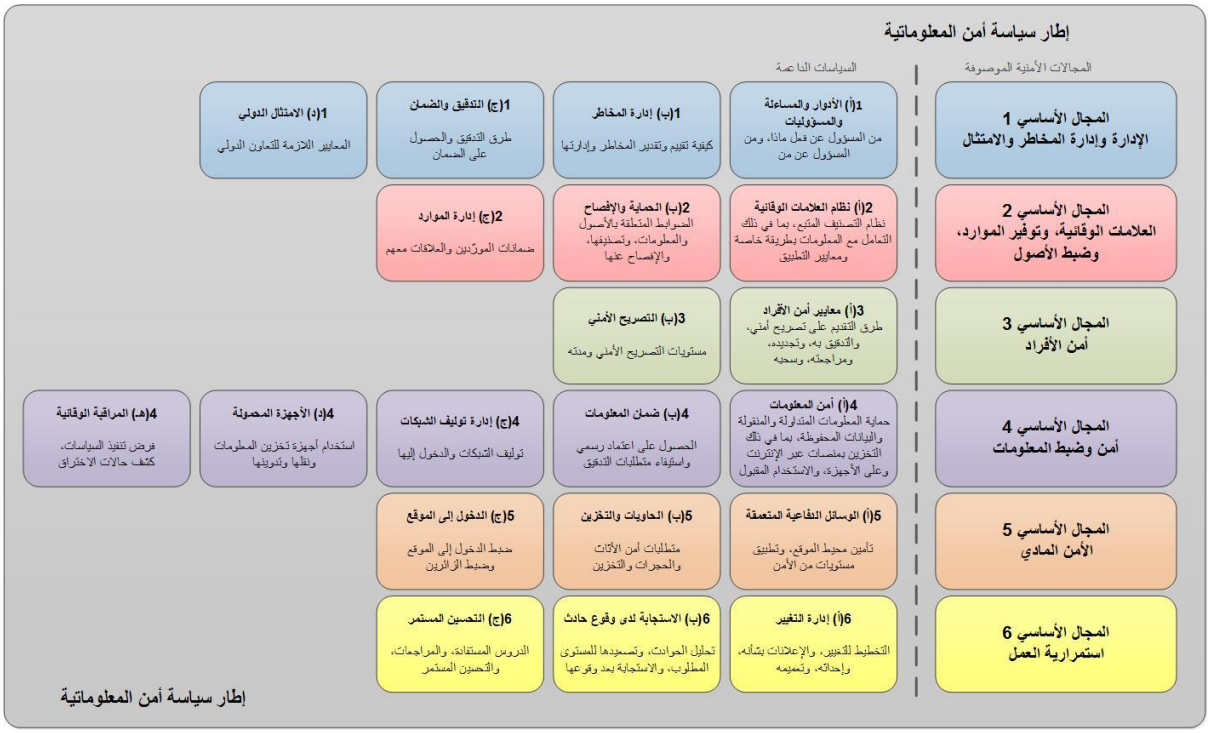
- الإدارة وإدارة المخاطر والامتثال
- العلامات الوقائية وتوفير الموارد وضبط الأصول
- أمن الأفراد
- أمن وضبط المعلومات

[1] تعبير "تسوير" يعني وضع حماية أو قيود حول المجالات التي لها أهمية أمنية.

- الأمن المادي
- استمرارية العمل

تُعتبر المسؤولية عن ضمان اتباع تدابير الأمن الوقائي للمعلوماتية من مهام كل فرد. ومع ذلك، توضح هذه الوثيقة كيفية تطبيق السياسات وإدارتها في مكان العمل.

ويبين الشكل رقم 3 مجالات سياسة أمن المعلوماتية الستة، وسلسلة السياسات التي ترتكز عليها.



الشكل 3 – إطار السياسة الأمنية

3 الإدارة

1.3 ترتيبات الإدارة

ترتيبات الإدارة - بما فيها طريقة ارتباط الأمن الوقائي للمعلوماتية بالمكونات الأخرى لإدارة العمل في مؤسسة ما - تشمل النواحي التالية، على سبيل المثال لا الحصر:

- تحديد الأدوار والمسؤوليات الأمنية
- الجوانب الأمنية، من سلامة الموظفين والسلامة العامة
- تضمين المتطلبات الأمنية في العقود
- توزيع الأدوار في إدارة الأمن
- رفع تقارير التدقيق والامتثال
- ضوابط منع الاحتيال
- الحصول على المعلومات من حكومات أجنبية وطريقة مناولة هذه المعلومات
- الإجراءات المتعلقة بالاستثناءات من السياسة
- كافة إجراءات المراجعة والتعديل

ينبغي أن تتوفر لكافة مجالات الأعمال تدابير تغطي عملية الإبلاغ عن حوادث الأمن الإلكتروني، وإدارة مثل تلك الحوادث، وإجراء التحقيقات الإلكترونية. من شأن هذه التدابير أن تحدد أدوار ومسؤوليات الموظفين المعنيين بإدارة الحوادث والتحقيقات.

2.3 المرحلة الأولى

المرحلة الأولى من تأسيس أمن وقائي للمعلوماتية هي توزيع الأدوار والمسؤوليات الأمنية، وإجراء تدقيق لكافة الأصول. انظر الفقرة 1(أ) "الأدوار والمساءلة والمسؤوليات" من أجل المزيد من التفاصيل حول تحديد الأدوار الأمنية، وانظر الفقرة 1(ب) "إدارة المخاطر" حول كيفية إجراء تدقيق على كافة الأصول كجزء من عملية تقييم المخاطر.

3.3 الوثائق

يُمكن تقديم سياسات وخطط وتدابير مؤسسة ما المتعلقة بأمن المعلوماتية في وثيقة واحدة، أو ضمن عدة وثائق منفصلة، أو أن تكون مدمجة ضمن وثائق تتعلق بالأنشطة الأخرى للمؤسسة. إلا أن من الضروري أن تبقى تلك الوثائق، مهما كانت طريقة تجميعها، محمية بالشكل المناسب ولكن متوفرة فور الحاجة إليها من أجل مراجعتها وإحالتها وتحديثها - انظر الفقرة 1(ج) "التدقيق والضمان" بشأن كيفية تحقيق ذلك.

وإذا لم تكن سياسات وخطط وتدابير المؤسسة حول الأمن الوقائي للمعلوماتية مجمعة في وثيقة واحدة، فيجب أن تتم صياغتها بناء على صلة كل منها بالأخرى، بناء على تقييم المخاطر في المؤسسة، وحسبما تؤثر كل وثيقة بالأخرى.

4.3 العلامات الوقائية

العلامات الوقائية هي سياسة استراتيجية تتبناها المؤسسة في كافة أعمالها، وهي تحدد فئات تصنيف المعلومات ذات الأهمية الخاصة بالنسبة للمؤسسة. فهذا يجعل بالإمكان تخصيص الحماية المناسبة لكل من الأصول والبيانات والوثائق بشكل متسق في مختلف أعمال المؤسسة، وإبلاغ مستخدميها فورا بكيفية التعامل معها.

لذا يجب أن تكون العلامات الوقائية:

- مبسطة وواضحة في لغتها؛
- مطبقة بشكل متسق على كافة أعمال المؤسسة دون استثناء؛
- مدعومة بسياسة توضح تفاصيل المتطلبات الأمنية وكيفية التعامل مع كل فئة؛
- تنص بشكل واضح على كيفية تصنيف المعلومات إلى فئات، والقواعد التي تضبط طريقة تخزينها وإرسالها وإتلافها.

لتكوين فهم مفصل للعلامات الوقائية المستخدمة وكيف تُطبق على الأصول المادية والمعلوماتية، انظر السياسة 2(أ) "العلامات الوقائية".

4 إطار سياسة أمن المعلوماتية - المجالات الأساسية

فيما يلي توصيف للمجالات الستة لإطار سياسة أمن المعلوماتية، والسياسات التي ترتكز عليها:

1.4 المجال الأساسي 1 – الإدارة وإدارة المخاطر والامتثال

إن متطلب تأسيس إطار لضمان التحكم بالمعلومات الخاضعة للضوابط والحفاظ عليه يعتبر أساسيا لضمان أن تكون استراتيجيات أمن المعلومات لأية مؤسسة متوائمة مع أهداف المؤسسة وداعمة لها. وهذا بدوره سيضمن أيضا الاتساق في تطبيق القوانين والقواعد من خلال الالتزام بالسياسات التي تشكل الضوابط الداخلية، وبوجود مدراء مسؤولين عن أمن المعلوماتية يتمتعون بالصلاحيات اللازمة.

مجال الإدارة تدعمه السياسات التالية:

1(أ) الأدوار والمساءلة والمسؤوليات – من المسؤول عن فعل ماذا، ومن المسؤول عن من

1(ب) إدارة المخاطر – كيفية تقييم وتقدير المخاطر وإدارتها

1(ج) التدقيق والضمان – طرق التدقيق والحصول على الضمان

1(د) الامتثال الدولي – المعايير اللازمة للتعاون الدولي

2.4 المجال الأساسي 2 – العلامات الوقائية، وتوفير الموارد، وضبط الأصول

إن ضمان توفير مقدار متناسب من الحماية للأصول والمعلومات هو أحد المتطلبات الحيوية لضمان وجود نهج متسق يتواءم مع التأثير الحاصل في حال فقدان معلومات أو أصول أو حدوث اختراق أمني أو إفشاء معلومات يشكل غير مصرح به.

مجال العلامات الوقائية وتوفير الموارد وضبط الأصول تدعمه السياسات التالية:

2(أ) نظام العلامات الوقائية – نظام التصنيف المتبع، بما في ذلك التعامل مع المعلومات بطريقة خاصة ومعايير التطبيق

2(ب) الحماية والإفصاح – الضوابط المتعلقة بالأصول والمعلومات، وتصنيفها، والإفصاح عنها

2(ج) إدارة الموارد – ضمانات المورّدين والعلاقات معهم

3.4 المجال الأساسي 3 – أمن الأفراد

متطلبات إدارة الأفراد على امتداد فترة التوظيف. وذلك يشمل المرحلة السابقة للتوظيف، وخلال فترة التوظيف وما بعد انتهاء التوظيف.

مجال أمن الأفراد تدعمه السياسات التالية:

3(أ) معايير أمن الأفراد – طرق التقديم على تصريح أمني، والتدقيق به، وتجديده، ومراجعته، وسحبه

3(ب) التصريح الأمني – مستويات التصريح الأمني ومدته

4.4 المجال الأساسي 4 – أمن وضبط المعلومات

متطلبات حماية المعلومات من العبث بها وفقدانها وإتلافها والإفصاح عنها لأطراف غير مصرح لها. ويشمل ذلك أحكام حماية المعلومات التي يُمكن الاطلاع عليها إلكترونيا، كما يشمل تفاصيل حماية الشبكات والأجهزة ومعدات تكنولوجيا المعلومات.

مجال أمن وضبط المعلومات تدعمه السياسات التالية:

4(أ) أمن المعلومات – حماية المعلومات المتداولة والمنقولة والبيانات المحفوظة، بما في ذلك التخزين بمنصات عبر الانترنت وعلى الأجهزة، والاستخدام المقبول.

4(ب) ضمان المعلومات – الحصول على اعتماد رسمي واستيفاء متطلبات التدقيق

4(ج) إدارة توليف الشبكات - توليف الشبكات والدخول إليها

4(د) الأجهزة المحمولة – استخدام أجهزة تخزين المعلومات ونقلها وتدوينها

4(هـ) المراقبة الوقائية – فرض تنفيذ السياسات – كشف حالات الاختراق

5.4 المجال الأساسي 5 – الأمن المادي

مجموعة من التدابير المادية والإجرائية المستخدمة لإعاقة الهجمات المادية على المؤسسة وردعها والإبلاغ عنها وتحليلها والاستجابة لدى وقوعها.

مجال الأمن المادي تدعمه السياسات التالية:

5(أ) الوسائل الدفاعية المتعمقة – تأمين محيط الموقع وتطبيق مستويات من الأمن

5(ب) الحاويات والتخزين – متطلبات أمن الأثاث والحُجُرات والتخزين

5(ج) الدخول إلى الموقع – ضبط الدخول إلى الموقع وضبط الزائرين

6.4 المجال الأساسي 6 – استمرارية العمل

متطلبات التعرف على خطر تعرض المؤسسة لتهديدات وأخطار داخلية وخارجية، إلى جانب متطلبات التعافي من الكوارث، وعودة المؤسسة للعمل، وإدارة الأزمات، وإدارة الحوادث، وإدارة الطوارئ، والتخطيط للحالات الطارئة.

مجال استمرارية العمل تدعمه السياسات التالية:

6(أ) إدارة التغيير – التخطيط للتغيير، والإعلانات بشأنه، وإحداثه، وتعميمه

6(ب) الاستجابة لدى وقوع حادث – تحليل الحوادث، وتصعيدها للمستوى المطلوب، والاستجابة بعد وقوعها

6(ج) التحسين المستمر – الدروس المستقاة، والمراجعات، والتحسين المستمر

5 التطبيق

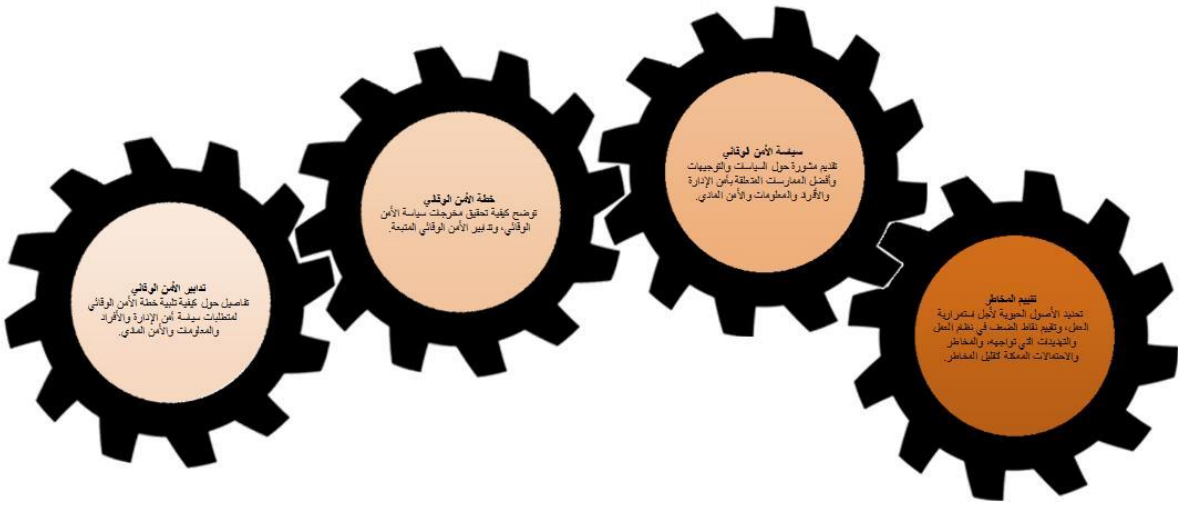
1.5 سياق ونهج السياسة

الأمن الوقائي للمعلوماتية يتيح ضمان سير العمل وتقديم الخدمات بكفاءة، كما أنه يُسهم بتحقيق الأهداف الاستراتيجية الوطنية الأعم في حماية البنية التحتية الوطنية والفضاء الإلكتروني.

والاستراتيجية الوطنية لأمن المعلوماتية لعام 2018 المعدّلة توضح كيفية تعزيز الحكومة لأمن المعلوماتية، وتحدد أولوياتها بمجال أمن المعلوماتية للحكومة وقطاع الأعمال والمواطنين.

وفي هذا السياق، فإن إطار سياسة أمن المعلوماتية يُحتّم على المؤسسات أن تطور خططا خاصة بها لإدارة الأمن الوقائي للمعلوماتية لديها من خلال سياسات وخطط وتدابير تتواءم مع السياسات المُضمّنة في إطار سياسة أمن المعلوماتية. ويُعتبر الأمن الوقائي للمعلوماتية مسؤولية المؤسسة والأفراد على حد سواء، وعلى كل شخص أن يكون مدركا للدور الذي يؤديه في تحقيق كافة متطلبات الأمن الوقائي للمعلوماتية والحفاظ عليها.

يوضح الشكل رقم 4 مثالا مُقترحا عن المكونات الأساسية لخطة إدارة الأمن الوقائي للمعلوماتية في المؤسسة. والمتطلب الأساسي هو أن تكون كافة مكونات نظام الأمن الوقائي للمعلوماتية مندمجة مع بعضها البعض، مع إمكانية استخدامها في وقت واحد.



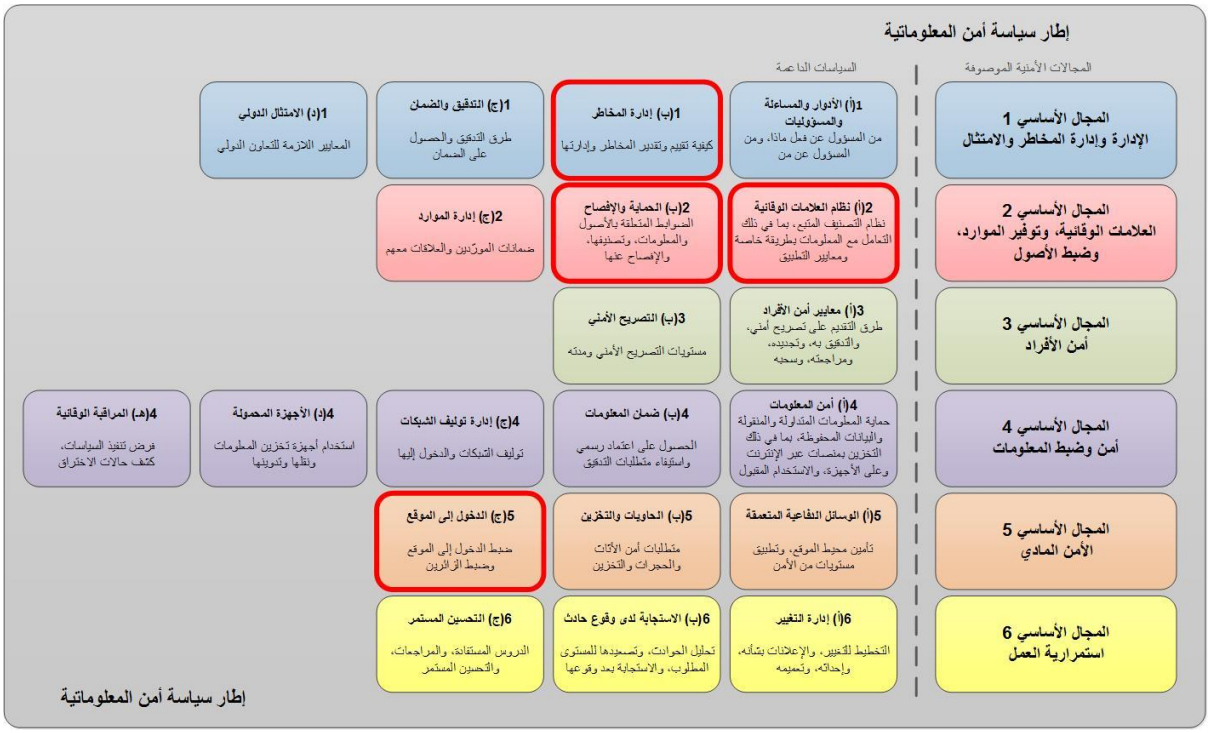
الشكل 4 - مثال لخطة إدارة الأمن الوقائي للمعلوماتية

2.5 أمثلة على استخدام هذا الإطار

فيما يلي شرح نموذج أولي عن استخدام إطار سياسة أمن المعلوماتية، وكيف أن السياسات الفردية تدعم بعضها البعض لتحقيق الغاية المرجوة من خطة إدارة الأمن الوقائي للمعلوماتية.

تعتزم المؤسسة (أ) بناء مرفق أمني جديد في أحد مواقعها القائمة. السياسات التوجيهية التي ستلجأ المؤسسة إلى الاستعانة بها تشمل ما يلي، على سبيل المثال لا الحصر، لضمان أن تبقى المؤسسة ملتزمة أمنيا:

2(ب) **الحماية والإفصاح** لضمان أن تتمكن المؤسسة من توفير الحماية الصحيحة بناء على التصنيفات في **2(أ) "نظام العلامات الوقائية"** للأصول الجاري تخزينها. وكذلك اتباع ما جاء في **5(ج) "الدخول إلى الموقع"** لضمان توفير معقل آمن وإجراء تقييم للأخطار كما جاء في **1(ب) "إدارة المخاطر"** وذلك لإبلاغ القسم عن الضوابط الإجرائية والفنية والمادية المعمول بها.



الشكل 5 - نموذج استخدام إطار السياسة الأمنية

يوضح المثال في الشكل رقم 5 يوضح استخداما مُبسطا لإطار السياسة الأمنية، ومن المنتظر مراجعة سياسات أخرى واتباعها حسبما تقتضيه الحاجة.

3.5 المبادئ التوجيهية

يقوم إطار سياسة أمن المعلوماتية هذا على المبادئ التالية:

- إطار سياسة أمن المعلوماتية لن ينسخ أو يحل محل القوانين والأحكام الوطنية المعمول بها في الأردن، تحت أي ظرف كان - بل المقصود من الإطار أن يُكمل ما هو موجود وأن يزيد من التركيز على الجوانب الأمنية؛

- إدارة أمن المعلومات على أعلى مستوى حكومي كأحد التهديدات القصوى للأمن الوطني؛

- تُنشئ الحكومة المستويات الملائمة للإدارة الوطنية والتنسيق والضبط لضمان اتباع نهج تعاوني إزاء تطوير الأمن والقدرات المتعلقة بالمعلومات، وحمايتها، والاستجابة للأزمات، والتعافي بعد وقوعها؛

- تقع على عاتق الحكومة مسؤولية القيادة لضمان أن المخاطر المتعلقة بالأمن الوقائي التي تتعرض لها أعمال الحكومة تُدار بطريقة فعالة، وبما يؤدي إلى زيادة الثقة بالحكومة من حيث تعاملها مع موظفيها والمتعاقدين معها والمواطنين والشركاء الدوليين؛

- وضع أولويات لتطبيق تدابير الأمن الوقائي على المؤسسات والأنظمة حسب درجة الخطر وتأثيره المُحتمل؛
- أمن المعلومات يعتبر مسؤولية مشتركة للمؤسسات والأفراد، سواء كانوا من الموظفين أو المتعاقدين أو من مستخدمي الخدمات؛
- بذل جهود كافية أيضا لضمان أن يدرك الأفراد ما يتوجب عليهم فعله لحماية أنفسهم على الانترنت؛
- وجود ثقافة إيجابية بشأن أمن المعلومات أمر بالغ الأهمية من أجل تحقيق أمن إلكتروني فعال، كما إن تطوير مهارات المواطنين والمؤسسات التجارية عنصر أساسي لنجاح قدرات الأمن الالكتروني؛
- تفويض مدراء على "مستوى مجلس الإدارة"[2] في كافة المؤسسات للاضطلاع بمسؤولية إدارة الأخطار الرقمية والتطبيق الصحيح لتدابير الأمن الالكتروني؛
- أمن المعلوماتية مشمول صراحة في كافة القرارات المتعلقة بالأشخاص والجوانب المادية والتكنولوجية؛
- يكون "الدفاع المُتعمق"[3] أحد المبادئ الرئيسية في تصميم الأمن الوقائي.

4.5 المعنيون بهذا الإطار

تنطبق هذه السياسات الواردة في إطار سياسة أمن المعلوماتية على كافة موظفي الحكومة والمتعاقدين معها وعلى كافة مستخدمي المعلومات الحكومية وأنظمة المعلومات التابعة لها والتي تساند أعمال الحكومة الأردنية وأصولها.

ورغم أن قائمة المستخدمين التالية ليست موسعة لتشمل الجميع، إلا أنها تشمل:

- كافة موظفي الحكومة المسؤولين عن إدارة الأمن؛
- كافة القطاعات، بما فيها الدفاع والداخلية والمالية والشؤون الخارجية والإعلام؛
- أية مؤسسة تجارية ملزمة تعاقديا بتزويد الحكومة أو مساندتها أو تمثيلها لدى وزارات الدفاع، والداخلية، والمالية، والشؤون الخارجية، والإعلام، والوزارات الأخرى؛
- أية جهة أخرى أو شخص مسؤول عن تطوير سياسات الأمن الوقائي للمعلوماتية، أو الخطط أو الإجراءات المتعلقة بها لصالح مؤسسات حكومية؛
- قيادات الأعمال في مختلف القطاعات وفي المجتمع عموما.

[2] تعبير "على مستوى مجلس الإدارة" يُقصد به عموما أعلى مستوى من السلطة داخل مؤسسة أو شركة تجارية أو داخل هيكل إداري من المسؤولين والمُساءلين عن كافة القرارات الاستراتيجية.

[3] تعبير "الدفاع المُتعمق" يشير إلى وجود عدة درجات من الضوابط الأمنية يُقصد منها توفير بديل في حال تعطل أحد تلك الضوابط.

5.5 نطاق الإطار

هذه المتطلبات تخص تدابير الأمن الوقائي:

- داخل المنشآت الحكومية؛
- داخل المنشآت الأخرى التي تتعامل مع المعلومات والأصول الحكومية؛
- المواقع التي يتواجد فيها موظفون حكوميون؛

وهذه المتطلبات توفر المشورة لأعضاء إدارة أمن المعلوماتية بشأن أفضل الممارسات.

وحيثما تكون المتطلبات التشريعية أعلى من الضوابط المحددة في هذه المتطلبات، تُعطى الأسبقية للمتطلبات التشريعية والتي لا بد من تطبيقها.

6 المتطلبات الدنيا لأمن المعلوماتية والالتزام بها

1.6 المتطلبات الدنيا لأمن المعلوماتية

يحدد إطار سياسة أمن المعلوماتية المتطلبات الدنيا على النحو التالي:

- ضمان الإدارة الفعالة لكافة المخاطر الأمنية التي يتعرض لها الأفراد والمعلومات والأصول؛
- توفير ضمان للحكومة وعامة الناس بأن الموارد والمعلومات الرسمية مُصانة بشكل جيد؛
- دمج الأمن الوقائي للمعلوماتية في الثقافة السائدة في المؤسسة.

2.6 الالتزام

لتحقيق النجاح وتوفير بيئة عمل آمنة، لا بد من وجود التزام بإطار سياسة أمن المعلوماتية ترتكز إليه كافة القرارات التي تُتخذ بشأن كل مما يلي:

- استيفاء المستلزمات - كيف تستخدم المؤسسة تدابير الأمن الوقائي للمعلوماتية لضمان استيفائها لمستلزمات ومعايير السياسة والاستجابة لتوقعات الحكومة؛
- الأداء - كيف تستخدم المؤسسة تدابير الأمن الوقائي للمعلوماتية لتُساهم في رفع أدائها عموما من خلال تقديم البضائع أو الخدمات أو البرامج بشكل آمن، مع ضمان سرية وسلامة وتوافر موظفيها ومعلوماتها وأصولها.
- المساءلة – كيف تكون المؤسسة خاضعة للمساءلة بشأن قراراتها، وتتوفر لديها آليات فعلية لضمان الالتزام بكافة المعايير المعمول بها حول الأمن الوقائي للمعلوماتية؛
- الشفافية والانفتاح – كيف تُظهر المؤسسة أنها تعمل بشفافية وأمانة وانفتاح خلال ممارستها لصلاحياتها وفي عملية اتخاذ القرارات؛
- الكفاءة – كيف تضمن المؤسسة أفضل استخدام للموارد المحدودة المتعلقة بالأمن الوقائي للمعلوماتية من أجل تحقيق أهداف المؤسسة، مع الالتزام باستراتيجيات قائمة على تحليل المخاطر من أجل تحسين الأداء؛
- القيادة – كيف يُمكن للمؤسسة أن تُظهر أن هناك التزاما في جميع أقسامها بتقديم أداء جيد من ناحية الأمن الالكتروني للمعلوماتية من خلال القيادة من أعلى الهرم.

ولتحقيق الالتزام، فإن كافة الأفراد كالمشار إليهم في الفقرة 4.5 أو أولئك المندرجين في المجالات المُشار إليها في الفقرة 5.5 يتم إبلاغهم من قبل السلسلة الإدارية التي يتبعونها بطريقة تحقيق الالتزام، وبالمسؤوليات الفردية المُحَدّثة لكل واحد منهم من أجل الوصول إلى ذلك الهدف.

7 التكامل

إن تبنّي إطار سياسة أمن المعلوماتية لا يُقصد منه أن يكون مهمة شاقة، ولكنه يتطلب التزاما من الإدارة العليا والحاجة لتغيير ممارسات وإجراءات وطرق عمل معينة قائمة قبل البدء بجني الثمار. لذا تُنصح كافة المؤسسات والشركات بالتخطيط أولا لنموذج عمل أمني متدرج حسب الأولويات، وتنفيذه بوتيرة قابلة للتطبيق ومعقولة التكلفة، على أن يحقق ذلك النموذج ما يلي:

- إنشاء هيكل تنظيمي جديد متوائم مع الاستراتيجية الأمنية ومع رؤية توفير الأمن المادي وأمن المعلومات والشبكات؛
- تحسين تجانس عملية اتخاذ القرارات من خلال استخدام قدرات وآليات جمع المعلومات الاستخباراتية عن التهديدات؛
- تحديد سياق التهديدات بشكل منتظم ودوري، وتعديل الإجراءات الأمنية بما يُلائم الحاجة وفي الوقت المناسب؛
- تهيئة بيئة يكون فيها أمن البرمجيات والأمن المادي يعملان بطريقة متناسقة ومتكاملة لتحقيق الاستفادة القصوى من الاستثمار في الأمن وتطبيق الضوابط وإدارتها؛
- تأسيس عملية تقييم للمخاطر والتهديدات الأمنية على المستوى الرسمي للمؤسسة، حيث يتم من خلال تلك العملية التعرف على المخاطر التي تهدد أمن وضع المؤسسة ومعلوماتها وأنظمتها وموظفيها، والتي يجب الحماية منها باستخدام ضوابط أمن البرمجيات والأمن المادي؛

توفير آلية فعالة لرفع التقارير عن الأداء إلى الوزراء بأسلوب موحد وقابل للقياس، حيث سيتمكن الوزراء على ضوء ذلك من معرفة درجة جاهزية المؤسسات لتقليل الأخطار الحالية والناشئة والاستجابة لدى حدوثها بأسلوب متجانس وثابت واستباقي، مع تسليط الضوء على الجوانب التي تحتاج للمعالجة.

8 معاني المصطلحات

Asset الأصول	شيء له قيمة بالنسبة للمؤسسة. الأصول يمكن أن تكون أكثر من مجرد منتجات مادية أو آلات، وتشمل البرمجيات والمعلومات والأفراد والسمعة.
Asset Owner مالك الأصول	الشخص الذي لديه مسؤولية إدارية مُعتمَدة لضبط إنتاج الأصول وتطويرها وصيانتها واستخدامها وأمنها.
Asset Register سجل الأصول	سجل تدوّن فيه كافة تفاصيل أصول المؤسسة.
Attack الهجوم	محاولة إلحاق ضرر بأحد الأصول بمختلف الوسائل، بما في ذلك الإتلاف أو الإفشاء أو التغيير أو الاطلاع عليه بشكل غير مصرح به.
Availability التوافر	أن يكون الشيء متاحا مع إمكانية استخدامه عند الطلب من طرف جهة مصرح لها (انظر ISO13335)
Classification Scheme مخطط التصنيف	طريقة تحديد تصنيفات للأصول لضمان أن تحظى بالمستوى المناسب من الحماية.
Classification التصنيف	علامة تُعطى للأصول وتحدد متطلبات حماية البيانات.
Confidentiality السرية	خاصية أن تكون المعلومات غير متاحة أو مفصح عنها لأفراد أو جهات أو عمليات غير مصرح لها (انظر ISO13335).
Control الضوابط	سياسات وتدابير وتوجيهات إرشادية لإدارة المخاطر.
Disclosure الإفصاح	إتاحة إمكانية اطلاع طرف جديد على الأصول.
Impact التأثير	هو ما ينتج عن حادثة تتعلق بأمن المعلومات يسببها تهديد يؤثر على الأصول.
Information Asset أصول المعلومات	معلومات يمكن تحديدها بأي شكل، ومدونة أو مخزنة على أي وسيلة، وتُصنّف على أنها "ذات قيمة" للمؤسسة.
Information Security Event حدث يتعلق بأمن معلومات	حدث يطرأ على خدمة أو نظام أو شبكة ويشير إلى وجود اختراق مُحتمل لأمن المعلومات. ويشمل ذلك انتهاك السياسة، أو فشل الضوابط، أو حالات غير معروفة سابقا.
Information Security Incident حادثة أمن معلومات	حدث يتعلق بأمن المعلومات يُمكنه إلحاق ضرر بعمليات المؤسسة أو تهديد أمنها.
Information System نظام المعلومات	نظام إلكتروني يختزن المعلومات أو يعالجها أو يرسلها.
Integrity سلامة الأصول	خاصية حماية دقة وتمام الأصول (انظر ISO13335).
Least Privilege أدنى امتياز	أن يكون امتياز الاطلاع على المعلومات الممنوح لأي مستخدم مقتصرا فقط على ما يلزمه الاطلاع عليه لإتمام ما هو موكل إليه من عمل أو مهام، لا أكثر.
Non-Disclosure Agreement اتفاقية عدم الإفشاء	عقد يوافق بموجبه طرف أو أكثر على عدم إفشاء معلومات سرية تبادلوها فيما بينهم كجزء ضروري من عملهم مع بعضهم البعض.
Need to know Principle مبدأ الحاجة لغرض المعرفة	تعبير "الحاجة لغرض المعرفة" يستخدم بمعنى أن يقتصر الكشف عن البيانات أو المعلومات الحساسة فقط على أولئك الذين يحتاجونها لإنجاز عملهم.

PISTOL	اختصار يشير إلى النهج، وأنظمة المعلومات، والمورّدين، والشركاء في العمل، والتكنولوجيا، والمؤسسة والأفراد، والمواقع والمباني.
Protective Marking العلامات الوقائية	انظر التصنيف.
Quality Management إدارة الجودة	كافة الأنشطة التي تمارسها المؤسسة لإدارة الجودة وضبطها وتنسيقها.
Separation of Duties - Principle مبدأ فصل المهام	لا ينبغي لشخص بمفرده أن يكون مسؤولا عن إنجاز أو ضبط مهمة، أو عدة مهام، من البداية للنهاية عندما تنطوي المهمة على إمكانية حدوث احتيال أو إساءة استخدام أو أي شكل آخر من الضرر.
Special Handling التعامل الخاص	حماية تكميلية تضاف إلى الحماية التي يفرضها تصنيف الأصول المعنية.
Strategy استراتيجية	خطة عمل مصممة لتحقيق هدف بعيد المدى أو هدف عام. مثال "سنبحث في هذا الاجتماع أهداف استراتيجيتنا حول التدقيق والضمان".
Supplier المورّد	مؤسسة مسؤولة عن توريد منتجات أو خدمات (انظر ISO 9000)
TOM	اختصار يشير إلى نموذج العمل المستهدف
Threat تهديد	السبب المحتمل لحادث قد ينشأ عنه اختراق لأمن المعلومات أو الإضرار بعمليات المؤسسة.
Supply Chain حلقة (سلسلة) التزويد	تسلسل العمليات الداخلة في إنتاج وتوزيع منتج أو خدمة.
Vulnerability نقطة ضعف	نقطة ضعف في أحد الضوابط أو الأصول.