هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

# إطار سياسات وإجراءات أمن المعلومات

## الدليل الإرشادي لسياسات وإجراءات أمن المعلومات للجهات الحكومية السعودية

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

# إطار سياسات وإجراءات أمن المعلومات

## الدليل الإرشادي لسياسات وإجراءات أمن المعلومات
## للجهات الحكومية السعودية

CERT.sa
المركز الوطني الارشادي لامن المعلومات
COMPUTER EMERGENCY RESPONSE TEAM

الطبعة الأولى – ١٤٣٢هـ

# المحتويات


الجزء الأول
مقدمة الدليل ٩

الجزء الثاني
دليل إعداد وتطوير سياسات وإجراءات أمن المعلومات ٣٣

الجزء الثالث
دليل تنفيذ السياسات والإجراءات ٥٧

الجزء الرابع
إدارة التغيير ٧٧

الجزء الخامس
الخطة التوعوية لسياسات وإجراءات أمن المعلومات ٨٩

الجزء السادس
خيارات تعيين موقع لإدارة أمن المعلومات في الهيكل التنظيمي ١٠٥

الجزء السابع
عملية مراجعة أمن المعلومات (ملخص دليل المراجعة) ١١٩

الجزء الثامن
المـــلاحـــق ١٣٣

# تمهيد

تم إعداد هذا الدليل من قبل المركز الوطني الإرشادي لأمن المعلومات (cert.gov.sa) بهيئة الاتصال وتقنية المعلومات (citc.gov.sa) في المملكة العربية السعودية تلبية لالتزاماتها النظامية بموجب القرار الصادر عن مجلس الوزراء رقم (١٩٤) وتاريخ ١٤٢٨/٦/١٠ هـ، بتكليف المركز الوطني الإرشادي لأمن المعلومات بهيئة الاتصالات وتقنية المعلومات – في المملكة العربية السعودية بإعداد وإصدار دليل إرشادات وإجراءات مفصل لسياسات أمن المعلومات، بما في ذلك الحد الأدنى من المتطلبات لمساعدة الجهات الحكومية في المملكة على إدارة مخاطر أمن المعلومات لديها.

الجزء الأول

# مقدمة الدليل

## مقدمة

علـى الرغم من تزايـد الوعي بأهمية أمن المعلومات للأعمال المختلفة، إلا أن تداخل القضايـا المتعلقة بذلك تعني أن حجم وشكل سياسات وإجـراءات أمـن المعلومات قد تختلف على نطاق واسع بين جهة حكومية وأخرى. وقد يعتمـد ذلك على العديد من العوامل التي تشمل حجم الجهـة الحكوميـة، وحساسيـة معلومات العمل التـي تمتلكها وتتعامل معها تلـك الجهة، وأعداد وأنـواع المعلومات، وأنظمـة الحاسب الآلي التي تستخدمها.

بالنسبة للجهات الحكومية الكبيرة، فقد يكون من الصعوبة بمكان تطوير وثيقة واحدة لسياسة أمن المعلومات تتناول جميع أنواع المستخدمين لـدى تلـك الجهة، وتغطي جميع مسائل أمن المعلومات الضرورية. والفكرة الأكثر فاعلية، هـي تطوير مجموعة من وثائق السياسات لتغطية كافـة أساسيـات أمن المعلومات، وتوجيهها نحو مستخدمين محددين، مما يعزز مـن كفاءة العمليات لجميع الأطـراف. وهذا الدليل يلقي الضـوء علـى العناصر الواجب أخذها في الاعتبار عند إعداد وإدارة سياسات وإجـراءات أمن المعلومات، ويقدم نموذجاً لمجموعة من وثائق سياسات وإجراءات أمن المعلومات، وعملية التطوير المصاحبة لذلك.

وتجـدر الإشـارة إلى أنـه لا توجـد طريقة واحدة فقـط لتطوير سياسات وإجـراءات أمن المعلومـات، إذ يجب الأخـذ في الاعتبار جملة من العوامـل، ومـن ضمنها نوع المستخدمين المستهدفين ونشاط وحجـم الجهة الحكومية، وقد تم أخذ جميع هذه العوامل في الاعتبار ضمن هذا الإطـار. وعامـل آخر وهو نضـوج العملية المتبعة في تطويـر السياسات والإجراءات. فالجهـة الحكومية التي لا توجد لديهـا حالياً سياسات وإجـراءات لأمـن المعلومات، أو يوجد لديها الحد الأدنى مـن ذلك فقط، قد تستخدم في البداية إستراتيجيـة مختلفة عن الجهة الحكومية التـي لديها إطار قوي مـن السياسات، ولكنها تريد تعزيزه، وأن تبدأ باستخدام السياسات والإجراءات للأغراض الأكثر تعقيداً مثل متابعة الالتزام بالتشريعات.

كمـا تقـدم هذه الوثيقة لمحة عامة عن إطار تطويـر سياسات وإجراءات أمن المعلومات الذي تم إعداده للجهات الحكومية في المملكة العربية السعوديـة. وتُعـد سياسات وإجراءات أمن المعلومـات أدوات إدارية رئيسية تساعد على إدارة مخاطر أمـن المعلومات التي تواجهها الجهة، ويجب أن تكون سياسات وإجراءات أمن المعلومات لدى أية جهة متوافقة مع مخاطر أمن المعلومات المحددة التي تواجهها تلك الجهة.

لقـد شهـدت الجهات الحكومية السعوديـة في الآونة الأخيرة تغييرات هامة من حيـث زيادة دور تقنية المعلومات في دعـم وحداتها الإدارية الرئيسيـة، وتقـديم الخدمات الإلكترونية والترابط بين الجهات الحكومية والمؤسسات الأخرى، وغيرها من الجوانب ذات العلاقة. كل ذلك أدى إلى زيادة كبيرة في أهمية أمن المعلومات للجهات الحكومية في المملكة. ويهدف هذا الدليل إلى مساعدة الجهات الحكومية في المملكة على تطوير سياسات وإجراءات أمن المعلومات لديها بصورة سريعة وفعالة، وبما يتوافق مع مخاطر أمن المعلومات التي تواجهها تلك الجهات.

والجمهور المستهدف من هذا الدليل هو الجهات الحكومية في المملكة العربية السعودية. غير أنه يمكن استخدامه من قبل جهات ومؤسسات القطاعـين العـام والخاص في المملكة وخارجها. وقد تم إعداد هذا الدليل من أجل استخدامه مـن قبل الوحدات الإدارية لأمن المعلومات أو تقنية المعلومات لدى الجهات الحكومية بهدف تطوير سياسات وإجراءات أمن المعلومات لديها.

## ١. أمر إعداد سياسات وإجراءات أمن المعلومات للجهات الحكومية السعودية

بموجب قرار مجلس الوزراء رقم ٨١ وتاريخ ١٤٣٠/٣/١٩هـ، القاضي بالموافقة على «ضوابط استخدام الحاسبات الآلية وشبكات المعلومات في الجهات الحكومية»، والذي يدعو جميع الجهات الحكومية إلى الالتزام بحد أدنى من المتطلبات الأمنية، بما يتوافق مع مخاطر أمن المعلومات التي تتعرض لها أصول المعلومات لديها.

وقد تم تقديم هذا الدليل إلى الجهات الحكومية كمجوعة شاملة من الأدلة والتوجيهات والأدوات التي يمكن أن تستخدمها إدارات هذه الجهات ضمن جهودها للالتزام بالقرار الحكومي آنف الذكر.

## ٢. مسئولية الجهات الحكومية السعودية

تعنى كل جهة حكومية سعودية بمسئولية إعداد وتطوير سياسات وإجراءات أمن المعلومات بما يتوافق مع احتياجاتها المحددة. ينبغي على الجهات الحكومية التي لا يوجد لديها حالياً سياسات وإجراءات لأمن معلومات أن تنشئ سياسات وإجراءات تناسبها باستخدام هذا الإطار. أما الجهات الحكومية التي توجد لديها سياسات وإجراءات لأمن المعلومات فينبغي عليها التأكد من أن إجراءات وسياسات أمن المعلومات الموجودة لديها تلبي الحد الأدنى من السياسات والإجراءات المشمولة في هذا الإطار.

## ٣. بيان إخلاء المسئولية

لقد تم إعداد دليل سياسات وإجراءات أمن المعلومات من قبل المركز الوطني الإرشادي لأمن المعلومات التابع لهيئة الاتصالات وتقنية المعلومات في المملكة العربية السعودية للقيام بالمهمة التي كلف بها، ولمساعدة الجهات الحكومية على إدارة مخاطر أمن المعلومات التي تحدق بأعمالها.

- تعتبر كل جهة حكومية مسئولة بنفسها عن إعداد وتطبيق سياساتها وإجراءاتها، والتأكد من الالتزام المطلوب منها.
- كما وتجدر الملاحظة أن السياسات والإجراءات الواردة في هذا الدليل تقدم الحد الأدنى من الضوابط (عناصر التحكم) للمستوى المحدد من المخاطر التي تتعرض لها أنظمة المعلومات. وتكون كل جهة حكومية مسئولة عن الالتزام بالحد الأدنى المذكور من المتطلبات الأمنية، وتحديد الضوابط الإضافية بما يتوافق مع مخاطر أمن المعلومات المحددة التي تتعرض لها أصول المعلومات لدى تلك الجهة.
- لا يتحمل المركز الوطني الإرشادي لأمن المعلومات أية مسئولية نحو عدم التزام الجهات الحكومية بهذا الإطار.
- لا يتحمل المركز الوطني الإرشادي لأمن المعلومات أية مسئولية لقاء انعدام تخفيف مخاطر أمن المعلومات لدى الجهة الحكومية.

## ٤. إقرار

لقد أخذت المنهجية المتبعة في تطوير هذا الدليل في الاعتبار المدخلات التي تم الحصول عليها من عدد من المعايير الدولية لأمن المعلومات، والأنظمة واللوائح السعودية، والأعمال المشابهة التي قامت بها الجهات الحكومية الأخرى، والمدخلات التي تم الحصول عليها من جهات حكومية سعودية. وفيما يلي قائمة بهذه المصادر:

- معايير معالجة أمن المعلومات الفدرالية الأمريكية (FIPS PUB ٢٠٠) – الحد الأدنى من المتطلبات الأمنية للمعلومات الفدرالية وأنظمة المعلومات.
- المعهد الوطني الأمريكي للمعايير والتقنية (NIST PUB ٨٠٠-٥٣) – ضوابط أمن المعلومات الموصى بها لأنظمة المعلومات الفدرالية.
- ألمانيا – دليل الحماية الأساسية لدى المكتب الفدرالي لأمن المعلومات.
- المواصفات القياسية العالمية لأمن المعلومات ISO/IEC ٢٧٠٠١.
- المدخلات من جهات حكومية مختارة.
- الأنظمة السعودية:
  - نظام التعاملات الإلكترونية
  - نظام مكافحة جرائم المعلوماتية.

## ٥. تعريف سياسات وإجراءات أمن المعلومات

### ٥.١. سياسات أمن المعلومات

سياسات أمن المعلومات هي قواعد عملية وفنية موثقة لحماية جهة ما من مخاطر أمن المعلومات التي تحدق بأعمالها وبنيتها التحتية التقنية، وتقدم وثائق السياسات المكتوبة هذه وصفاً عاماً للضوابط المختلفة التي ستستخدمها المؤسسة لإدارة مخاطر أمن المعلومات لديها. وتعتبر وثائق سياسات أمن المعلومات إعلاناً رسمياً عن نية الإدارة لحماية أصول المعلومات لديها من المخاطر ذات العلاقة.

قد تكون سياسات أمن المعلومات مدعومة بإجراءات لأمن المعلومات في بعض الحالات، وتبين هذه الإجراءات الأنشطة الرئيسية اللازمة لتطبيق تلك السياسات.

### ٥.٢. سياسات أمن المعلومات المتعلقة بأنظمة محددة

تقدم هذه السياسات ضوابط أمنية محددة لتأمين نظام معلومات من نوع معين.

### ٥.٣. إجراءات أمن المعلومات

هي الخطوات التفصيلية والتعليمات حول كيفية أداء المهام استناداً إلى المعرفة التقنية والنظرية.

## ٦. الحاجة إلى السياسة الأمنية

يجب أن تؤدي السياسة الأمنية أغراضاً كثيرة، منها:

- حماية الموظفين والمعلومات.
- تحديد أساسيات السلوك المتوقع من المستخدمين، ومدراء الأنظمة، والإدارة، وموظفي الأمن.
- تفويض موظفي الأمن بالمراقبة والرصد والتحري.
- تحديد تبعات المخالفات والتفويض باتخاذ اللازم حيالها.
- تحديد الموقف الأساسي المجمع عليه للمؤسسة فيما يختص بالأمن.
- المساعدة في خفض المخاطر إلى الحد الأدنى.
- المساعدة في متابعة الالتزام بالأنظمة والتعليمات والتشريعات.

تقدم سياسات وإجراءات أمن المعلومات إطاراً لأفضل الممارسات الممكن اتباعها من قبل جميع الموظفين. وتساعد على التأكد من خفض المخاطر إلى الحد الأدنى، ومن أن الاستجابة تتم تجاه أية حوادث أمنية بصورة فاعلة. وستساعد سياسات أمن المعلومات كذلك على إشراك الموظفين في جهود الجهة المعنية لتأمين أصولها المعلوماتية، كما ستساعد عملية تطوير هذه السياسات على تحديد أصول المعلومات لدى الجهة الحكومية.

تحدد سياسة أمن المعلومات أسلوب الجهة الحكومية في التعامل مع المعلومات، وتعلن داخلياً وخارجياً أن المعلومات هي أحد أصول تلك الجهة، وهي ملك لها، ويتعين حمايتها من الوصول، والتعديل، والإفصاح، والإتلاف بشكل غير مصرح به.

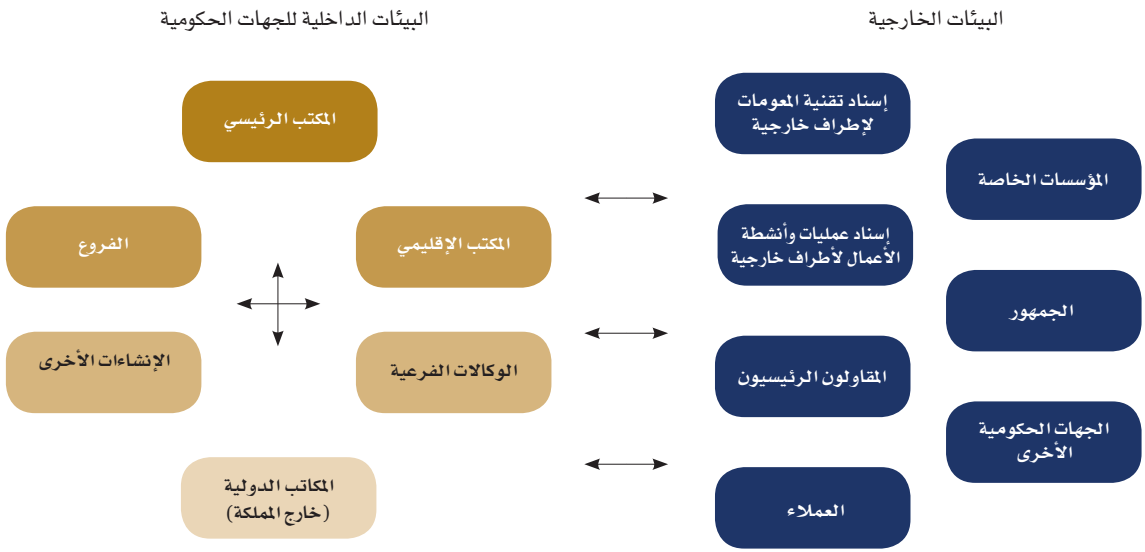
## ٧. الجوانب الأساسية التي تؤثر على احتياجات سياسات أمن المعلومات لدى الجهة الحكومية

تتكون الجهات الحكومية في المملكة العربية السعودية من عدد كبير من الإدارات والأقسام المنتشرة عبر عدد من الكيانات، تتضمن: المكتب الرئيسي، مكاتب الفروع، المكاتب الإقليمية، المرافق التصنيعية، الجهات الحكومية الفرعية، إلخ.

وفي سياق أعمالها الاعتيادية، فإن الجهات الحكومية قد تحصل على، أو تعالج، أو تبلغ، أو تخزن، أو تتلف معلومات ذات مستويات حساسية مختلفة، وذلك باستخدام أدوات يدوية أو آلية. وتتعرض الجهة الحكومية إلى مخاطر أمن المعلومات في حال تعرض سرية، وتكامل، وتوافر المعلومات التي بحوزة إداراتها وأقسامها إلى الانتهاك الأمني.

تتعامل الجهات الحكومية مع عدد من المنشآت في بيئاتها الخارجية مثل العملاء، الموردين، المقاولين، الجهات الحكومية الأخرى، مقدمي خدمات الأعمال (عندما تقوم الجهة الحكومية بإسناد جزء من أعمالها لأطراف أخرى)، مقدمي خدمات تقنية المعلومات (عندما تقوم الجهة الحكومية بإسناد جزء من أعمال تقنية المعلومات لديها لأطراف أخرى)، الجمهور، والمنشآت الأخرى.

في سياق أعمالها الاعتيادية، تتبادل الجهات الحكومية المعلومات مع المنشآت الخارجية المعنية. وقد تقوم تلك المنشآت كذلك باستلام، معالجة، تبليغ، خزن،أو إتلاف المعلومات المتعلقة بالجهات الحكومية. وتتم تأدية هذه الأنشطة باستخدام وسائل يدوية أو آلية مختلفة.




وبذلـك تتعرضـ الجهة الحكومية لمخاطر أمن المعلومات إذا ما تم انتهاك سرية، تكامل، أو توافر المعلومات المتبادلة مع الأطراف الخارجية أو التي تقوم بها أطراف خارجية (حسبما ذكر أعلاه).

وبالتـالي، فـإن مخاطر أمن المعلومات ومتطلبات سياسات أمن المعلومات يمكن أن تختلف من جهة حكومية لأخرى بناءً على طبيعة أعمالها وبيئة التقنية لديها. وفيما يلي بعض الجوانب الرئيسية التي تؤثر على متطلبات سياسات أمن المعلومات:

- الأقسام الإدارية لدى الجهة الحكومية وأعمالها وعلاقاتها الداخلية والخارجية.
- متطلبات سرية وتكامل وتوافر المعلومات التي بحوزة وقيد استخدام الجهة نفسها أو الأطراف الخارجية.
- الوسائل اليدوية والآلية المستخدمة في تجميع، معالجة، تخزين، أو إتلاف هذه المعلومات.
- جوانب أخرى تتعلق بالجهات الحكومية في المملكة مثل الأنظمة واللوائح التي يتعين عليها الالتزام بها.

## ٨. الطريقة المستخدمة في تطوير هيكل سياسات وإجراءات أمن المعلومات

تعتمد مخاطر أمن المعلومات التي تنطبق على أية مؤسسة بشكل كبير على طبيعة أعمالها وبيئتها التقنية. وبالتالي فإن تحديد مخاطر أمن المعلومات ومجالات السياسات ذات العلاقة التي تنطبق على الجهات الحكومية السعودية تتطلب فهماً للجوانب العملية والتقنية للجهات الحكومية، واستخلاص جوانب مخاطر أمن المعلومات الرئيسية ذات العلاقة، وتستند إلى تحديد مجالات سياسات أمن المعلومات الرئيسية المطبقة.

ولكي يتسنى التعامل بشكل شامل مع مخاطر أمن المعلومات والمجالات المتعلقة بسياسات أمن المعلومات، وتطوير معايير مناسبة لفئات المخاطر، فقد اعتمد هذا الدليل على المدخلات التي تم استخلاصها من عدد من المعايير الدولية لأمن المعلومات، والأنظمة واللوائح السعودية، والأعمال المشابهة التي تم القيام بها من قبل الجهات الحكومية الأخرى، والتي تشمل ما يلي:

- المواصفات القياسية العالمية لأمن المعلومات ISO/IEC 27001.
- الأنظمة السعودية.
- إطار ممارسات تقنية المعلومات CoBiT.
- المدخلات من جهات حكومية.
- معايير معالجة أمن المعلومات الفدرالية الأمريكية (FIPS PUB 200) – الحد الأدنى من المتطلبات الأمنية للمعلومات الفدرالية وأنظمة المعلومات.
- المعهد الوطني الأمريكي للمعايير والتقنية (NIST PUB 53 -800) – ضوابط أمن المعلومات الموصى بها لأنظمة المعلومات الفدرالية.
- ألمانيا – دليل الحماية الأساسية لدى المكتب الفدرالي لأمن المعلومات.

## ٩. وضع فئات لسياسات أمن المعلومات المطلوبة لإدارة مخاطر أمن المعلومات

هناك طرق مختلفة لتصور تطوير سياسات أمن المعلومات، ويتم تحديد فئات سياسات أمن المعلومات بناءً على مجموعات التحكم الخاصة بها (مثل التحكم بالوصول، الالتزام، استمرارية العمل، إلخ)، وبما يتوافق مع معايير أمن المعلومات الدولية مثل (ISO/ 27001) (في هذا الدليل يسمى هذا النوع «سياسات أمن المعلومات العامة»). وهناك كذلك سياسات أمن المعلومات المتعلقة بأنظمة معلومات معينة. ويدعم هذا الدليل تطوير سياسات أمن المعلومات سواء السياسات العامة أو تلك المتعلقة بأنظمة محددة، وتأخذ الجوانب التالية في الاعتبار لتحديد فئات تطوير سياسة أمن المعلومات للجهات الحكومية:

- مستودع للمساعدة في تطوير مجموعة نموذجية من سياسات أمن المعلومات، وتسهيل تطوير سياسات عامة وأخرى تتعلق بأنظمة معينة.
- تختلف احتياجات أمن المعلومات لدى الجهات الحكومية من حيث أهمية وحساسية المخاطر التي تواجهها وقوة السياسات المطلوبة.
- يفترض أن تغطي السياسات نطاقاً واسعاً من المستخدمين لدى الجهة المعنية، وينبغي أن تحدد السياسات الجمهور المستهدف من أجل تسهيل تبليغها وتنفيذها بشكل فاعل.

وبناءً على تحليل العوامل آنفة الذكر، فإن هذا الدليل يصنف تطوير سياسات أمن المعلومات للفئات التالية:

١. سياسات أمن المعلومات العامة:

أ. تصنف سياسات أمن المعلومات العامة بناءً على مجموعة التحكم (مثل التحكم بالوصول، استمرارية النشاط، سياسة الاستخدام المقبول، إلخ). تحدد سياسات أمن المعلومات العامة مخاطر أمن المعلومات الاعتيادية التي تنطبق على معظم

الجهات. كما أن هناك سياسات عامة محددة يتم مساندتها بإجراءات لتسهيل تنفيذها.

ب. تحدد سياسات أمن المعلومات العامة المجموعة المحددة من الجمهور المستهدف.

٢. سياسات أمن المعلومات المتعلقة بأنظمة محددة (وتستخدم لتطوير سياسات أمن المعلومات المتعلقة بأنظمة محددة مبنية على المخاطر).

أ. تُصنف معايير أمن المعلومات المتعلقة بأنظمة محددة بناءً على أنواع محددة من الأنظمة التي تحددها هذه الوثيقة (وهي التطبيقات، نظام تقنية المعلومات، الشبكات، البنية التحتية) مما يساعد الجهات الحكومية على تطوير معايير متعلقة بأنظمة محددة بناءً على درجة المخاطر التي تتعرض لها تلك الأنظمة واستناداً إلى أنواع أنظمة المعلومات المستخدمة في المؤسسة، وسريتها، وتكاملها، ومتطلبات توافرها.

ب. حيثما ينطبق فإن سياسات أمن المعلومات التي تتعلق بأنظمة معينة تدعم بحد أقصى ثلاثة مستويات من متطلبات أمن المعلومات (وهي عالي، متوسط، عادي). ويجب ملاحظة أن وضع المعايير ذات المستويين المتوسط والعالي يتضمنان ضوابط متعلقة بالمستوى الأقل من نفس النظام حيثما ينطبق ذلك، وأن وضع المعايير ذات المستوى الأعلى ستدعم وجود المعايير ذات المستوى الأدنى وذلك بإضافة عدد قليل من الضوابط (عناصر التحكم) إلى المعيار الخاص بنفس النظام.

## ١٠. الفوائد الرئيسية لطريقة التصنيف المقترحة

فيما يلي الفوائد الرئيسية لطريقة التصنيف المقترحة:

١. ستدعم معايير التصنيف عملية تطوير سياسات وإجراءات أمن المعلومات المقترحة:

أ. مجالات السياسات المحددة على أنها سياسات أمنية عامة ستساعد على وضع سياسات أمنية أساسية بسرعة وفاعلية دون جهود كبيرة.

ب. ستساعد السياسات المتعلقة بأنظمة محددة على تطوير سياسات مبنية على المخاطر لأنظمة معلومات محددة.

٢. الهيكل النموذجي للسياسات المتعلقة بأنظمة محددة يوفر المرونة وإمكانية التوسع لتحديث/ توسيع مستودع المعايير بأقل جهود ممكنة.

أ. يمكن إضافة أنواع جديدة من السياسات المتعلقة بأنظمة عامة إلى القائمة الحالية للمعايير.

ب. المعايير الخاصة بالمنتجات التقنية للموردين مثل خادم بريد مايكروسوفت (Microsoft Exchange)، وخادم يونكس (UNIX)، وغيرها، يمكن أن تضاف إلى قائمة المعايير الحالية. وهذا سيدعم المعايير الحالية العامة للأنواع المختلفة من أصول المعلومات.

ج. يمكن تعديل المعايير الحالية وتحديثها دون تأثير أو بأقل قدر من التأثير على السياسات المتعلقة بأنظمة محددة.

٣. تحديد الجمهور المستهدف في السياسات العامة سيساعد على التبليغ الفاعل للسياسات إلى المستخدمين المعنيين.

## ١١. لمحة عامة عن الدليل ومكوناته

تم تطوير هذا الدليل لاستخدامه من قبل الجهات الحكومية لتحديد احتياجاتها الأمنية، ولاستخدام منهجية مبنية على المخاطر لتطوير سياسات وإجراءات أمن المعلومات لديها باستخدام مستودعات تحوي وثائق مسبقة لمعايير وسياسات أمن المعلومات. ويقدم هذا الدليل منهجاً مرناً، تم تطويره لمساعدة الجهات الحكومية في تطوير وتنفيذ سياسات وإجراءات أمن المعلومات لديها بسرعة وفاعلية، ويتصف إطار تطوير سياسات وإجراء أمن المعلومات بالخواص التالية:

- يوفر التوافق بين سياسات وإجراءات أمن المعلومات – التي سيتم تطويرها – واحتياجات العمل.
- يقدم منهجاً مرناً في تطوير سياسات وإجراءات أمن المعلومات.
- يمكن استخدامه من قبل الجهات الحكومية ذات الجاهزية الأمنية المتدنية أو المتقدمة فيما يختص بتطوير سياسات أمن المعلومات.
- يمكن استخدامه من قبل الجهات الحكومية التي لديها موظفين ذوي مهارات أمنية متدنية أو متقدمة، أي أنه لا يحتاج إلى موارد بشرية من ذوي المهارات العالية جداً لإنجاز جزء رئيسي من مهام تطوير السياسات.
- يمكن استخدامه من قبل الجهات الحكومية مع متطلبات أمنية متدنية أو متقدمة.
- يوفر الوقت والجهد.

كما أن هذا الدليل المطور يساعد على ما يلي:

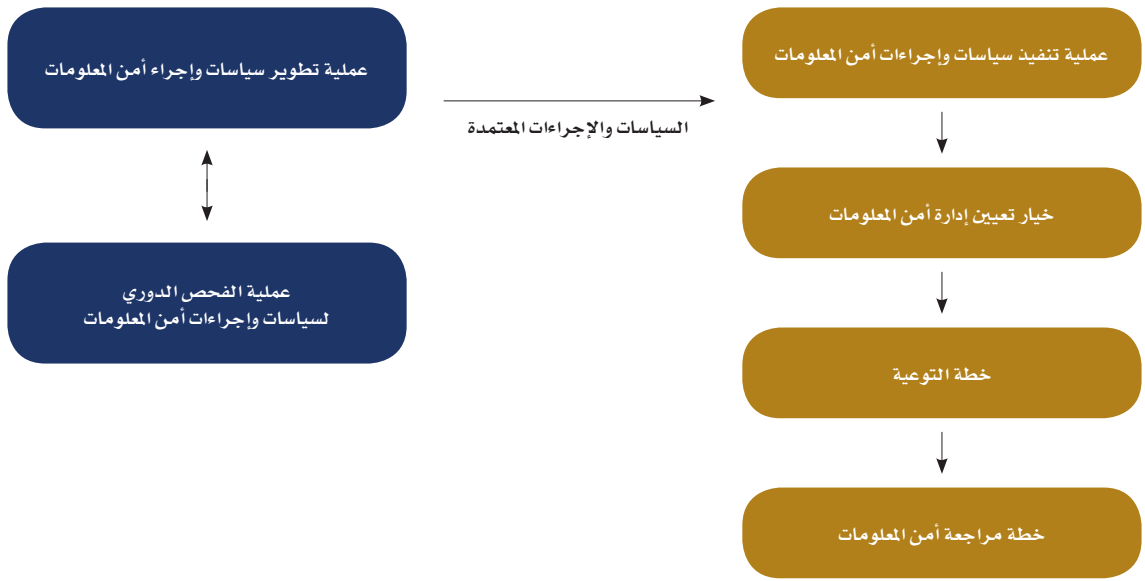
- تخطيط وتطوير سياسات وإجراءات أمن المعلومات.
- انتقاء الخيار المناسب لتعيين إدارة أمن المعلومات ضمن الهيكل التنظيمي لدى الجهة الحكومية.
- تنفيذ سياسات وإجراءات أمن المعلومات المطورة.
- خلق الوعي بسياسات وإجراءات أمن المعلومات المطورة.
- تحديد وتصنيف أنظمة المعلومات داخل الجهات الحكومية.
- مراقبة تكامل أمن أنظمة المعلومات لدى الجهات الحكومية.
- الالتزام بالتشريعات والأنظمة المحلية التي قد تتضمن قوانين تنطبق على الجهات الحكومية فيما يتعلق بأمن المعلومات.
- مراجعة وفحص الالتزام بتشريعات وأنظمة سياسات وإجراءات أمن المعلومات.

## ١٢. مكونات الدليل

يشتمل الدليل على المكونات الرئيسية التالية التي ستستخدم لطرح سياسات وإجراءات أمن المعلومات لدى الجهة الحكومية:

١. الدليل الإرشادي لسياسات وإجراءات أمن المعلومات.
   أ. وثيقة عمليه لآلية تطوير سياسات وإجراءات أمن المعلومات.
   ب. وثيقة عمليه لآلية تنفيذ سياسات وإجراءات أمن المعلومات.
   ج. وثيقة خيارات تعيين إدارة أمن المعلومات ضمن الهيكل التنظيمي.
   د. نموذج من خطة التوعية بأمن المعلومات.
٢. قاعدة بيانات للسياسات والإجراءات.
   أ. مستودع السياسات العامة.
   ب. مستودع السياسات المتعلقة بأنظمة محددة.
   ج. مستودع الإجراءات.

تصف الأقسام التالية مكونات الدليل والعلاقة بينها:

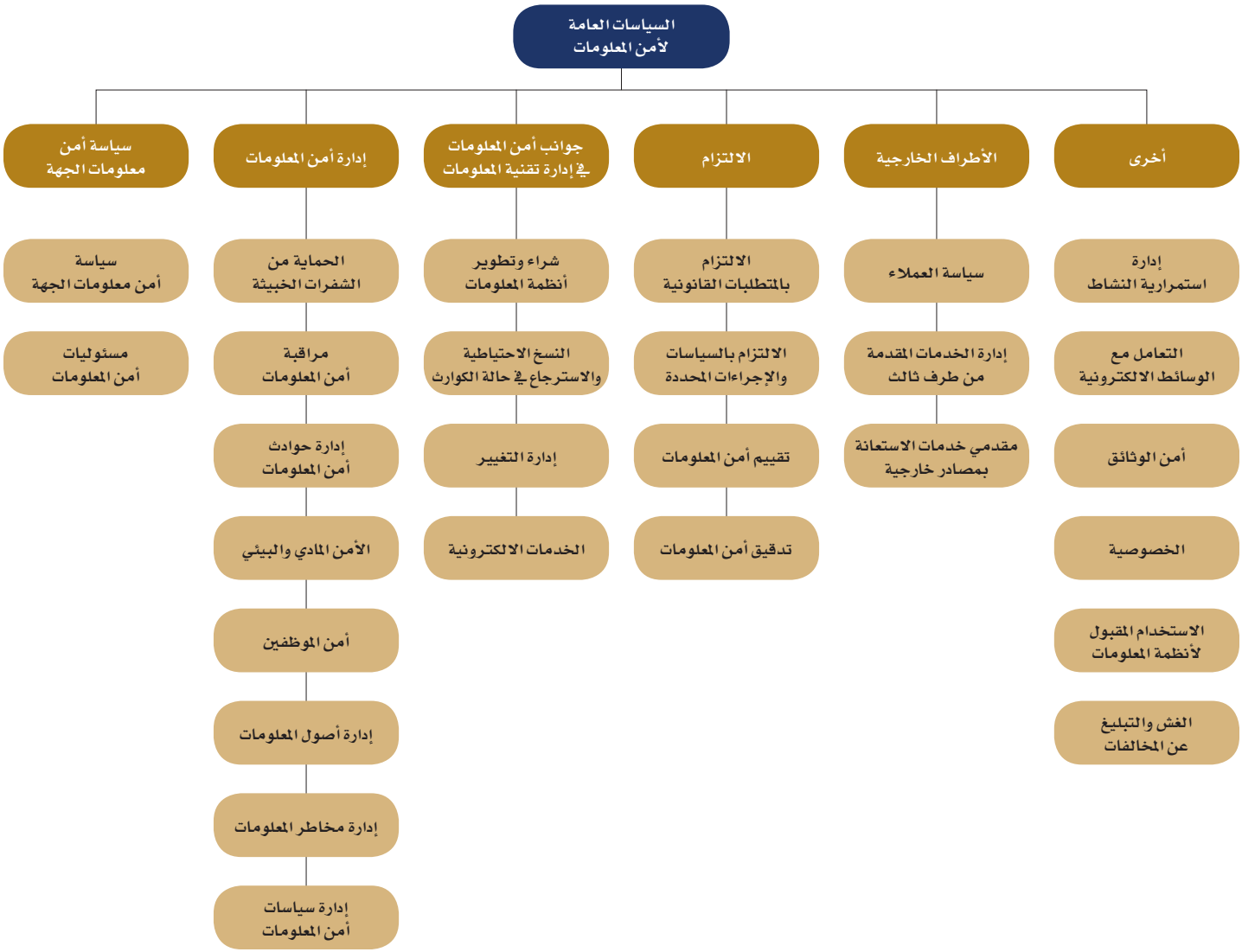



### ١٢.١. عملية تطوير سياسات وإجراءات أمن المعلومات.

توضح هذه العملية الخطوات المستخدمة لتطوير سياسات وإجراءات أمن المعلومات المبنية على المخاطر. وتستخدم هذه العملية نماذج مستودعات السياسات والإجراءات العامة لتطوير سياسات ومعايير أمن المعلومات المبنية على المخاطر للجهات الحكومية.

### ١٢. ٢. نموذج لمستودع السياسات العامة.

يظهر الشكل التالي قائمة موحدة واضحة لفئات سياسات أمن المعلومات العامة التي من شأنها التأثير على مخاطر أمن المعلومات لدى الجهات الحكومية.


السياسات العامة
لأمن المعلومات
أخرى
الأطراف الخارجية
الالتزام
جوانب أمن المعلومات
في إدارة تقنية المعلومات
إدارة أمن المعلومات
سياسة أمن
معلومات الجهة
إدارة
استمرارية النشاط
التعامل مع
الوسائط الالكترونية
أمن الوثائق
الخصوصية
الاستخدام المقبول
لأنظمة المعلومات
الغش والتبليغ
عن المخالفات
سياسة العملاء
إدارة الخدمات المقدمة
من طرف ثالث
مقدمي خدمات الاستعانة
بمصادر خارجية
الالتزام
بالمتطلبات القانونية
الالتزام بالسياسات
والإجراءات المحددة
تقييم أمن المعلومات
تدقيق أمن المعلومات
شراء وتطوير
أنظمة المعلومات
النسخ الاحتياطية
والاسترجاع في حالة الكوارث
إدارة التغيير
الخدمات الالكترونية
الحماية من
الشفرات الخبيثة
مراقبة
أمن المعلومات
إدارة حوادث
أمن المعلومات
الأمن المادي والبيئي
أمن الموظفين
إدارة أصول المعلومات
إدارة مخاطر المعلومات
إدارة سياسات
أمن المعلومات
سياسة
أمن معلومات الجهة
مسئوليات
أمن المعلومات

(الشكل ١)

يصف الجدول التالي سياسات أمن المعلومات المذكورة في الشكل السابق (الشكل ١):

| الرقم | فئات السياسات | مجالات السياسات | الوصف |
|---|---|---|---|
| ١ | سياسة أمن معلومات الجهة | سياسة أمن معلومات الجهة | تهدف هذه السياسة إلى تبليغ التزام الإدارة وعرض الأهداف الرئيسية لتأسيس ضوابط لأمن المعلومات مبنية على المخاطر التي قد تتعرض لها الجهة. |
| | | مسئوليات أمن المعلومات | تهدف هذه السياسة إلى توزيع المسئوليات المرتبطة بتحقيق مختلف أهداف أمن المعلومات لدى الجهة، ووضع الإطار العام لتأسيس علاقات العمل التعاونية بين «إدارة أمن المعلومات»، وإدارات الأعمال الأخرى و«إدارة تقنية المعلومات». |
| ٢ | إدارة أمن المعلومات | التوعية بأمن المعلومات | تهدف هذه السياسة إلى تقديم التوعية المناسبة لمستخدمي أنظمة المعلومات لدى الجهة بناءً على الاحتياجات المحددة لأمن المعلومات. تشمل هذه التوعية ما يتعلق بأمن المعلومات وبتهديدات أمن المعلومات، وسياسات وإجراءات ومعايير أمن المعلومات لدى الجهة. |
| | | سياسة إدارة الوصول المنطقي | تهدف هذه السياسة إلى التحكم بالوصول المنطقي إلى أنظمة المعلومات لدى الجهة مما يكفل دقة وسرية وتوافر المعلومات. |
| | | الحماية من الشفرات الخبيثة | تهدف هذه السياسة إلى حماية أنظمة المعلومات لدى الجهة من البرامج الخبيثة (مثل الفيروسات، ديدان الحاسب الآلي، أحصنة طروادة، قنابل البريد الإلكتروني، إلخ). |
| | | إدارة حوادث أمن المعلومات | تهدف هذه السياسة إلى التأكد من التبليغ عن جميع حوادث أمن المعلومات المتعلقة بأنظمة المعلومات لدى الجهة ومتابعتها والتحقيق فيها وحلها بالسرعة الواجبة وبصورة فاعلة. |
| | | أمن الموظفين | تهدف هذه السياسة إلى الحد من احتمال إساءة استخدام أو إتلاف أنظمة المعلومات لدى الجهة، وذلك من خلال التأكد من نزاهة الموظفين الذين يتم منحهم إمكانية الوصول إلى أنظمة المعلومات لدى المؤسسة. |
| | | إدارة أصول المعلومات | تهدف هذه السياسة إلى التأكد من أن أنظمة المعلومات لدى الجهة قد تم تحديدها وتعيين مسئولين محددين عنها، وتصنيفها بشكل مناسب بما يتوافق مع طبيعة هذه الأنظمة وتصنيف مخاطر أمن المعلومات المتعلقة بها، مما يساعد على تحديد الضوابط الأمنية المناسبة لها. |
| | | إدارة مخاطر أمن المعلومات | تهدف هذه السياسة إلى التأكد من قيام الجهة باكتشاف وتحديد مخاطر أمن المعلومات المتعلقة بأنظمة المعلومات لديها مع الأخذ في الاعتبار التهديدات ونقاط الضعف التي تعاني منها تلك الأنظمة وأثر ذلك على سير العمل. كما تقوم المؤسسة بالتخطيط لاتخاذ مبادرات مناسبة لتخفيف مخاطر أمن المعلومات التي تم تحديدها. |
| | | إدارة سياسات أمن المعلومات | تهدف هذه السياسة إلى إبقاء وتبليغ سياسات ومعايير وإجراءات أمن المعلومات لدى الجهة، وذلك وفقاً لمتطلبات سير العمل والأنظمة واللوائح المطبقة في المملكة العربية السعودية. |
| | | الأمن المادي والبيئي | تهدف هذه السياسة إلى تحديد القواعد الأساسية لمنع الدخول غير المصرح له والتدخل فيما يتعلق بمرافق وأنظمة أمن المعلومات لدى الجهة وكذلك حماية والحفاظ على أمن المعلومات والموظفين من التعرض إلى التهديدات المادية المختلفة، والتي من شأنها التأثير سلبياً على خدمات أنظمة المعلومات أو توقفها عن العمل. |

| الرقم | فئات السياسات | مجالات السياسات | الوصف |
|---|---|---|---|
| | | مراقبة أمن المعلومات | تهدف هذه السياسة إلى التأكد من أن مراقبة حالة أمن المعلومات المتعلقة بأنظمة المعلومات لدى الجهة تتم بشكل دائم من خلال تخطيط ونشر أساليب أمنية ملائمة بما يتوافق مع مخاطر ومدى حساسية وأهمية أنظمة المعلومات. |
| ٣ | جوانب أمن المعلومات في إدارة تقنية المعلومات | النسخ الاحتياطية والاسترجاع في حالة الكوارث | تهدف هذه السياسة إلى التأكد من أنه يتم عمل نسخ مساندة للمعلومات الإلكترونية واسترجاعها لدى الجهة بشكل مخطط وسريع وفعال وآمن بناء على متطلبات العمل. |
| | | الخدمات الإلكترونية | تهدف هذه السياسة إلى التأكد من أن الجهة تتعامل مع المخاطر المحيطة بأنظمة المعلومات التي تدعم الخدمات الإلكترونية بناءً على أفضل الممارسات المطبقة بهذا الصدد وطبقاً للأنظمة واللوائح المتبعة في المملكة. |
| | | شراء وتطوير أنظمة المعلومات | تهدف هذه السياسة إلى التأكد من التكامل الأمني طوال دورة حياة شراء وتطوير أنظمة المعلومات لدى الجهة. |
| | | إدارة التغيير | تهدف هذه السياسة إلى التأكد من التحكم الفاعل بجميع التغييرات التي تطرأ على أنظمة المعلومات الرئيسية كي يتسنى الحد من احتمالات انقطاع أو توقف خدمات تقنية المعلومات أو الغش والتحايل الناشئ عن التغييرات غير المصرح بها في أنظمة المعلومات. |
| ٤ | الالتزام | الالتزام بالمتطلبات القانونية | تهدف هذه السياسة إلى التأكد من التزام الجهة بالأنظمة واللوائح التي تنطبق عليها. |
| | | الالتزام بالسياسات والإجراءات المحددة | تهدف هذه السياسة إلى التأكد من مراقبة الالتزام بالسياسات والمعايير والإجراءات الأمنية الخاصة بأمن المعلومات لدى الجهة من قبل موظفيها والأطراف الثالثة العاملة معها. |
| | | تقييم أمن المعلومات | تهدف هذه السياسة إلى التأكد من قيام الجهة بإجراء تقييم أمني لأنظمة المعلومات الرئيسية لديها بناءً على متطلبات العمل، وذلك لتحديد الثغرات في تلك الأنظمة، ومن ثم اتخاذ الإجراءات المناسبة لحل تلك الثغرات. |
| | | تدقيق أمن المعلومات | تهدف هذه السياسة إلى التأكد من قيام الجهة بتخطيط وتنفيذ مراجعات وعمليات تدقيق مستقلة لأمن المعلومات المتعلقة بأنظمتها المعلوماتية بما يتوافق مع خطورة وحساسية تلك الأنظمة، ومن ثم اتخاذ الإجراءات لمعالجة الملاحظات التي تم استخلاصها من عملية المراجعة والتدقيق. |
| ٥ | الأطراف الخارجية | سياسة العملاء | تهدف هذه السياسة إلى التأكد من حفاظ الجهة على أمن معلومات عملائها والتأكد من تطبيق ضوابط أمنية كافية عند منح العملاء إمكانية الوصول إلى خدمات تقنية المعلومات لديها. |
| | | إدارة الخدمات المقدمة من طرف ثالث | تهدف هذه السياسة إلى التأكد من أن الجهة تدير مخاطر أمن المعلومات التي قد تنجم عن أنشطة الأطراف الثالثة التي تقدم خدماتها لتلك الجهة. |
| | | مقدمي خدمات الاستعانة بمصادر خارجية | تهدف هذه السياسة إلى التأكد من قيام الجهة بإدارة مخاطر أمن المعلومات الناجمة عن مقدمي الخدمات الخارجية المصدر والذين تمت الاستعانة بهم لخدمة الجهة. |

| الرقم | فئات السياسات | مجالات السياسات | الوصف |
|---|---|---|---|
| ٦ | أُخرى | إدارة استمرارية النشاط | تهدف هذه السياسة إلى تحديد الإجراءات المناسبة الواجب اتخاذها لتخفيف آثار حدوث أي توقف أو انقطاع لأنشطة العمل، وحماية عمليات/ أنشطة العمل الحساسة من الآثار الناجمة عن إخفاق/ تعطل أنظمة المعلومات أو الكوارث، والتأكد من استعادة الأنظمة بأسرع ما يمكن. |
| | | التعامل مع الوسائط الإلكترونية | تهدف هذه السياسة إلى حماية الوسائط الإلكترونية لدى الجهة مثل (أجهزة الذاكرة الموصولة على منافذ USB، الأقراص الصلبة المتنقلة، وسائط بيانات المدخلات/المخرجات مثل DVD والأقراص المدمجة وغيرها) من الاستخدام والسرقة والوصول إليها بشكل غير مصرح به. |
| | | أمن الوثائق | تهدف هذه السياسة إلى حماية المعلومات الحساسة لدى الجهة من التلف والسرقة والدخول غير المصرح به إليها. |
| | | الخصوصية | تهدف هذه السياسة إلى الحفاظ على سرية وتكامل وتوافر المعلومات الشخصية التي بحوزة الجهة ضمن أنظمتها المعلوماتية. |
| | | الاستخدام المقبول لأنظمة المعلومات | تهدف هذه السياسة إلى وضع قواعد الاستخدام المقبول لأنظمة المعلومات لدى الجهة. |
| | | الغش والتبليغ عن المخالفات | تهدف هذه السياسة إلى التأكد من أن الغش والأنشطة المحظورة في أنظمة المعلومات لدى الجهة يتم منعها والتبليغ عنها والتحقيق فيها واتخاذ الإجراءات المناسبة نحوها في حال وقوعها. |

بالنسبة للنماذج المختارة أعلاه من سياسات أمن المعلومات، فإن مستودع سياسات أمن المعلومات العامة يتصف بما يلي:

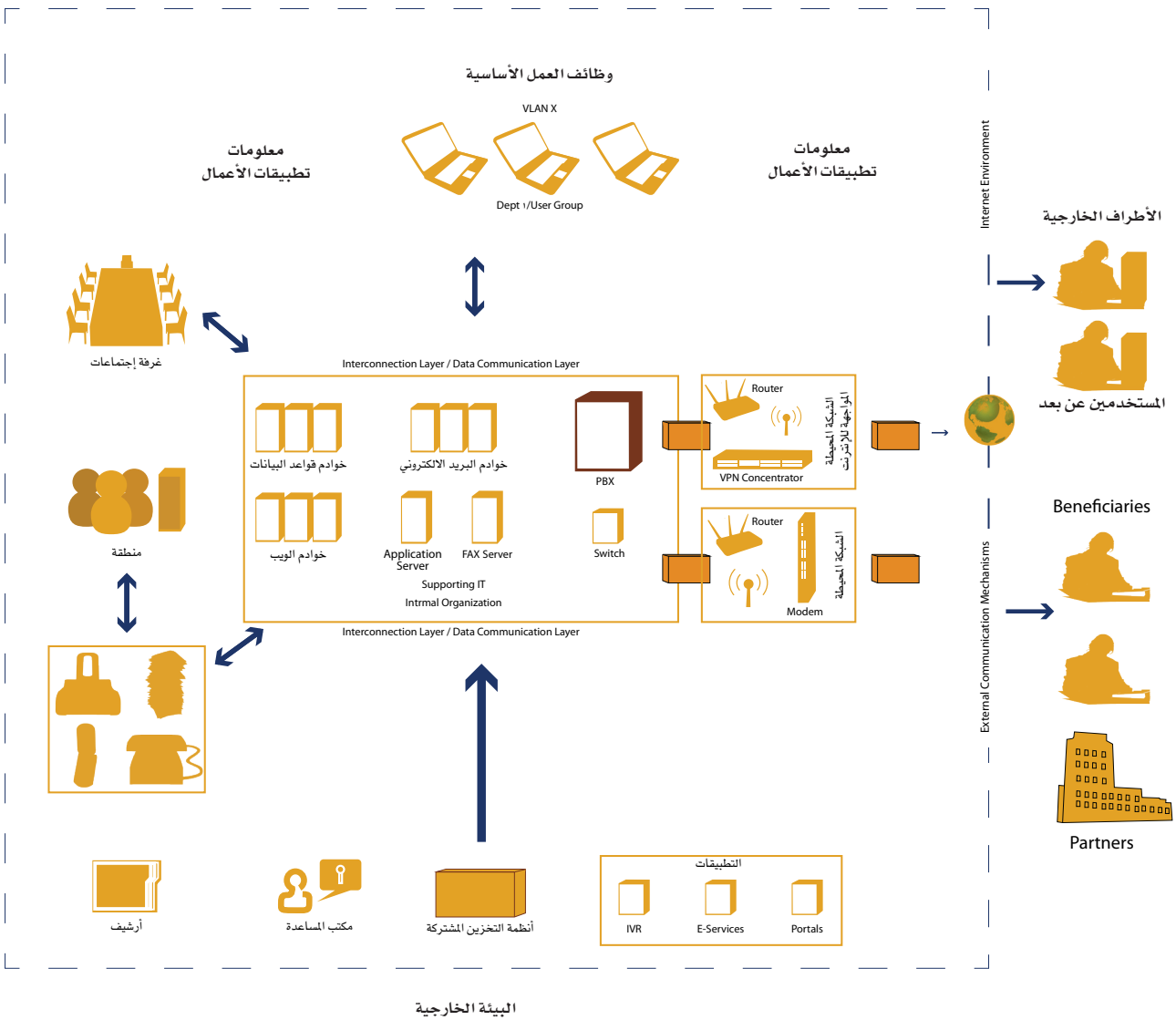
- يتضمن بنود السياسات المطلوبة للتعامل مع المخاطر المتعلقة بمجالات سياسات أمن المعلومات المحددة.
- يتضمن الإجراءات (حيثما ينطبق) المطلوبة لتطوير بنود السياسات.

تحتوي سياسات أمن المعلومات العامة على عدد من الإجراءات المساندة. وتستخدم هذه السياسات والإجراءات جنباً إلى جنب مع السياسات المتعلقة بأنظمة معلومات محددة، وأفضل الممارسات الأخرى المتعلقة بأمن المعلومات وذلك لتطوير برامج مراجعة وتدقيق أمن المعلومات لدى الجهات الحكومية، وتطوير رسائل التوعية الملائمة والمتعلقة بأمن المعلومات كجزء من خطة التوعية.

للمزيد من التفاصيل حول سياسات أمن المعلومات العامة، فضلاً راجع مستودع سياسات أمن المعلومات العامة.

## ١٢. ٣. نموذج لمستودع السياسات المتعلقة بأنظمة معلومات محددة

يوضح الشكل التالي العوامل البيئية لدى الجهات الحكومية التي من شأنها التأثير على الاحتياجات الأمنية لمعلوماتها:




(الشكل ٢)

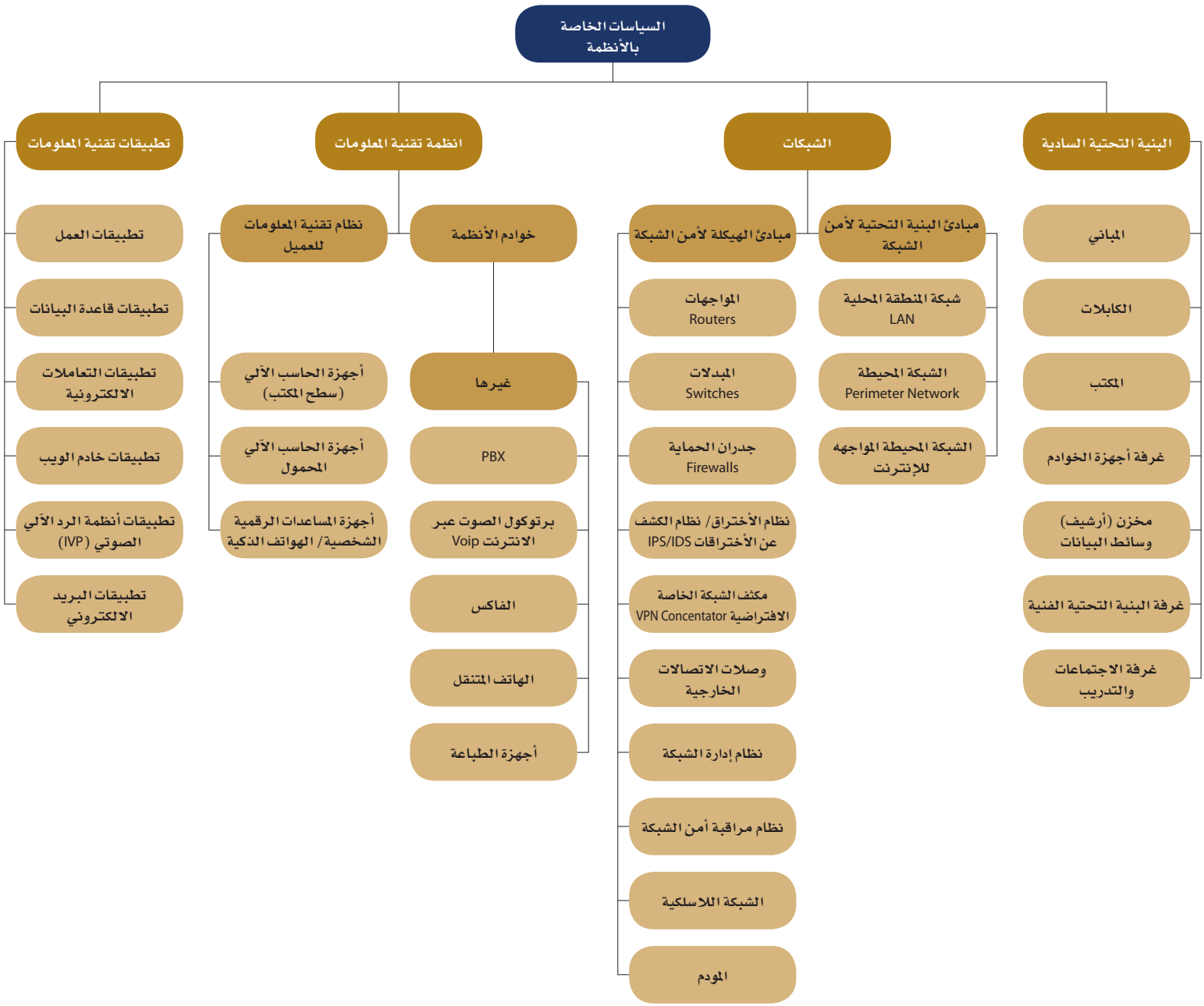
حسبما ورد في التوضيح الوارد أعلاه (الشكل ٢)، فإنه:

- يتم مساندة الجهة الحكومية بمجموعة من الوظائف الأساسية والمساندة. وتقوم هذه الوظائف بتجميع، معالجة، تخزين، تبليغ، أو إتلاف المعلومات كجزء من سير أعمال النشاط. وقد تختلف متطلبات سرية، وتكامل، وتوافر المعلومات التي تؤديها وظائف العمل اعتماداً على احتياجات العمل.
- يتم التعامل مع المعلومات من قبل وظائف العمل:
  - باستخدام وسائل آلية، مثل تطبيقات تقنية المعلومات التي تعالج المعلومات المتعلقة بتلك الوظائف.
  - أو باستخدام طرق يدوية مثل الوثائق والاجتماعات وغيرها من هذه الطرق.
  - أو باستخدام كلتا الطريقتين التي سبق ذكرهما.
- يتم الحصول على المعلومات ومعالجتها باستخدام أنواع مختلفة من تطبيقات تقنية المعلومات، مثل برامج خوادم التطبيقات، وبرامج خوادم الويب، ويتم مساندة هذه التطبيقات بواسطة البنية التحتية لأنظمة تقنية المعلومات.
- يتم الوصول إلى المعلومات عبر خوادم تطبيقات تقنية المعلومات من قبل المستخدمين باستعمال تطبيقات العميل. وتتواجد تطبيقات العميل عادة في أجهزة الحاسب الآلي الخاصة بالعميل، وتشمل أجهزة سطح المكتب، الأجهزة المحمولة، أجهزة المساعد الشخصي PDA، إلخ.
- يتم حفظ المعلومات في خوادم قاعدة البيانات، أجهزة الحاسب الآلي الخاصة بالعميل، آليات التخزين المركزية للبيانات (النسخ المساندة)، أجهزة التخزين المتنقلة، إلخ.
- يتم الوصول إلى المعلومات من خدمات تطبيقات تقنية المعلومات لدى الجهة الحكومية من خلال الشبكة المحلية للجهة (LAN) أو الشبكة الواسعة (WAN) لدى تلك الجهة.
- كما يمكن الوصول إلى خدمات تطبيقات تقنية المعلومات (والمعلومات المساندة) عن بعد باستخدام آليات اتصال عن بعد مختلفة، مثل الوصول اللاسلكي، الوصول عبر الهاتف، الوصول عبر الإنترنت، إلخ.
- يمكن الحصول على المعلومات، أو معالجتها أو تخزينها أو تبليغها باستخدام آليات/ وسائل أخرى مثل الوثائق، الاجتماعات، نظام الهاتف، الفاكس، إلخ.
- يمكن أن يكون للجهة الحكومية إدارة تقنية معلومات واحدة أو أكثر لإدارة البنية التحتية لتقنية المعلومات الداعمة لأقسام الجهة الإدارية.
- توضع تطبيقات تقنية المعلومات الأساسية في العادة في موقع مركزي (غرفة خوادم، مركز بيانات).
- يمكن أن يكون للجهة الحكومية إدارة أمن معلومات واحدة أو أكثر (ضمن أو خارج إدارة تقنية المعلومات) لإدارة الجوانب المتعلقة بأمن المعلومات.
- من شأن البنية التحتية أن تسهل عملية التفاعل والتعامل بين الأطراف المختلفة ذات العلاقة مثل العملاء، الموردين، الشركاء، المقاولين، الجهات الحكومية الأخرى، إلخ. ويكون لتلك المنشآت/ الجهات مستويات وصول مختلفة إلى معلومات الجهات الحكومية بناءً على دورها الذي تم تحديده.
- يتم التعامل عادة مع الجوانب الأمنية المتعلقة بالبيئة المادية لدى الجهات الحكومية من قبل إدارة منفصلة، مثل إدارة الأمن المادي، أو إدارة المباني.
- يتعين على الجهات الحكومية الالتزام بعدد من الأنظمة واللوائح، والتي يتضمن بعضها أمور متعلقة بأمن المعلومات.

قد تواجه الجهات الحكومية مخاطر أمن معلومات من أي من المصادر المذكورة أعلاه إذا ما استغلت الثغرات الأمنية التي تحويها هذه المصادر من قبل التهديدات المحدقة بأمن المعلومات. وقد تختلف مخاطر أمن المعلومات وسياسات أمن المعلومات المطلوبة لدى الجهات الحكومية بناءً على نوعية البنية التحتية لأمن المعلومات لديها.

وبناءً على تحليلات المعلومات المتقدم ذكرها، فإن التوضيح التالي يظهر أنواع أنظمة المعلومات المستخدمة في الحصول على، معالجة، تبليغ، وتخزين المعلومات لدى الجهات الحكومية[1].

(١) لقد تم تحديد أنظمة المعلومات هذه لتمكين عدد كبير من الجهات الحكومية السعودية من إعداد أنظمة معلوماتهم وفقاً لها. غير أن القائمة لا يمكن أن تكون شاملة لكل شيء. بناءً على متطلبات محددة، قد تحتاج الجهات الحكومية السعودية إلى أنواع مختلفة من أنظمة المعلومات. وتعطي المنهجية المقترحة المرونة لإضافة أنواع أخرى من أنظمة المعلومات مستقبلاً وفقاً للمخاطر المحددة التي تتعرض لها.


السياسات الخاصة بالأنظمة
البنية التحتية السادية
المباني
الكابلات
المكتب
غرفة أجهزة الخوادم
مخزن (أرشيف) وسائط البيانات
غرفة البنية التحتية الفنية
غرفة الاجتماعات والتدريب
الشبكات
مبادئ البنية التحتية لأمن الشبكة
شبكة المنطقة المحلية LAN
الشبكة المحيطة Perimeter Network
الشبكة المحيطة المواجهه للإنترنت
مبادئ الهيكلة لأمن الشبكة
المواجهات Routers
المبدلات Switches
جدران الحماية Firewalls
نظام الأختراق/ نظام الكشف عن الأختراقات IPS/IDS
مكثف الشبكة الخاصة الافتراضية VPN Concentator
وصلات الاتصالات الخارجية
نظام إدارة الشبكة
نظام مراقبة أمن الشبكة
الشبكة اللاسلكية
المودم
انظمة تقنية المعلومات
خوادم الأنظمة
غيرها
PBX
برتوكول الصوت عبر الانترنت Voip
الفاكس
الهاتف المتنقل
أجهزة الطباعة
نظام تقنية المعلومات للعميل
أجهزة الحاسب الآلي (سطح المكتب)
أجهزة الحاسب الآلي المحمول
أجهزة المساعدات الرقمية الشخصية/ الهواتف الذكية
تطبيقات تقنية المعلومات
تطبيقات العمل
تطبيقات قاعدة البيانات
تطبيقات التعاملات الالكترونية
تطبيقات خادم الويب
تطبيقات أنظمة الرد الآلي الصوتي (IVP)
تطبيقات البريد الالكتروني

(الشكل ٣)

للإطلاع على نماذج من السياسات الأمنية المتعلقة بأنظمة معلومات محددة، فضلاً راجع الملحق (٣).

بالرجوع إلى العينة المختارة في الصفحة السابقة (الشكل ٣) من المعايير الأمنية المتعلقة بأنظمة محددة، فإن مستودع سياسات أمن المعلومات المتعلقة بأنظمة محددة يتصف بما يلي:

- يحدد الضوابط المطلوبة لمعالجة المخاطر المتعلقة بأنظمة محددة فيما يشير إلى ما يتعلق من سياسات أمن المعلومات العامة التي تنطبق على النظام بصفة عامة.
- يطور بنود المعايير وفقاً للضوابط المحددة.
- يحدد مستوى السرية، التكامل، والتوافر (CIA: Confidintiality، Integrity، and Availability) مثل (عالي، متوسط، عادي) لكل بند من بنود السياسات.

بعض نماذج السياسات المتعلقة ببعض الأنظمة التي سبق ذكرها في الشكل السابق الواردة أعلاه ترتبط بسياسة أمن معلومات عامة محددة. وتستخدم سياسات أمن المعلومات المتعلقة بأنظمة محددة جنباً إلى جنب مع سياسات أمن المعلومات العامة وأفضل الممارسات الأمنية ذات العلاقة لتطوير برامج مراجعة وتدقيق أمن المعلومات لدى الجهات الحكومية، ورسائل التوعية بأمن المعلومات كجزء من خطة التوعية.

للمزيد من المعلومات حول السياسات الأمنية المتعلقة بأنظمة معلومات محددة، فضلاً راجع مستودع سياسات أمن المعلومات المتعلقة بأنظمة محددة.

## ١٢.٤. نموذج مستودع الإجراءات

يشتمل الجدول أدناه على قائمة مدمجة لإجراءات أمن المعلومات:

| الرقم | الإجراء | الوصف |
|---|---|---|
| ١ | التوعية بأمن المعلومات | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها لتطوير وتنفيذ خطة التوعية بأمن المعلومات. |
| ٢ | سياسة إدارة الوصول للأنظمة | يدير هذا الإجراء وصول المستخدمين إلى أنظمة المعلومات لدى الجهات الحكومية. |
| ٣ | الحماية من الشفرات الخبيثة | يساعد هذا الإجراء على تخفيف مخاطر أمن المعلومات المصاحبة لاكتشاف/ تحديد فيروسات / شفرات خبيثة. |
| ٤ | إدارة حوادث أمن المعلومات | يقدم هذا الإجراء الأنشطة المتعلقة بالتعامل مع الحوادث الأمنية وجميع الإجراءات ذات العلاقة بما في ذلك التحري عن وتحليل ومتابعة حالة الحوادث. |
| ٥ | أمن الموظفين | يحدد هذا الإجراء المبادرات الرئيسية التي سيتم القيام بها لحماية أنظمة المعلومات لدى الجهات الحكومية من سوء الاستخدام، أو التدمير من قبل الموظفين والمقاولين. |

| الرقم | الإجراء | الوصف |
|---|---|---|
| ٦ | مراقبة أمن المعلومات | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها لمراقبة تكامل أمن وأنظمة المعلومات لدى الجهات الحكومية. |
| ٧ | إدارة أصول المعلومات | يحدد هذا الإجراء الخطوات المحددة التي ستستخدمها الجهات الحكومية لتحديد أنظمتها المعلوماتية وتصنيف تلك الأنظمة من خلال فحص وتحديد المخاطر المصاحبة لها. |
| ٨ | إدارة سياسات أمن المعلومات | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها لإدارة سياسات وإجراء أمن المعلومات لدى الجهات الحكومية. |
| ٩ | الأمن الداخلي والبيئي | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها لضمان وجود الضوابط الضرورية لتقليل مخاطر السرقة و/أو إلحاق الضرر بالمعلومات وأنظمة المعلومات. |
| ١٠ | النسخ الاحتياطية والاسترجاع في حالة الكوارث | يحدد هذا الإجراء المبادرات التي سيتم القيام بها لوضع القواعد المتعلقة بالنسخ الاحتياطية، وتخزين واستعادة المعلومات الإلكترونية. |
| ١١ | إدارة حوادث أمن المعلومات | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها للتأكد من أن الأمن هو جزء متكامل لأنظمة المعلومات. |
| ١٢ | إدارة التغيير | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها للتحكم بالتغييرات التي تجري على أنظمة المعلومات لدى الجهات الحكومية من أجل التقليل من أثر الحوادث الناشئة عن التغيير على جودة الخدمة إلى أقصى حد ممكن. |
| ١٣ | الالتزام بالمتطلبات القانونية | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها لمراقبة التشريعات والأنظمة التي قد تتضمن قوانين تنطبق على الجهات الحكومية فيما يتعلق بأمن المعلومات. |
| ١٤ | تقييم أمن المعلومات | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها للتأكد من وجود ضوابط أمن معلومات مناسبة لأنظمة المعلومات (أو مجموعة من أنظمة المعلومات) لدى الجهات الحكومية. |
| ١٥ | تدقيق أمن المعلومات | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها للتأكد من وجود ضوابط أمن معلومات مناسبة لأنظمة المعلومات (أو مجموعات أنظمة المعلومات) لدى الجهات الحكومية والخدمات وأنشطة سير العمل. |
| ١٦ | التعامل مع الوسائط الإلكترونية | يحدد هذا الإجراء الأنشطة الرئيسية التي سيتم القيام بها لحماية الوسائط الإلكترونية لدى الجهات الحكومية مثل (منافذ USB، الأقراص الصلبة، البيانات المدخلة/ المخرجة) من التلف، والسرقة، والوصول غير المصرح به. |

جميع الإجراءات المقترحة مرتبطة بالإجراءات المتعلقة بسياسات أمن المعلومات العامة، وتستخدم لتحديد الخطوات الواجب اتباعها للتأكد من تحقيق أهداف بنود هذه السياسات.

للمزيد من التفاصيل حول إجراءات أمن، فضلاً راجع وثيقة إجراءات أمن المعلومات.

## ١٢.٥. خيارات تعيين إدارة أمن المعلومات

لقد تطور تنظيم أمن المعلومات على مدى عدة ع قود ماضية، متخذاً أسماءً عدة، مثل أمن البيانات، أمن الأنظمة، إدارة الأمن، أمن المعلومات، وحماية المعلومات. وجاءت تلك التسميات لتعكس توسع نطاق أعمال إدارات أمن المعلومات. وبصرف النظر عن المسمى الذي تتبعه الجهات الحكومية، فإن التركيز الأساسي لتنظيمات أمن المعلومات هو التأكد من سرية، وتكامل وتوافر المعلومات.

ولا يوجد حاليا نموذج واحد ضمن الهياكل التنظيمية لأمن المعلومات ينطبق على جميع حالات إدارة أمن المعلومات أو نطاق المسئوليات. كما أن الموقع الذي يجب أن يكون تنظيم أمن المعلومات تابعاً له قد تطور كذلك. وقد تم إعداد وثيقة تحتوي على خيارات تعيين إدارة أمن المعلومات (أي خيارات وضعها ضمن الهيكل التنظيمي للجهة)، وذلك لمساعدة الجهات الحكومية التي ليست لديها إدارة أمن معلومات حالياً على تأسيس تلك الإدارة بناءً على المبادئ المحددة في الوثيقة المذكورة. أما الجهات الحكومية التي لديها إدارة أمن معلومات، فيجب أن تكون مسئولة عن التأكد من أن المسئوليات الحالية لإدارة أمن المعلومات لديها تتوافق مع ما تضمنته وثيقة تعيين إدارة أمن المعلومات، وبالتالي، فإن عليها أن تأخذ في اعتبارها تعزيز هيكل أمن المعلومات الحالي لديها باستخدام الوثيقة المذكورة والاسترشاد بها.

وتقدم وثيقة خيارات تعيين إدارة أمن المعلومات خيارات مختلفة لوضع إدارة أمن المعلومات ضمن الهيكل التنظيمي لدى الجهات الحكومية في المملكة العربية السعودية، على اعتبار إيجابيات وسلبيات كل خيار. والحل المختار لتعيين إدارة أمن المعلومات لدى الجهات الحكومية سيأكد على تعيين الأدوار والمسئوليات للأشخاص/ الوظائف ذات العلاقة وفقاً للهيكل التنظيمي لأمن المعلومات في إطار سياسات وإجراءات أمن المعلومات لدى الجهات الحكومية.

وتتضمن وثيقة خيارات تعيين إدارة أمن المعلومات كذلك الأدوار والمسئوليات المتعلقة بمراجعة وتدقيق أمن المعلومات ووحدة متابعة التنفيذ (ضمن إدارة الأمن). ويتضمن ذلك مسئوليات الوحدة نحو القيام بمتابعة تنفيذ سياسات وإجراءات أمن المعلومات لدى الجهات الحكومية، وكذلك القيام بمراجعات وتدقيق مستمر لتلك السياسات والإجراءات (مثل المراجعة السنوية).

لمزيد من التفاصيل حول خيارات تعيين إدارة أمن المعلومات، فضلاً راجع وثيقة خيارات تعيين إدارة أمن المعلومات.

## ١٢.٦. عملية تنفيذ سياسات وإجراءات أمن المعلومات

عند اكتمال تطوير، وتعديل، وتحديث، والاتفاق على جميع سياسات وإجراءات أمن المعلومات، فيجب أن يلي ذلك عملية تنفيذ الجهات الحكومية لسياسات وإجراءات أمن المعلومات المحددة. وتكون هذه المرحلة في العادة أصعب من إعداد السياسات والإجراءات، وذلك لأن الجهات الحكومية تحتاج في هذه المرحلة إلى تدريب وتعليم موظفيها للتصرف بشكل "آمن" والالتزام بكل عنصر أساسي مشار إليه في السياسات والإجراءات الأمنية الرسمية.

لا يتطلب التنفيذ الملائم تثقيف الموظفين فحسب حول كل عنصر من العناصر الأساسية الحرجة في السياسات والإجراءات الأمنية الرسمية، ولكن يتطلب أيضاً تغيير أدوار هؤلاء الموظفين في محاولة لحماية أنظمة المعلومات المهمة لدى الجهات الحكومية.

وبعد الاعتماد الرسمي لسياسات وإجراءات أمن المعلومات، فإنه

ينبغـي على كل جهة حكومية أن تبـدأ بالتنفيذ المرحلي لسياساتها وإجراءاتها المعتمدة باستخـدام عملية تنفيذ سياسات وإجراءات أمن المعلومات. وستتأكد الجهات الحكومية خلال تلك العملية من سـد الفجوة التي كانت لديها فيما يتعلق بسياسات وإجراءات أمن المعلومات. وتتم هذه العملية بالتـوازي مع التوعية بأمن المعلومات التي تم تقديمها كجزء من هذا الإطار.

لمزيـد مـن المعلومات حـول عملية تنفيـذ سياسـات وإجـراءات أمن المعلومات، فضلاً راجع دليل تنفيذ سياسات وإجراءات أمن المعلومات.

## ١٢. ٧. نموذج من خطة التوعية

يمكن تعريـف برنامج التوعيـة الأمنية بأنه أحد العوامـل الرئيسية المساعـدة على التنفيذ الناجح لسياسات وإجـراءات أمن المعلومات في كامل الجهة الحكومية. ويهـدف البرنامج إلى بيان الدور المحدد لكل موظف في إطار المجهـود الجماعي لتوفير أمن أنظمة المعلومات في الجهات الحكومية، حيث يقوم البرنامج بالتغطية التفصيلية لكل عنصر أساسي ضمن سياسات وإجراءات أمن المعلومات. كما يهدف البرنامـج إلى توليد اهتمام متزايد في مجال أمن المعلومات بطريقة سهلـة الفهم وفاعلة حيث تساهـم في تعزيز فهم الموظفين بالمخاطر الأمنية وأهمية الأمن لإجراءات العمل لدى الجهات الحكومية.

لتطوير وتنفيـذ برنامج التوعية بأمن المعلومات، يتعين على الجهة الحكوميـة الرجوع إلى إجراء خاص بأمـن المعلومات ضمن وثيقة الإجـراءات والذي يوضـح الخطوات الرئيسية التـي عليها القيام بهـا، كمـا يشتمل على نمـوذج لبرنامـج التوعية بأمـن المعلومات والذي يعد جزءا من هـذا الإطار. وسيساعد نموذج التوعية بأمن المعلومات الجهات الحكومية علـى تنفيذ سياسات وإجراءات أمن المعلومـات من خلال رفـع الوعي بين موظفيها فيمـا يتعلق بالأمن وأهميتـه. ويتضمن البرنامج بنوداً مثل نماذج من الرسائل، طرق ووسائل تبليغ تلك الرسائل، وعدد مرات التذكير بها.

لمزيـد من المعلومات حول تطوير برنامـج التوعية بأمن المعلومات، فضـلاً راجـع وثيقة إجـراءات أمـن المعلومـات ووثيقـة النموذج المقدمة لبرنامج التوعية بأمن المعلومات.

## ١٢. ٨. عمليـــــــة إدارة التغييـر (مشـمولة فـي دليل التنفيذ)

إن الغرض مـن عمليـة إدارة التغيير هو تقـديم التوجيه والآليات لتسهيـل مواجهة الموظـف للفـترة الانتقالية التي تمـر بها الجهة الحكوميـة من حالتهـا الراهنـة إلى الحالة المستقبليـة المرغوبة، وذلك وفقـاً لمتطلبات عمليـة تنفيذ أمن المعلومـات. وتعنى عملية إدارة التغيـير بالجانـب المتعلـق بالموظفين من التغيـير المصاحب لتنفيذ سياسات وإجراءات أمن المعلومات.

ولدعـم هذا المفهـوم، تتضمـن عمليـة إدارة التغيـير العديد من العناصر مثل تقييم وتخفيف المخاطر، وتكوين فريق لإدارة التغيير يتميز بالنشاط والتماسـك، وإدارة مقاومة التغيير، والاتصال مع وإشـراك جميـع الأطراف ذات العلاقة. إضافـة لذلك فإن عملية إدارة التغيـير تقدم نقطة مرجعيـة وتوائم بين جميع أنشطة إدارة التغيـير والتوعية طوال مراحل تنفيذ سياسات ومعايير وإجراءات أمن المعلومات.

إن عمليـة إدارة التغيـير التي تم تطويرها ستدعـم التنفيذ الناجح لسياسات وإجراءات أمن المعلومات من خلال المساعدة على تخفيف التحديات التنظيمية والفردية التي من شأنها إعاقة التنفيذ.

للمزيد من المعلومات حول الجوانب المتعلقة بإدارة التغير في تنفيذ سياسات وإجراءات أمن المعلومات، فضلاً راجع دليل التنفيذ.

## ٩.١٢. عملية مراجعة وتدقيق أمن المعلومات

إن الغرض من عملية مراجعة أمن المعلومات هو رسم منهجية أساسية لاتباعها من قبل الجهات الحكومية فيما يختص بالآتي:

- تخطيط وتبليغ عمليات مراجعة أمن المعلومات لديها.
- تنفيذ عمليات مراجعة أمن المعلومات لديها.
- تبليغ ومتابعة نتائج عمليات مراجعة أمن المعلومات لديها، وكذلك متابعة الإجراءات الواجب اتخاذها حيال ذلك.

تحتوي وثيقة الإجراءات على الخطوات الأساسية التي يجب أن تقوم بها الجهات الحكومية لتطوير وتنفيذ مراجعات أمن المعلومات، إضافة إلى احتواءها على نموذج لعملية مراجعة أمن المعلومات كجزء من الإطار الكلى.

بعد استكمال إعداد وتنفيذ سياسات وإجراءات أمن المعلومات لدى الجهات الحكومية بشكل رسمي، فإن على تلك الجهات تطوير وتنفيذ مراجعة أمن المعلومات لديها باستخدام عملية مراجعة أمن المعلومات المقدمة. إن برامج مراجعة أمن المعلومات التي تم تطويرها والتي تشكل جزءاً من عملية المراجعة والتدقيق، تستخدم الضوابط المذكورة في مستودعات نماذج سياسات أمن المعلومات العامة وسياسات أمن المعلومات المتعلقة بأنظمة محددة. كما تستخدم برامج المراجعة هذه أفضل الممارسات الموصى بها من قبل موردي التقنية ومن مصادر مرموقة أخرى.

للمزيد من التفاصيل حول عملية مراجعة وتدقيق أمن المعلومات، فضلاً راجع وثيقة إجراءات أمن المعلومات ووثيقة نموذج عملية مراجعة أمن المعلومات.

الجزء الثاني

# دليل إعداد وتطوير سياسات وإجراءات أمن المعلومات

## ١. لمحة عامة

بمـا أن وجـود سياسـات وإجـراءات أمـن معلومـات جيـدة يوفر الاساسيـات للتنفيذ الناجـح للسياسات المتعلقـة بأمن المعلومات، فـإن ذلك يعتبر المقياس الأول الواجب اتخاذه للتقليل من مخاطر الاستخدام غير المقبول لمصادر المعلومات لدى الجهات الحكومية.

فالخطوة الأولى نحو تعزيز الأمن لدى الجهة الحكومية هو إدخال سياسـات وإجراءات أمن معلومات دقيقة وقابلـة للتطبيق، وتبليغ الموظفـين بالجوانب المختلفة من مسئولياتهـم، والاستخدام العام لمـوارد الجهـة الحكوميـة، وتوضيح كيفيـة التعامل مـع المعلومات الحساسـة. ويجب أن تصـف السياسات كذلـك بالتفصيل معنى الاستخدام المقبول، وأن تذكر كذلك الأنشطة المحظورة.

إن التطوير (والتنفيذ الملائم) لسياسات وإجراءات أمن المعلومات نافع جداً كونه يحوّل جميع موظفي الجهة الحكومية إلى مشاركين في جهودها للحفاظ على أمن اتصالاتها، ليس هذا فحسب، وإنما يساعـد كذلـك على تخفيف مخاطـر المخالفات الأمنيـة المحتملة الناتجـة عـن أخطـاء "العامل البشـري" ويتعلق هـذا الأمر بعدة مشـاكل مثـل قيام الموظفـين بالكشف عن المعلومـات إلى مصادر غير معروفـة (أو غير مصرح لها)، الاستخدام غير الآمن أو غير اللائق للإنترنت، والكثير من الأنشطة الأخرى الخطرة.

إضافـة لمـا تقدم، فـإن عمليات بنـاء سياسـات وإجـراءات أمن المعلومـات ستساعـد أيضـاً على تحديـد أنظمة المعلومـات المهمة والحساسـة لـدى الجهـة الحكوميـة، والطـرق الواجـب اتباعها لحمايتهـا، وتخـدم كذلـك بمثابـة وثيقـة مركزية تُعنـى بحماية أنظمة المعلومات.

تعـد الجهـات الحكوميـة التـي لا يوجـد لديهـا حاليـاً سياسات وإجـراءات أمن معلومات مسئولة عـن تطوير سياسات وإجراءات أمن المعلومات لديها بناءً على الإرشادات المذكورة في هذه الوثيقة. أمـا لجهات الحكومية التي توجد لديهـا سياسات وإجراءات لأمن المعلومـات، فهي مسئولة عن التأكد مـن أن سياساتها وإجراءاتها الحاليـة تغطي السياسات والإجراءات التي تنطبق عليها والمقدمة ضمن هذا الإطار.

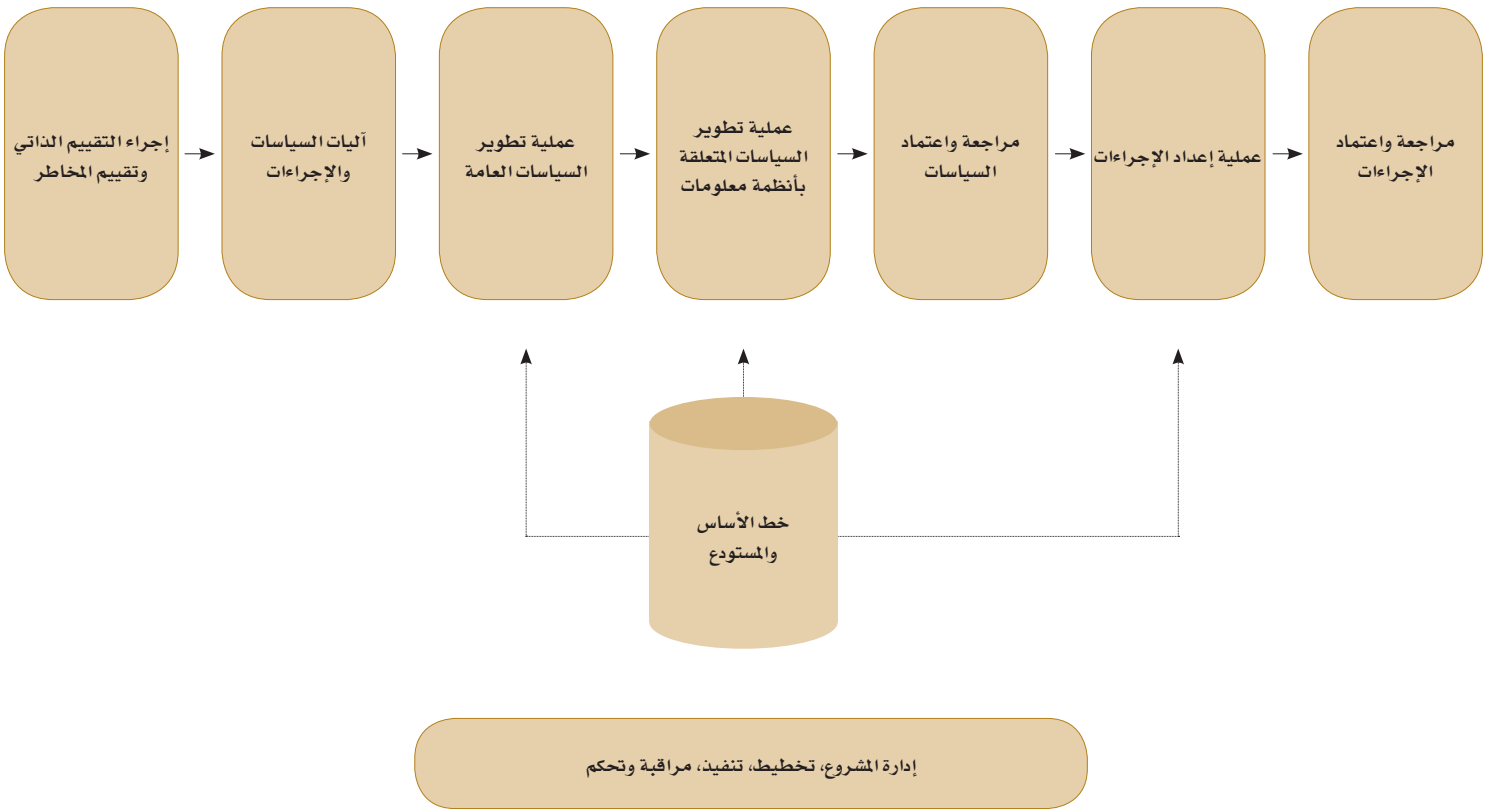
## ٢. الهدف

تهدف عملية تطوير سياسات وإجراءات أمن المعلومات إلى تحديد منهجيـة أساسية يجب اتباعها من قبل الجهات الحكومية لتطوير سياسات وإجـراءات مناسبة تتناغم مع أهداف البرنامج الشامل لإدارة امن المعلومات ضمن كل جهة حكومية، والتأكد في نفس الوقت مـن إلمام الموظفـين، والمقاولين، والأطـراف الثالثـة بمسئولياتهم لحماية أنظمة المعلومات القيّمة والمعلومات الحساسة.

## ٣. وصف العملية

تساعـد عملية تطوير سياسات وإجـراءات أمن المعلومات الجهات الحكومية على تطوير سياسات وإجراءات أمن المعلومات لديها بما يتوافق مع أفضل الممارسات، ومتطلبات الأعمال الفردية، والأنظمة واللوائـح المناسبـة، الأمر الذي يؤدي إلى وضـع وتطبيق سياسات وإجـراءات فاعلـة لأمـن المعلومـات، والتـي تساعد علـى تأسيس طريقة متماثلة وقابلة للتكرار لإدارة مخاطر أمن المعلومات.

ويوضـح الشكل التـالي العمليـات الرئيسية التي يجـب أن تتبعها الجهة الحكومية لتطوير سياسات وإجراءات أمن المعلومات لديها.




الشكل ٤

*ملاحظة: يشتمل المستودع الأساسي على السياسات العامة، والسياسات المتعلقة بأنظمة محددة، والإجراءات العامة التي يتم تقديما كجزء من الحزمة، مع إطار تطوير سياسات ومعايير وإجراءات أمن المعلومات. وسيستخدم هذا المستودع كمرجعية أساسية من قبل الجهة لتحديد الحد الأدنى من المتطلبات المتوقعة من قبل الجهة بموجب هذا الإطار.

## ٤. تخطيط المشروع، وتحديد نطاق تطوير سياسات وإجراءات أمن المعلومات

### ٤.١. الأهداف

تهدف الخطوة الأولى إلى التأكد من تنفيذ عملية تطوير سياسات وإجراءات أمن المعلومات كمشروع. وحسبما يتضح من الرسم البياني أعلاه، فإن العملية برمتها ستتبع ممارسات إدارة المشاريع في التخطيط والتنفيذ والرقابة.

وسيتم إطلاق المشروع بمجرد اعتماده من الإدارة العليا للجهة الحكومية.

### ٤.٢. تحديد الأدوار والمسئوليات

سيكون على المسئول التنفيذي الأول تعيين الأدوار والمسئوليات عن مشروع تطوير سياسات وإجراءات أمن المعلومات. وستكون الأدوار التالية مطلوبة لعملية التطوير:

- المسئول عن المشروع: يتم تعيين هذا الدور عموماً إلى المسئول التنفيذي الأعلى في الجهة. ويجب على المسئول عن المشروع أن يبدأ المشروع وسيكون مسئولاً عنه، ويضطلع بالمسئوليات التالية:
  - قيادة المشروع.
  - تأمين اعتماد ميزانيات المشروع.
  - تقبل المسئولية عن المشاكل الذي قام مدير المشروع بتصعيدها.
  - تحديد أهداف وغايات المشروع.
  - تحديد مؤشرات الأداء الرئيسية المستهدف.
  - تحديد أعضاء لجنة التوجيه.
- لجنة التوجيه: وظيفتها الأساسية الإشراف على نشاطات إدارة المشروع التي يؤديها مدير المشروع. ويتضمن ذلك، دون حصر، مراجعة تقييم المتطلبات، وتقارير نتائج التحليل (الفجوة بين الوضع المرغوب مستقبلا في مقابل الوضع الحالي)، والمراقبة المستمرة، ومراجعة المشروع بالكامل. ويجب أن تتأكد لجنة التوجيه من إطلاع جميع الأطراف المعنية بحالة المشروع وتقدم سير العمل فيه. وتضطلع لجنة التوجيه بالمسئوليات التالية:
  - مراجعة واعتماد مخرجات التقييم الذاتي
  - التحقق من صحة وتحديد أولويات المخاطر المحددة
  - مراجعة واعتماد المخاطر المحددة
  - مراجعة التقارير الصادرة عن مدير المشروع
  - مراجعة التقارير إزاء مؤشرات الأداء العامة المستهدفة.
- مدير المشروع: يكون مسئولاً عن تخطيط وتنفيذ مشروع تطوير سياسات وإجراءات أمن المعلومات. ويضطلع بالمسئوليات التالية:
  - الحفاظ على الأهداف والغايات التي حددها المسئول عن المشروع.
  - تعيين فريق المشروع.
  - إجراء تقييم ذاتي، وإعداد التقارير لعرضها على لجنة التوجيه.
  - تقييم احتياجات المشروع للموارد.
  - تقييم وإعداد الميزانية التقديرية المطلوبة للمشروع.
  - تحديد أولويات المراحل المختلفة لعملية التطوير.
  - التأكد من الالتزام بخطة المشروع المعتمدة.
  - التأكد من تمتع الموارد البشرية بالمهارات المطلوبة.
  - مراقبة ومتابعة المشروع.

- الدعوة إلى وتسهيل اجتماعات الإدارة العليا لتدارس المشاكل الرئيسية وإجراء المراجعة والموافقة على الحلول.

- فريق المشروع: يتكون فريق المشروع من أعضاء من إدارة أمن المعلومات وإدارة تقنية المعلومات، ويضطلع بالمسئوليات التالية:
  - إجراء التقييم الذاتي.
  - إجراء تقييم المخاطر.
  - تطوير سياسات وإجراءات أمن المعلومات.
  - تصميم وتطوير سياسات وإجراءات أمن المعلومات بحسب المتطلبات والاحتياجات.
  - تنفيذ المهام التي كلفهم بها مدير المشروع.

## ٤.٣. تطوير عقد وخطة المشروع

يكون مدير المشروع مسئولاً عن إعداد لائحة المشروع وخطة المشروع. وقد تم تضمين نموذج عقد المشروع في الملحق (٢)، ويهدف العقد إلى التعامل مع الجوانب التالية:

- تحديد الأطراف المعنية الرئيسية.
- تحديد نطاق العمل في مشروع تطوير سياسات وإجراءات أمن المعلومات، ويمكن أن يتضمن النطاق واحداً أو أكثر من الأمور التالية:
  - جميع أنظمة المعلومات لدى الجهة الحكومية أو جزء محدد منها.
  - وظائف العمل الأساسية لدى الجهة الحكومية.
  - المكتب الرئيسي للجهة الحكومية.
  - المكتب الرئيسي والمكاتب الفرعية / الجهات التابعة للجهة الحكومية.
  - إلخ.
- تحديد الخطوات، وتسلسل الأعمال، والإطار الزمني للمشروع المحدد.
- تحديد فريق المشروع.

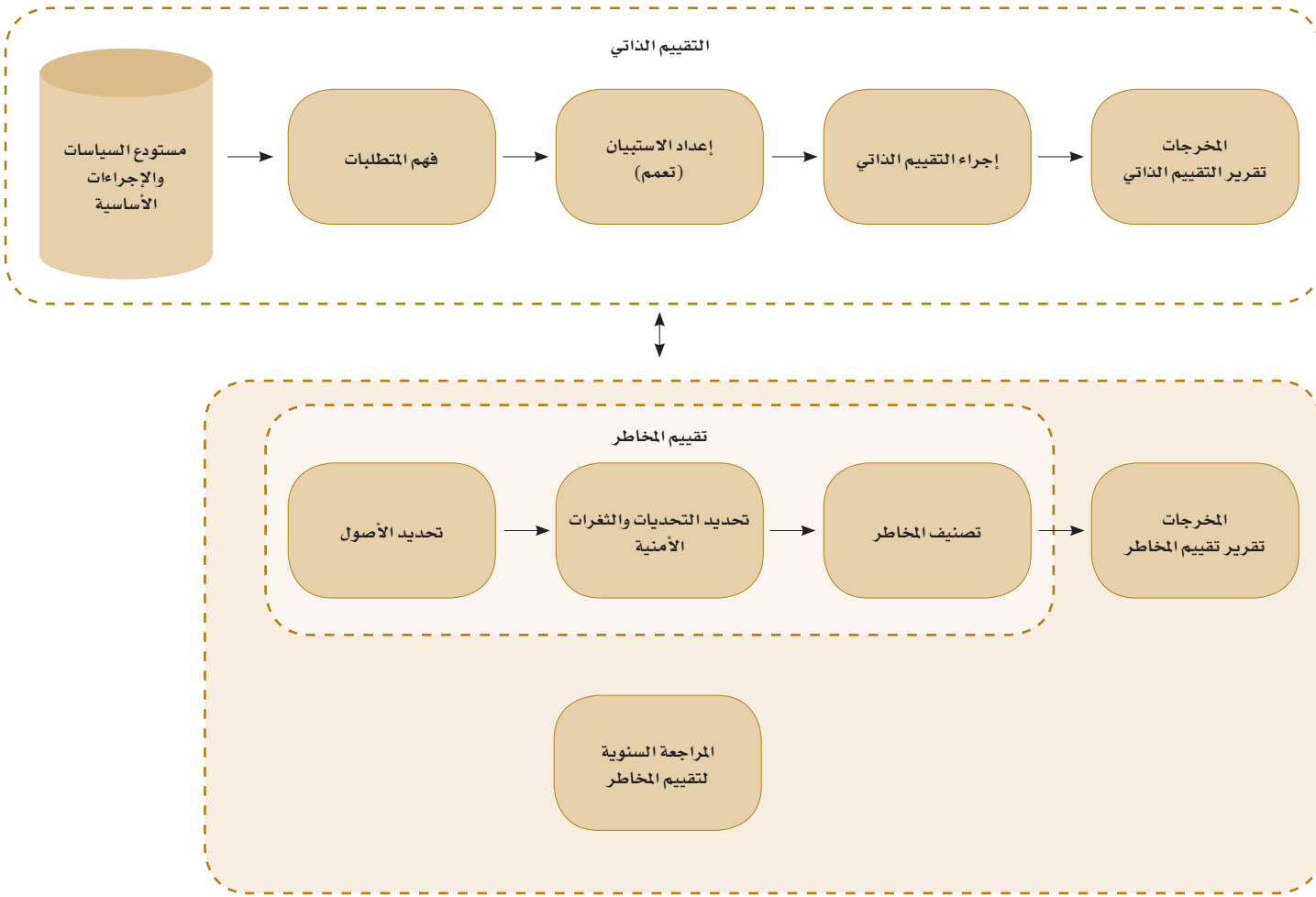
تم تضمين المزيد من المعلومات حول الجوانب المختلفة لإدارة المشروع، بما في ذلك نطاق العمل في المشروع، ضمن دليل التنفيذ.

## ٤.٤. إجراء التقييم الذاتي وتقييم المخاطر

عملية التقييم الذاتي هي جزء أساسي من إطار التطوير العام، والهدف منها مزدوج، فهي تهدف أولاً إلى معرفة موقف الجهة فيما يتعلق بوجود الحد الأدنى من السياسات الأمنية الأساسية لديها، وتهدف ثانياً إلى المساعدة في تطوير أو إعادة تطوير وتصميم سياسات وإجراءات أمنية شاملة تلبي المتطلبات الأمنية لديها كما في (الشكل ٥).

وتقع مسئولية إجراء وتنسيق مراحل التقييم الذاتي للمخاطر الأمنية على مدير مشروع التطوير، والذي من المحبذ أن يكون مدير / مسئول أمن المعلومات، وفي حال عدم توفر هذا المنصب لدى الجهة، فإن الشخص التالي المناسب لإجراء هذه التقييمات سيكون هو مدير تقنية المعلومات، الذي يجب أن يكون لديه فهم مناسب وخبرات ملائمة في أعمال تقنية المعلومات والعمليات المتبعة لدى المؤسسة.

ومن الملاحظ أيضاً، أنه بينما يكون مدير المشروع مسئولاً عن إجراء هذه التقييمات، فإن مصدر المعلومات سيظل هو الطرف المعني الرئيسي مع المسئولين عن العمل. وستكون مدخلاتهم عنصراً أساسياً في هذه التقييمات.


التقييم الذاتي
مستودع السياسات والإجراءات الأساسية
فهم المتطلبات
إعداد الاستبيان (تعمم)
إجراء التقييم الذاتي
المخرجات تقرير التقييم الذاتي
تقييم المخاطر
تحديد الأصول
تحديد التحديات والثغرات الأمنية
تصنيف المخاطر
المخرجات تقرير تقييم المخاطر
المراجعة السنوية لتقييم المخاطر

(الشكل ٥)

### ٤. ٤. ١. فهم المتطلبات

لأداء التقييم الذاتي، يتوجب على الجهة أن تفهم وتدرك أولاً التزاماتها ومتطلباتها بخصوص أمن المعلومات. يقوم مدير المشروع، أو أحد أعضاء فريق تطوير السياسات، باستخدام الآليات التالية لإجراء التقييم الذاتي.

#### ١. الاجتماع مع الأطراف المعنية الرئيسية

يجب أن يتم الاجتماع مع الأطراف المعنية الرئيسية لفهم دوافع العمل والتقنية التي تؤثر على الجهة، وتهدف هذه الاجتماعات إلى فهم العمليات المتبعة لدى وظائف (إدارات وأقسام) العمل الرئيسية وخدمات التقنية الرئيسية أو الوظائف المساندة.

يجب الاجتماع مع الموظفين المسئولين عن الجوانب الرئيسية التالية لهذا الغرض:

- تقنية المعلومات.
- الموارد البشرية.
- الشئون الإدارية والمرافق.
- الشئون المالية.
- دعم خدمات الشبكة.
- دعم تقنية المعلومات.
- تطوير التطبيقات، إذا كان ذلك يتم داخلياً.
- مركز البيانات.

#### ٢. مراجعة الوثائق

ستعطي دراسة الوثائق الرئيسية ذات العلاقة معلومات تعين على فهمّ العمليات، والأنشطة، والأساليب التشغيلية.

وفيما يلي العوامل الرئيسية المتعين أخذها في الاعتبار:

**١. عوامل تقييم المخاطر التي تتعرض لها الجهة الحكومية**

يجب أن يفهم مدير المشروع البيئة التي تعمل ضمنها الجهة الحكومية. وفيما يلي بعض العوامل الرئيسية:

- تحديد عملائها الرئيسيين.
- تحديد عدد ومدى أهمية الخدمات المقدمة.
- عدد مواقع العمل للجهة الحكومية.
- مدى أهمية الأصول لدى الجهة الحكومية.
- توقعات الأطراف المعنية وفقد الشهرة والسمعة.

**٢. الأنظمة واللوائح المطبقة**

يتعين على الجهة تحديد جميع الأنشطة واللوائح ذات العلاقة المطبقة في المملكة العربية السعودية. ويتضمن ذلك المتطلبات النظامية والإشرافية أو اتفاقيات العقود مع الجهات/ المؤسسات الأخرى.

يمكن استخدام نتائج هذه المرحلة لتحديد أولويات تنفيذ الضوابط في مرحلة معالجة المخاطر.

## ٤. ٤. ٢. إعداد الاستبيان

لمساعدة الجهة على تحديد الفجوات في إطار أمن المعلومات، يقوم فريق مشروع التطوير بإعداد استبانة تقييمية، وهي عبارة عن أداة لإجراء تقييم للضوابط المطبقة في كل مجال من مجالات السياسات المتبعة لدى المؤسسة. ويجب أن تستند الاستبانة على مجالات السياسات المدرجة في الجدول (١)، وأن يغطي وظائف العمل المهمة والحساسة لدى الجهة الحكومية.

### ١. هيكل الاستبانة

تحتوي استبانة التقييم الذاتي على ثلاثة أقسام وهي: مقدمة، أسئلة حول الضوابط الحالية والمتوقعة في مجالات السياسة قيد المراجعة، وإيضاحات/ ملاحظات إضافية. ويجب أن تحتوي الاستبانة على صفحة مقدمة يُطلب فيها إدراج وصفاً لمجال السياسة الجاري تقييمها، كما أنه يتضمن تصنيف السرية، والتكامل، والتوافر لأصول الجهة.

وقد تم تضمين نموذج عينة لاستمارة التقييم الذاتي في الملحق (٤).

ويمكن تقسيم الأسئلة إلى فئتين رئيسيتين اعتماداً على مجال السياسة التي سيتم تغطيتها، وهما: (١) الضوابط الإدارية، و(٢) الضوابط الفنية حسبما يتضح من الجدول (١).

الجدول رقم (١)

| مجالات السياسات التي تحتاج لضوابط إدارية | مجالات السياسة التي تحتاج لضوابط فنية |
|---|---|
| سياسة أمن معلومات الجهة | سياسة إدارة الوصول المنطقي |
| مسئوليات أمن المعلومات | الحماية من الشفرات الخبيثة |
| التوعية بأمن المعلومات | التعامل مع الوسائط الإلكترونية |
| الاستخدام المقبول لأنظمة المعلومات | إدارة حوادث أمن المعلومات |
| أمن الوثائق | أمن الموظفين |
| الخصوصية | إدارة أصول المعلومات |
| الغش والتبليغ عن المخالفات | الأمن المادي والبيئي |

| مجالات السياسات التي تحتاج لضوابط إدارية | مجالات السياسة التي تحتاج لضوابط فنية |
|---|---|
| إدارة مخاطر أمن المعلومات | النسخ الاحتياطية والاستعادة في حالة الكوارث |
| إدارة سياسات أمن المعلومات | الخدمات الإلكترونية |
| الالتزام بالمتطلبات القانونية | شراء وتطوير أنظمة المعلومات |
| إدارة الخدمات المقدمة من طرف ثالث | إدارة التغيير |
| مقدمو خدمات الاستعانة بمصادر خارجية | مراقبة أمن المعلومات |
| سياسة العملاء | تقييم أمن المعلومات |
| | مراجعة وتدقيق أمن المعلومات |
| | الالتزام بالسياسات والإجراءات المحددة |
| | إدارة استمرارية العمل |

لكـي يتسنى قياس فاعليـة الضوابط (عناصر التحكم) الحالية، وكذلك لتحسين فاعلية السياسـات ذات العلاقة خلال السنوات القادمة، فقد تم تحديد خمس مستويات لقياس الفاعلية لكل سؤال يتعلق بالضوابط.

- مستوى الفاعلية/ ١- هدف الضوابط موثق في السياسة الأمنية، ولكنه لا يحتوي على أي إجراءات، والضوابط غير مطبقة.
- مستوى الفاعلية/ ٢- ضوابط أمنية موثقة في الإجراءات ولكنها غير مطبقة.
- مستوى الفاعلية/ ٣-تم تطبيق الإجراءات، ولكن لا يتم فحصها أو مراجعتها.
- مستوى الفاعلية/ ٤- يتم إجراءات وضوابط أمنية يتم فحصها ومراجعتها دورياً.
- مستوى الفاعلية/ ٥- الإجراءات والضوابط الأمنية متكاملة بشكل تام ضمن برنامج شامل.

## ٤. ٤. ٣. إجراء التقييم الذاتي

### ١. مسئوليات التقييم الذاتي

أ. يفضل أن يكون الشخص الذي يقوم بإجراء التقييم الذاتي أحد موظفي أنظمة المعلومات وملماً بمجال السياسة التي قيد المراجعة. وسيكون هذا الشخص عضواً في فريق المشروع المسئول عن السياسات والإجراءات بما يتوافق مع هذا الإطار.

ب. يجب أن تتم مقابلة الأشخاص المسئولين عن المجالات الرئيسية التالية لإدارة الاستبانة:

- تقنية المعلومات.
- الموارد البشرية.
- الشئون الإدارية والمرافق.
- الشئون المالية.
- دعم خدمات الشبكة.
- دعم تقنية المعلومات.
- تطوير التطبيقات، إذا كان ذلك يتم داخلياً.
- مركز البيانات.

ج. تقع مسئولية تحليل المعلومات الواردة في هذه الاستبانة على رئيس قسم/ إدارة أمن المعلومات (الذي سيكون كذلك مديراً لمشروع تطوير السياسات والإجراءات هذا). ويجب أن يكون الهدف الأساسي من هذا التحليل تضمين جوانب الضعف أو الفجوات في السياسة ضمن خطوات لاحقة حسبما تم تحديده في وثيقة الإطار هذه.

### ٢. إدارة الاستبانة

يمكن إدارة استبانة التقييم الذاتي باستخدام أكثر من طريقة واحدة من الطرق التالية:

- من خلال فحص الوثائق ذات العلاقة؛
- من خلال الاجتماع مع الأطراف المعنية الرئيسية؛
- من خلال فحص الضوابط، ومثال ذلك فحص سجلات التغيير، حسابات النظام النشطة، إلخ).

إن الوثائق المساندة الموضحة لتفاصيل ونتائج الاختبارات التي تم إجراؤها ستشكل قيمة إضافية للتقييم ويسهل من إجراء المراجعة مستقبلاً.

خلال مرحلة التقييم، إذا وجدت أجزاء من الاستبانة غير مطابقة لمجال السياسة الجاري مراجعتها، فيجب أن يتم التأشير عليها بعبارة «لا ينطبق»، ويجب تسجيل إيضاح لاستبعادها.

يتوجب على الشخص الذي يجري التقييم أن يراجع السياسات والمعايير والإجراءات ذات العلاقة في جميع المجالات التي تنطبق عليها المراجعة، ويقوم بالتقييم حسب التسلسل التالي:

- عدم وجود سياسات ومعايير وإجراءات موثقة، ويؤشر عليها بعبارة «لا يوجد».
- يوجد سياسات ومعايير وإجراءات موثقة، (المستوى-١).
- يوجد إجراءات لتنفيذ الضوابط (المستوى-٢).
- تم تنفيذ الضوابط (المستوى-٣).
- تم فحص وتحسين الضوابط إذا كانت غير فاعلة (المستوى-٤).
- الضوابط هي جزء من الثقافة التنظيمية لدى الجهة (المستوى-٥).

وقد تم إيضاح نموذج للاستبانة في الملحق (٤).

### ٣. تقارير التقييم الذاتي

بعـد اكتمـال التقييم الذاتي، يتوجب علـى مدير المشروع إعداد تقرير التقييـم الذاتي وعرضه على لجنة التوجيـه. ويجب أن يبرز التقرير الفجوات التي تعاني منها الجهة الحكومية بعد تحليل الوضع الحالي لجميع السياسات الأساسية التسع والعشرين، ويجب أن يصف التقرير لكل من التسع والعشرون سياسة الآتي:

- مجالات السياسات الأساسية التي لم يتم نشرها حالياً لدى (اسم الجهة).
- التغطية الجزئية، والفجوات الناتجة في مجالات السياسات التي تم تطبيقها فعلياً.
- تحديد أولويات الفجوات ومجالات السياسات الناقصة بناءً على التقييم.

## ٤. ٤. ٤. تقييم مخاطر أمن المعلومات

يجـب أن يكـون هناك طريقة منهجية لإدارة أمن المعلومات لتحديد الاحتياجات التنظيمية المتعلقة بمتطلبات أمن المعلومات. ويجب أن تعنى الجهود الأمنية بالمخاطر بشكل فاعل وموثوق. ويعد تقييم مخاطر أمن المعلومات جزءاً متكاملاً مع أية عملية لإدارة أمن المعلومات.

وفيمـا يلـي وصفاً نموذجياً لعملية تقييم المخاطر التي سيتم اتباعها من قبل (اسم الجهة) لمعرفة وفهم المخاطر التي تواجهها. وستستخدم النتيجة في المراحل اللاحقة من إطار تطوير سياسات وإجراءات أمن المعلومات.

### ١. تحديد أصول المعلومات

يعـرف الأصـل بأنه أي شئ ذي قيمة لـدى الجهة، وبالتالي يحتاج لحماية. ولأغراض إطار تطوير سياسـات وإجراءات أمن المعلومات هذا، فـإن تركيـز (اسم الجهة) يجب أن يبقى منصباً على أصول المعلومات. ولتسهيل عملية التعريف، يمكن وضع أصول المعلومات في مجموعات حسبما يتضح من الجدول (٢).

الجدول (٢)

| نوع الأصل | الوصف |
|---|---|
| الخدمات الأساسية | الأنشطة الرئيسية لدى الجهة أو الخدمات التي تقدمها |
| الموظفون | المستخدمون العامون، الموظفون الإداريون، الموظفين الفنيون |
| الأجهزة | المعدات والأجهزة الثابتة؛ المعدات المتحركة؛ الوثائق الورقية؛ الوسائط الإلكترونية؛ أجهزة الشبكة |

| نوع الأصل | الوصف |
|---|---|
| البرامج | نظام التشغيل؛ تطبيقات العمل؛ سجلات الإعدادات العامة |
| المعلومات | المعلومات الحيوية للجهة؛ المعلومات الشخصية؛ المعلومات الإستراتيجية؛ السجلات الإلكترونية |
| مقدمو الخدمات | الأطراف الثالثة المقدمة للخدمات؛ الموردون |
| الموقع | الموقع المادي؛ خدمات المنافع العامة |
| الأصول غير الملموسة | سمعة / شهرة المؤسسة |

يجب تحديد مقياس لتقييم أصول المعلومات، وذلك باستخدام وسائل نوعية أو كمية، حيث تحدد طرق التقييم النوعية درجات القيمة، مثل عالية جداً، متدنية، متدنية جداً، متوسطة، فيما تحدد طرق التقييم الكمية قيمة الأصل من حيث القيمة القابلة للعد.

ومن بين الطريقتين المذكورتين، فإن الطرق الكمية لا تستخدم عموماً بسبب الصعوبات العملية في تحديد قيمة الأصول المفردة.

الطريقة النوعية المستخدمة عموماً في تقييم الأصول هي من أجل تقييم القيمة طبقاً للعوامل الثلاثة (السرية؛ التكامل؛ التوافر). ويشتمل الجدول (٣) على نموذج لذلك:

الجدول (٣)

| نوع الأصل | اسم الأصل | السرية<br>س<br>عالية = ٣<br>متوسطة =٢<br>عادية = ١ | التكامل<br>ت<br>عالية = ٣<br>متوسطة = ٢<br>عادية = ١ | التوفر<br>و<br>عالي = ٣<br>متوسط = ٢<br>عادي = ١ | قيمة الأصل<br>س × ت × و |
|---|---|---|---|---|---|
| أجهزة وعتاد حاسب آلي | المفتاح الأساسي | ٢ | ١ | ٣ | ٦ |
| معلومات | السجلات الشخصية | ٣ | ٣ | ٣ | ٢٧ |

### ٢. تحديد التهديدات والثغرات الأمنية

يجب تحديد التهديدات والثغرات الأمنية لكل نوع من أنواع الأصول أثناء عملية تحديد الأصول، ويشكل ذلك أساساً لتحليل المخاطر.

التهديد هو حادثة محتملة من البيئة الخارجية، ويمكن أن تلحق الضرر بالأصول مثل المعلومات، والعمليات، والأنظمة، والموظفين، مما يؤدي بالتالي إلى إلحاق الضرر بالمؤسسة. يمكن تحديد مصادر التهديدات من خلال التشاور مع المسئولين من أقسام الأصول، والمرافق، والشئون الإدارية، والمختصين الأمنيين، والجماعات المختصة، إلخ.

تكون مصادر التهديدات أساساً خارجية، ويمكن وضعها ضمن مجموعات حسب الأنواع التالية:

| مصادر التهديدات | أمثلة |
|---|---|
| بشرية | القراصنة (الهاكرز والمتسللين) الخارجيين |
| فنية | فشل الوصلات من مزود خدمات الاتصالات |
| بيئية | الحريق، الأوبئة |

بعد تحديد الأصول والمخاطر، يتوجب على مدير المشروع تحديد الثغرات الأمنية التي يمكن أن تستغلها تلك التهديدات. وتعرف الثغرات الأمنية بأنها نقاط الضعف الحالية في المؤسسة، ويمكن تحديدها في المجالات التالية:

- الموظفين.
- السياسات التنظيمية.
- السياسات والإجراءات.
- البيئة المادية.
- أنظمة المعلومات.
- البرامج.
- مقدمي الخدمات الخارجيين.

وقد تم تضمين نماذج من التهديدات والثغرات الأمنية في الملحق (ج). وتجدر ملاحظة أن القائمة المدرجة في ذلك الملحق لا تشمل جميع التهديدات والثغرات الأمنية، وينبغي على الجهة تطوير هذا الجدول وتعديله بما يتوافق مع متطلباتها.

### ٣. تصنيف المخاطر

عندما يتم تحديد المخاطر التي تنطوي عليها السيناريوهات المختلفة وفئات الأصول الرئيسية لدى المؤسسة، فإنه يتم تصنيف تلك المخاطر بناء على التالي:

- أثر التهديد على المؤسسة.
- احتمالية أو إمكانية حدوث التهديد.

أثر التهديد واحتمالات حدوثه سيحدد جوانب تنفيذ إطار تطوير سياسات وإجراءات أمن المعلومات التي ينبغي على الإدارة أن تركز جهودها فيها.

تشارك الأطراف المعنية الرئيسية في تحديد أثر واحتمال وقوع المخاطر الرئيسية المحددة لدى المؤسسة. وبعد ذلك يتم تجميع القيم التراكمية لتقييم المخاطر لتحديد التصنيف الكلي للمخاطر (عالية، متوسطة، عادية). وقد تم تضمين نموذج تصنيف المخاطر ونماذج من ذلك في الملحق (٤) للرجوع إليها.

### ٤. التصنيف الكلي للمخاطر لدى الجهة

إضافة إلى تقييم المخاطر الفردية التفصيلية المذكورة في الخطوة السابقة، فعلى الإدارة أن تقوم كذلك بالتعرف على وفهم مجموعة المخاطر الكلية التي تتعرض لها الجهة. ويجب الأخذ في الاعتبار العوامل الكمية والنوعية.

- العوامل الكمية:

يجب أن تقوم الإدارة بتجميع التقييم الكلي للمخاطر التي تتعرض لها الجهة للحصول على معدل عام لتقييم جميع المخاطر الفردية كجزء من عملية تقييم المخاطر. وفي العادة يعتبر معدل تقييم بسيط للمخاطر كافيا، غير أن الإدارة قد تقرر إعطاء أوزان إضافية لمجالات محددة من المخاطر ومن ثم تحسب المعدل الموزون.

- العوامل النوعية الواجب أخذها في الاعتبار:

تقوم الإدارة كذلك بتدقيق مزدوج والتحقق من تصنيفات المخاطر المذكورة أعلاه بما يتوافق مع الاعتبارات الأخرى المتعلقة بطبيعة الجهة وجوانب عملياتها ضمن الإطار العام للحكومة السعودية والاقتصاد الوطني. وبالتالي، فقد يكون مطلوباً من إدارة الجهة الحكومية زيادة تصنيف المخاطر إلى المستوى الأعلى أو المتوسط، إذا لزم الأمر.

- أهمية الجهة للحكومية: يتم الحصول على الإرشادات من الوزارة المعنية.
- أهميتها للاقتصاد والأمن الوطني: سيعتمد ذلك على القطاعات الاقتصادية.

- الأمن الوطني:
  - الأمن الوطني.
  - الشئون الأمنية.
- الخدمات المدينة والعامة:
  - الخدمات المدنية والعامة.
  - التعليم.
- الشئون المالية والاقتصاد الوطني.
- الشئون الصحية.
- القطاع التجاري وغيره:
  - التجاري والصناعي.
  - الاتصالات والتقنية.
  - النفط والغاز والمعادن.
  - النقل.
  - غير ذلك.
- مستوى التفاعل مع الجمهور والخدمات المقدمة من الجهة الحكومية.

### ٥. تقييم المخاطر والتقارير

بعد اكتمال عملية تقييم المخاطر، يتوجب على مدير المشروع إعداد تقرير تقييم المخاطر ورفعه إلى لجنة توجيه أمن المعلومات. ويجب أن يشتمل التقرير ملخصاً عاماً للمخاطر التي تواجهها المؤسسة، إضافة إلى التفاصيل التالية:

- التهديدات.
- الثغرات الأمنية.
- اسم الأصل.
- قيمة الأصل،
- بيان المخاطر.
- أثر التهديدات.
- الاحتمالات.
- تصنيف المخاطر المتأصلة.

## ٤.٥. آليات تطوير السياسات والإجراءات

يتطلب هذا الإطار من الجهة الالتزام الكامل بمتطلبات أمن المعلومات التي تفرضها الحكومة السعودية.

### ٤.٥.١. عوامل إتخاذ القرارات

في إطار الالتزام المتواصل بالمتطلبات الملزمة، فإنه يمكن لـ (اسم الجهة) اختيار القيام بتطوير وتحديث سياسات وإجراءات أمن المعلومات الخاصة بها بنفسها، أو تبني السياسات والإجراءات المقدمة من هذا الإطار مع إجراء تعديلات عليها حسب احتياجاتها.

وستأخذ الإدارة في اعتبارها العوامل التالية قبل اتخاذ قرارها بشأن الآليات التي ستستخدم بصرف النظر عن طريقة التطوير التي اختارتها:

١. حجم إدارة أمن المعلومات الحالية.
٢. توفر المهارات والخبرات الداخلية.
٣. الفهم الأولي للتكاليف استناداً إلى عدة عوامل مثل درجة التعقيد، التنوع، التفرد، وحجم العمليات لدى تلك الجهة.
٤. القيود الزمنية اعتماداً على المواعيد المتاحة.

بناءً على أحكام الإدارة المتعلقة بالعوامل المذكورة أعلاه، فسيتم تبني أحد المنهجيين من قبل الإدارة العليا (إما التطوير الذاتي، أو التعديل حسب المتطلبات). وسيرد أدناه التوجيهات المتعلقة بكلا المنهجين:

كما أن الإدارة قد تختار منهجية متخلفة، من خلال تطبيق التطوير الذاتي على بعض مجالات السياسات المختارة، فيما تختار طريقة التعديل حسب الحاجة لمجالات السياسات المتبقية بهدف تقنين التكاليف وخفض الوقت الذي تستغرقه هذه العملية.

### ٤.٥.٢. تعديل سياسات وإجراءات أمن المعلومات المقدمة حسب الحاجة

من المتعارف عليه أن الكثير من الجهات الحكومية قد تواجه مواعيد صارمة من قبل الحكومة، أو قد لا يكون لديها الموارد والمهارات المطلوبة للقيام بعملية التطوير الذاتي. وبالتالي، فقد تم تطوير مجموعة كاملة من السياسات والإجراءات وتقديمها مع إطار التطوير هذا لاستخدامها من قبل إدارة (اسم الجهة) لدعمها وتمكينها من الالتزام بهذه المتطلبات.

يمكن لـ (اسم الجهة) إعداد سياساتها وإجراءاتها خلال فترة زمنية قصيرة من خلال تعديل السياسات والإجراءات المقدمة مع إطار التطوير هذا (والتي يمكن أن تعتبر كذلك بمثابة مستودع الحد الأدنى الأساسي للسياسات والإجراءات). ولهذا الغرض، سيتم تكليف مسئول أمن المعلومات بالمسئولية الأساسية عن

تطوير سياسات وإجراءات أمن المعلومات حسب احتياجات الجهة المعنية. ويجب أن يتمتع مسئول أمن المعلومات بالمهارات التالية:

- المعرفة الغزيرة بأمن المعلومات.
- المعرفة الغزيرة بالجهة الحكومية.
- خبرات سابقة في كتابة سياسات وإجراءات أمن المعلومات.
- مهارات الكتابة الفنية.

إضافة لذلك، يمكن الحصول على دعم إضافي لمدة قصيرة من الإدارات الأخرى أو من أطراف خارجية على أساس الحاجة الماسة لذلك.

## ٤. ٥. ٣. التطوير الذاتي لسياسات وإجراءات أمن المعلومات

اعتماداً على العوامل الموصوفة أعلاه، فقد تقرر إدارة (اسم الجهة) تأسيس السياسات والإجراءات الخاصة بها باتباع طريقة التطوير الذاتي. ويمكن أن تقوم بذلك من خلال تعيين خبير في أمن المعلومات لدى الشركة، أو يمكن الحصول على المساعدة من طرف خارجي.

يجب تطوير السياسات بناءً على معايير متنوعة، تشمل -دون حصر- ما يلي:

- معايير معالجة أمن المعلومات الفدرالية الأمريكية (FIPS PUB 200) - الحد الأدنى من المتطلبات الأمنية للمعلومات الفدرالية وأنظمة المعلومات.
- المعهد الوطني الأمريكي للمعايير والتقنية (NIST PUB 800-53) - ضوابط أمن المعلومات الموصى بها لأنظمة المعلومات الفدرالية.
- ألمانيا - دليل الحماية الأساسية لدى المكتب الفدرالي لأمن المعلومات.
- المواصفات القياسية العالمية لأمن المعلومات (ISO/IEC 27001).
- الأنظمة السعودية:
  - نظام التعاملات الإلكترونية.
  - نظام مكافحة جرائم المعلوماتية.

على إدارة (اسم الجهة) أن تتأكد من الالتزام الكامل بالمتطلبات الرسمية لأمن المعلومات. وبالتالي فإن عليها تغطية جميع جوانب السياسات الأساسية وعددها (٢٩) الواردة ضمن وثيقة السياسات المقدمة مع إطار التطوير هذا. غير أنه يمكن للإدارة أن تغتنم هذه الفرصة لتعزيز و/أو إضافة مجالات أخرى لتغطيتها إذا استدعت ذلك أية عمليات فريدة تقوم بها الجهة في أي مجال من مجالات السياسات.

### ١. التطوير الذاتي من قبل موظفي الجهة نفسها

الخيار الأول لتطوير السياسة يجب أن يكون التطوير الداخلي من قبل موظفي المؤسسة. ويجب أن يتمتع خبراء أمن المعلومات الذين يكلفون بهذه المسئولية بالمهارات والكفاءات التالية:

- شهادات أمن المعلومات.
- المعرفة الغزيرة بأمن المعلومات.
- المعرفة الغزيرة بالجهة الحكومية.
- خبرات سابقة في كتابة سياسات وإجراءات أمن المعلومات.
- مهارات الكتابة الفنية.
- مهارات كتبة سياسات وإجراءات أمن المعلومات.

في حال عدم توفر معظم المتطلبات المذكورة أعلاه ضمن الموارد الداخلية الحالية، فينبغي على الإدارة النظر في توظيف موارد إضافية.

### ٢. التطوير بمساعدة مقاولين من خارج الجهة الحكومية

في حال إشراك مقاول خارجي في تطوير السياسات والإجراءات، ينبغي على الوزارة التأكد من توفر الخبرات والكفاءات المناسبة لدى هذا الطرف الخارجي ووجود الموارد الداخلية المناسبة لديه، إضافة لذلك، فإن صلاحية المراجعة النهائية واعتماد السياسات والمعايير والإجراءات التي يطورها ذلك الطرف الخارجي، يجب أن تكون لدى مدير أمن المعلومات والإدارة العليا لدى (اسم الجهة).

وتنطبق الآليات المذكورة أعلاه على كل مجال من مجالات السياسات الواقعة ضمن السياسات والإجراءات التي تم تطويرها.

## ٦.٤. عملية تطوير السياسات العامة لأمن المعلومات

بناءً على التقييم الذاتي، وتقييم المخاطر المذكورة آنفاً، فسيكون فريق المشروع قادراً على تحديد السياسات التي تحتاج إلى التطوير.

وعند تحديد مجالات السياسات بوضوح، يكون فريق المشروع مسئولاً عن تصميم هيكل للسياسة وتوثيق المعلومات اللازمة تبعاً لذلك، ويمكن استخدام هيكل السياسة التالي كأساس لوضع سياسات أمن المعلومات العامة.

- **اسم السياسة:** اسم مجال السياسة.
- **الغرض من السياسة:** وصف موجز للغرض من السياسة.
- **مجال تطبيق السياسة:** تحديد الإدارات والجهات المختلفة الداخلية والخارجية وكذلك الأشخاص الذين تنطبق عليهم هذه السياسة.
- **المسئول التنفيذي:** تحديد الشخص الذي يضطلع بالصلاحية والمسئولية النهائية عن أي تغييرات أو تحديثات تجري على السياسة. يجب اعتماد أي تغييرات أو تحديثات على السياسة من قبل المسئول التنفيذي عن السياسة.
- **راعي وثيقة السياسة:** الشخص المسئول عن إبقاء وحفظ السياسة وتبليغها وتحديثها بناءً على توجيهات المسئول التنفيذي عن السياسة.
- **إلزامية التنفيذ:** تحدد تبعات ونتائج أية مخالفة لهذه السياسة.
- **قيود سياسة أمن المعلومات:** يشتمل هذا القسم وصف لجزئية القيود/الضوابط المتعلقة بالسياسة المحددة.
- **تاريخ نفاذ السياسة:** يحدد هذا القسم التاريخ الذي يسري فيه تطبيق السياسة، ومنه يجب إتباعها.

**مثال:**

*اسم السياسة: سياسة أمن معلومات الجهة*

*الغرض: الغرض من هذه السياسة هو تبليغ التزام الإدارة وعرض الأهداف الرئيسية لتأسيس ضوابط لأمن المعلومات مبنية على المخاطر التي قد تتعرض لها (اسم الجهة).*

*مجال تطبيق السياسة: تنطبق هذه السياسة على جميع الموظفين، والموردين، وشركاء العمل، وموظفي المقاولين، الأقسام الإدارية لدى (اسم الجهة) سواء كانوا يعملون بصفة دائمة أو مؤقتة، وبصرف النظر عن مواقع عملهم*

*المسئول التنفيذي: مدير أمن المعلومات*

*راعي وثيقة السياسة: مدير تقنية المعلومات*

*إلزامية التنفيذ: في حالة مخالفة أي موظف أو طرف ثالث*

*(موردين، مقاولين، شركاء عمل، إلخ) لهذه السياسة، فسيتعرض لإجـراءات نظامية وفقاً لسياسات الجهـة، وأنظمة ولوائح المملكة العربيـة السعوديـة، والتـي تشمـل- دون حصـر - نظـام العمـل والعمال، ونظـام مكافحة جرائـم المعلوماتية، ونظـام التعاملات الإلكترونية، إلخ...*

*قيود سياسة أمن المعلومات.*

*الأهـداف الرئيسية لأمن المعلومات لـدى الجهة: يجب أن يقتصر استخـدام أنظمـة المعلومـات لدى (اسـم الجهة) علـى أغراض العمـل المصرح بها فقط، وعلى موظفين محدوديـن وفقاً لسياسة الاستخدام المقبول لأنظمة المعلومات.*

سيكون على فريق المشروع متابعـة عملية التحكم بالوثيقة حسبما ورد في الملحق (٣) أثناء إنشاء السياسات.

## ٤.٧. عمليـة تطوير سياسـات أمـن المعلومات المتعلقة بأنظمة معلومات محددة

بنـاءً علـى التقييـم الذاتـي وتقييـم المخاطـر، فسيتـم تحديـد وتصنيف أصـول المعلومات، وسيتم تعيين تقييم مخاطر لكل أصل من الأصول.

وبنـاءً علـى مجـالات السياسات المحـددة في السياسـات العامة، سيكـون فريق المشـروع مسئولاً عـن إعداد هيكل المعايـير وإكمال المعلومـات تبعاً لذلك. ويمكـن استخدام هيـكل السياسات التالي المتعلقـة بأنظمـة محددة كمثـال على إعـداد السياسـات المتعلقة بأنظمة أمنية محددة.

- **مجـال السياسـة:** يصف هـذا القسم مجـال السياسة التي تنتمي إليها السياسة المتعلقة بالأنظمة.
- **مجـال السياسـة المتعلقة بالأنظمة:** ويشـير ذلك إلى الفئة التي تقع تحتها السياسة المتعلقة بالأنظمة.
- **بنـود المعيـار التفصيليـة:** يصـف هذا القسم بنـود التحكم بالمعيار المحدد.
- **مجـال التطبيـق:** يحـدد هـذا القسـم تصنيـف المخاطـر (السرية، التكامل، التوفر) للجهة التي ستطبق هذا المعيار.
- **أنظمـة تقنيـة المعلومات المحددة:** يحدد هـذا القسم أنظمة تقنية المعلومات التي ينطبق عليها المعيار.
- **رقم المعيار:** ويشير إلى الرقم المرجعي لبنود المعيار.

**مثال:**

- **مجال السياسة** – التوعية بأمن المعلومات
- **مجـال السياسة المتعلقة بالأنظمـة** – جلسات التوعية بأمن المعلومات
- **بنود السياسة التفصيلية:**

١. يجب أن تركز البرامج التوعوية على المستويات الأمنية.

٢. يجب عقد البرامج دورياً على الأقل لمرة واحدة كل ٦ أشهر.

٣. يجب قياس فاعلية البرنامج وتصحيحها وتحسينها بشكل مناسب مع مرور الوقت.

٤. يجب أن يخضع جميع الموظفين الجدد إلى تدريب أمني توعوي كجزء من عملية تأهيلهم للوظيفة.

٥. يجب أن تستخدم برامج التوعية عدة طرق كالبريد الإلكتروني، والملصقات، والفيديو، أو التدريب في غرف التدريس.

- **مجالات التطبيق:** الجهات ذات المخاطر المرتفعة والمتوسطة والعادية.

سيكون على فريق المشروع متابعـة عملية التحكم بالوثيقة حسبما ورد في الملحق (٣) أثناء إنشاء السياسات.

## ٨.٤. مراجعة واعتماد سياسات أمن المعلومات

بعد اكتمال إعداد السياسات العامة لأمن المعلومات والسياسات المتعلقة بأنظمة محددة، يجب رفع الوثائق إلى لجنة التوجيه للمراجعة والاعتماد، ويتم أخذ مرئيات جميع الأطراف ذات العلاقة للتحقق من قبول السياسات التي تم إعدادها. وتقوم لجنة التوجيه بقبول أو رفض تلك السياسات. ويتم إخضاع السياسات المرفوضة إلى التغيير وفقاً لملاحظات اللجنة.

## ٩.٤. عملية إعداد إجراءات أمن المعلومات

عند استلام الموافقة على سياسات ومعايير أمن المعلومات، يكون فريق المشروع مسئولاً عن إعداد الإجراءات لجميع السياسات والمعايير المعلقة بالسياسات المعتمدة. ويخضع إعداد الإجراءات كذلك إلى الإجراءات الحالية المتبعة من قبل إدارة تقنية المعلومات أو سياسات وإجراءات الموارد البشرية.

يمكن استخدام الإجراء التالي كمثال لإعداد إجراءات أمن المعلومات:

- **الهدف:** يذكر هذا القسم الهدف من الإجراء المتعلق بأمن المعلومات.
- **مرجعية السياسة:** يحدد هذا القسم السياسة المعنية بالإجراء المحدد.
- **الإجراء:** يقوم هذا القسم بإدراج ووصف الأنشطة المنهجية التي سيتم اتباعها بموجب الإجراء. ويجب أن يتم دائماً وصف هذه الأنشطة من حيث الإجراءات المحددة من قبل الأطراف المحددة. وبعض هذه الأنشطة ستكون ذات قيمة مضافة، وتحتاج للمراجعة والاعتماد، فيما ستكون الأنشطة الأخرى إدارية، ويتعين إضافتها لإكمال سير العملية.
- **النموذج ذي العلاقة:** يحدد هذا القسم أسماء النماذج ذات العلاقة، إن وجدت، التي يشتمل عليها الإجراء.

**مثال:**

- **إدارة الوصول المنطقي:** تهدف إجراءات إدارة الوصول المنطقي إلى إدارة دخول المستخدمين إلى أنظمة المعلومات لدى (اسم الجهة).
- **إجراء استحداث ملف الوصول بجماعة من المستخدمين.**
- **الهدف:** يوضح هذا الإجراء الأنشطة الرئيسية لإنشاء ملف الوصول الخاص بجماعة من المستخدمين إلى أنظمة المعلومات. وتكون ملفات المستخدمين مصحوبة بمجموعة من الصلاحيات المتفق عليها ومسبقة التحديد التي تعتبر مناسبة لجماعة محددة من مستخدمي نظام المعلومات.
- **السياسة المرجعية:** سياسة إدارة الوصول المنطقي.
- **الإجراء:** عند الإعداد الأولي لنظام ما، يكون مدير تقنية المعلومات مع المسئول عن نظام المعلومات مسئولين عن تحديد وتنفيذ ملفات جماعة المستخدمين قبل أن يوضع النظام في بيئة الإنتاج. أما بالنسبة للنظام الموضوع فعلياً في بيئة الإنتاج، فإن موظفي التطوير/ الإعداد المعنيين مع المسئول عن نظام المعلومات يتكفلون بهذه المسئولية.

يقوم موظف تقنية المعلومات المعني (المذكور أعلاه) بالتنسيق مع المسئول عن نظام المعلومات لتحديد ما يلي:

- الجماعة المحتملة من المستخدمين الذين يستخدموا النظام.
- نوع الوصول الذي يحتاجه هؤلاء المستخدمين لأداء المهام المكلفين بها.

## ٤.١٠. مراجعة واعتماد إجراءات أمن المعلومات

بعد اكتمال إعداد إجراءات أمن المعلومات، يجب رفع الوثائق إلى لجنة التوجيه للمراجعة والاعتماد، ويتم أخذ مرئيات جميع الأطراف ذات العلاقة للتأكد من قبول السياسات وجدوى الإجراءات التي تم إعدادها. وتقوم لجنة التوجيه بقبول أو رفض تلك الإجراءات. ويتم إخضاع الإجراءات المرفوضة إلى التغيير وفقاً لملاحظات اللجنة.

## ٤.١١. إدارة المشروع

### ٤.١١.١. الهدف

تهدف هذه العملية لما يلي:

- الإدارة والإشراف على تطوير سياسات وإجراءات أمن المعلومات.
- رفع التقارير عن حالة تطوير سياسات وإجراءات أمن المعلومات إلى لجنة التوجيه.

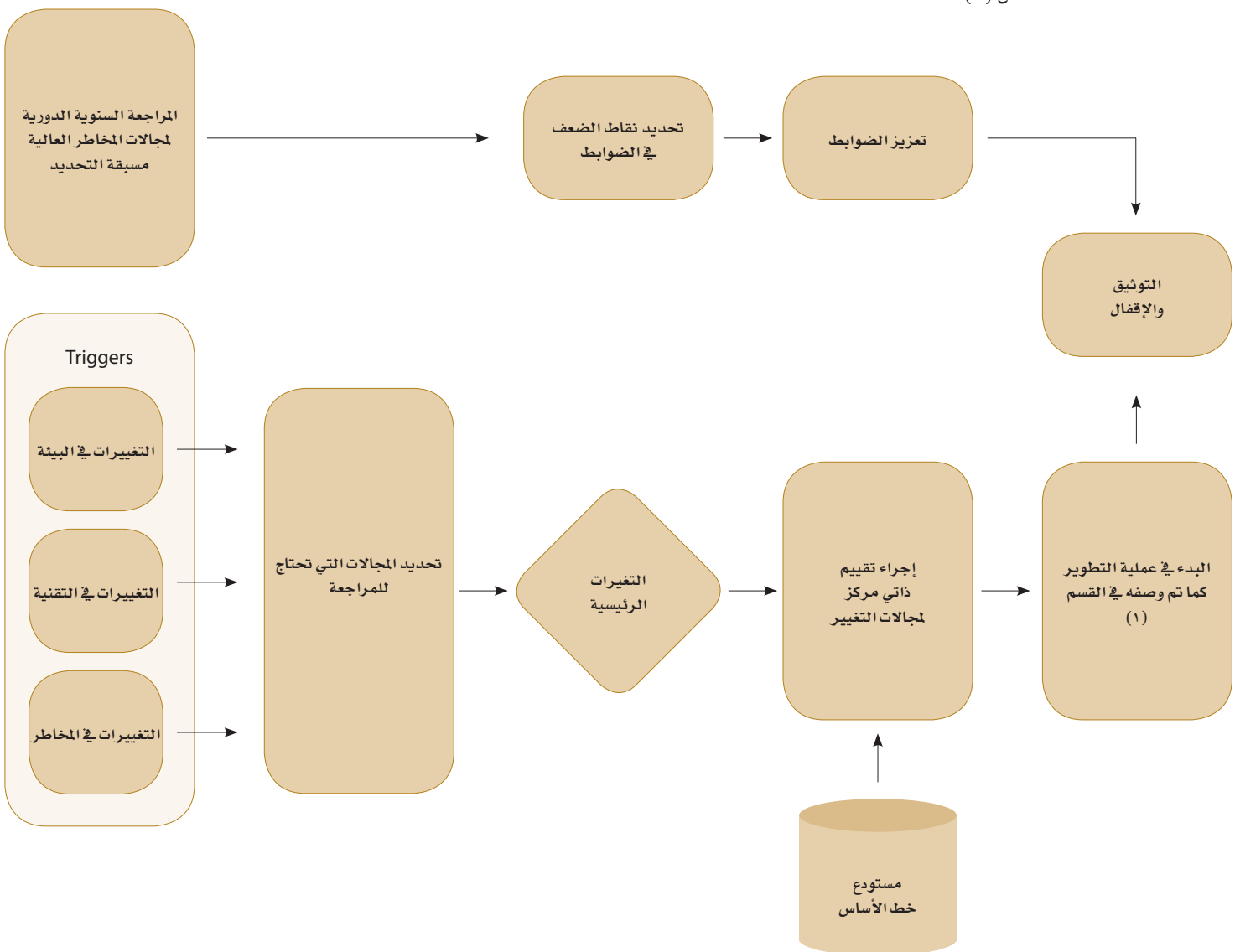
### ٤.١١.٢. إدارة المشروع

طوال مراحل تطوير سياسات وإجراءات أمن المعلومات، يجب على فريق المشروع الحفاظ بشكل مستمر على إدارة قوية وفاعلة للمشروع، ويجب على كل إدارة (جهة حكومية) أن تطبق إجراءات تأكيد الجودة للتأكد من تلبية متطلبات أمن المعلومات، وتفادي تأخر المشروع وتجاوزه لمدته المقررة.

وينبغي على مدير مشروع مراقبة تطوير سياسات وإجراءات أمن المعلومات، وأن يواظب على استمرارية تقديم تقارير الحالة باستخدام نموذج تقرير حالة المشروع الوارد في الملحق (٢) القسم ٣-٥، إلى لجنة التوجيه.

## ٤. ١٢. المراجعة السنوية لسياسات وإجراءات أمن المعلومات

الشكل (٦)



### ٤.١٢.١. المراجعة الدورية

يتعين على (اسم الجهة) إجراء مراجعات دورية على المجالات ذات المخاطر العالية المحددة مسبقاً في السياسيات والمعايير والإجراءات، ويجب الإبقاء على وجود فصل في المهام والواجبات أثناء المراجعات؛ بمعنى أن الموظفين المشاركين أثناء عملية التطوير يجب ألا يشاركوا في مراجعة السياسات والإجراءات.

استناداً إلى تصنيف مخاطر أصول المعلومات لدى (اسم الجهة)، يقوم فريق المراجعة باختيار المجالات عالية المخاطر، وإجراء مراجعات على السياسات والمعايير والإجراءات الفاعلة تبعاً لذلك، ويتم تعديل أو تحسين الضوابط المتعلقة بنقاط الضعف التي تم تحديدها أثناء عملية المراجعة.

### ٤.١٢.٢. تحديد المجالات التي تحتاج للمراجعة

تنشأ الحاجة إلى مراجعة السياسات والإجراءات من وجود تغييرات ملحة ومستمرة على بيئة وتقنيات ومخاطر العمل. والتغييرات التي تطرأ مع مرور الوقت تسبب انعدام كفاءة وفاعلية السياسات والإجراءات، مما يسبب زيادة في مجالات المخاطر. وتكون لجنة التوجيه مسئولة عن إعداد عملية مراجعة سنوية لسياسات وإجراءات أمن المعلومات.

قد تكون التغييرات التي تطرأ طفيفة أو رئيسية أو كبيرة، وبناءً على تصنيف التغيير، يمكن أن تكون عملية المراجعة تفصيلية أو مختصرة، ويتوجب على لجنة التوجيه تشكيل فريق مراجعة للقيام بما يلي:

- تحديد وتصنيف التغييرات في البيئة.
  - الحجم.
  - الفروع.
  - الخدمات.
  - الموظفين.
  - الموقع المادي.
  - القوانين والأنظمة الحكومية.
- تحديد وتصنيف التغييرات في التقنية.
  - تطبيقات تقنية المعلومات.
  - أنظمة تقنية المعلومات.
  - الشبكات.
  - البنية التحتية المادية.

#### ٤.١٢.٢.١. عملية التغييرات الرئيسية الهامة

في حال استدعت الحاجة لإجراء تغييرات هامة في البيئة، تقوم لجنة التوجيه بتوجيه إدارة أمن المعلومات بإجراء تقييم ذاتي مركز يغطي مجال التغيير.

**١. التقييم الذاتي المركز (المكثف)**

يجب إجراء التقييم الذاتي المركز طبقاً للإرشادات المذكورة في القسم (ب)، الذي يتضح من عنوانه أن هذا التقييم الذاتي سيقتصر على المجالات المحددة لإجراء التغييرات الرئيسية عليها. ويتم من خلال التقييم الذاتي تحديد الفجوة بين السياسات والمعايير والإجراءات، مقارنة بالحد الأدنى المطلوب من السياسات والإجراء والمعايير.

**٢. البدء في عملية التطوير**

بعـد تحديـد الفجـوة، تقوم لجنة التوجيه إمـا بتحديد مجموعة مـن المشاريع أو مشروعاً واحـداً. وستعتمد المشاريع علـى حجم التغييرات المحددة من قبل فريق المراجعة. وتقوم لجنة التوجيه بتعيين مدير للمشروع يكون مسئولاً عن عملية التطوير التالية، الموضحة في القسم (أ).

### ٤. ١٢. ٢. ٢. عملية التغييرات الطفيفة

عنـد تحديـد تغييرات طفيفة، تقوم لجنـة التوجيه بتفويض فريق المراجعة بتحديد نقاط الضعـف في الضوابط المطبقة من خلال سياسات الإجراءات الحالية.

**١. تحديد نقاط الضعف في الضوابط**

يُطلـب مـن فريق المراجعـة تقييم الفاعلية الحالية للضوابط المستخدمـة، مما يعني قيام فريق المراجعة بإجـراء عينة من الاختبارات على السياسـات والمعايير والإجراءات. وعلـى الفريق المذكور أن يفهم أولاً السياسة والمعايير والإجراءات المتعلقة بهذه الضوابط. بعد ذلك يأخذ حالة مخالفة للسياسات المبلغ عنها سابقاً ويحدد الجوانب التي تم الإخفاق في تخفيف المخاطر المتعلقة بها. ومن ثم ينتج تقرير يرفع للجنة التوجيه للمراجعة والاعتماد.

**٢. تعزيز الضوابط**

تحتاج الجوانب المحددة التي أخفقت فيها تدابير التخفيف الى تحسين الضوابط الحالية، مما قد يستدعي إنشاء بنود إجراءات جديدة، أو إضافة خطوات أخرى لإجراء المهام المختلفة المتعلقة بتخفيف المخاطر.

## ٤. ١٢. ٣. التوثيق وإغلاق الحالة

يتم توثيق جميع نتائج المراجعة وعرضها على لجنة التوجيه للمراجعة النهائية والاعتماد.

الجزء الثالث

# دليل تنفيذ السياسات والإجراءات

# ١. مقدمة

## ١.١. الغرض

تقدم هذه الوثيقة الإرشادات المتعلقة بتنفيذ سياسات وإجراءات أمن المعلومات لدى (اسم الجهة). وتقدم هذه الوثيقة كذلك النماذج اليدوية والإلكترونية ذات العلاقة لدعم هذا التنفيذ.

إن تنفيذ وتسليم سياسات وإجراءات أمن المعلومات لهو من المسئوليات الرئيسية للجهات الحكومية، وينصب التركيز على التنفيذ السليم لسياسات أمن المعلومات واستمرارية تسليمها ضمن الوقت المقرر وفي حدود الميزانيات، وبمستوى مقبول من الجودة.

ويتم إصدار إطار تطوير سياسات وإجراءات أمن المعلومات إلى الإدارة العليا لكل جهة حكومية في إطار زمني محدد، ومن بعد تقديم الإطار تصبح الإدارة العليا مسئولة عن التأكد من اتباع برامج تنفيذ ملائمة بما يكفل التنفيذ الناجح. **ومن المهم ملاحظة أن القصد من هذا الدليل مساعدة الجهات الحكومية على تنفيذ السياسات والإجراءات المعتمدة، الناشئة عن عملية التطوير والتي يجب إكمالها قبل البدء في أنشطة التنفيذ.**

إن تنفيذ سياسات وإجراءات أمن المعلومات سيسهل من تبني نظام إدارة أمن المعلومات متكامل. وقد تم تصميم برنامج التنفيذ هذا ليدعم (اسم الجهة) في تنفيذ ونشر سياسات وإجراءات أمن المعلومات على مراحل بما يتوافق مع أولويات الإدارة.

ويجري التركيز في دليل التنفيذ هذا على المبادئ العامة التي تساعد على تنفيذ الفاعل، معولاً على الخبرات الحالية للجهات الحكومية، وعلى الممارسات الريادية المتبعة في إدارة المشاريع/ البرامج وأمن المعلومات.

## ١.٢. المسئول عن البرنامج

يكون المسئول التنفيذي الأعلى لدى (اسم الجهة) (الوزير/ المحافظ / نائب الوزير/المحافظ / المدير العام، إلخ) هو المسئول عن برنامج أمن المعلومات، ويضطلع بالصلاحية والمسئولية عن تنفيذ سياسات وإجراءات أمن المعلومات بما يتوافق مع الإرشادات المقدمة لهذا الغرض.

# ٢. موقع إدارة أمن المعلومات ضمن الهيكل التنظيمي

يقوم المسئول التنفيذي الأعلى لدى الجهة بتأسيس وظيفة أمن المعلومات وفقاً لوثيقة خيارات موقع إدارة أمن المعلومات في الهيكل التنظيمي، المقدمة في وثيقة منفصلة. ويجب أن يوضح الهيكل التنظيمي علاقة إدارة أمن المعلومات مع المناصب الرئيسية الأخرى ذات العلاقة في المؤسسة. وسيتم تحديد هذه العلاقة في سياق الجوانب التالية:

- علاقات التقارير (التبعية الإداريه) التي تغطي جميع جوانب الالتزام بأمن المعلومات.
- العلاقة الإدارية التي تغطي الأمور المتعلقة بالشئون الإدارية والميزانية لإدارة أمن المعلومات.

تأسيس إدارة أمن المعلومات هو متطلب سابق لإعداد برنامج التنفيذ. وسيتم تعيين مدير أمن المعلومات للقيام بدور مدير برنامج التنفيذ، فيما سيتم تحديد المزيد من الأدوار والمسئوليات في القسم ١,٥.

## ٣. التعليمات المفروضة على برنامج التنفيذ

عند استلام إطار أمن المعلومات، يجب التأكد من اكتمال جميع الوثائق المستلمة وفقاً للملحق ٨,١.

وسيكون على المسئول عن البرنامج إصدار التعليمات المفروضة على جميع الأطراف ضمن الجهة حيث يطلب منهم تنفيذ سياسات وإجراءات أمن المعلومات المعتمدة؛ وذلك بناء على الإطار الزمني الذي تحدده الحكومة السعودية.

## ٤. إعداد برنامج التنفيذ

بعد إصدار تعليمات التنفيذ، يتعين على المسئول عن البرنامج إعداد الهيكليات الأساسية لبرنامج تنفيذ أمن المعلومات. ويجب أخذ الجوانب الرئيسية التالية في الاعتبار.

### ٤.١. إتباع منهجية تحليلية

ينصح باستخدام منهجية تحليلية لتنفيذ سياسات وإجراءات أمن المعلومات، مما يضمن إمكانية تنفيذ برنامج العمل من خلال إعدادات موضوعية واضحة، بناءً على هدف خطة العمل لدى (اسم الجهة)، بحيث تبدأ المنهجية من الإدارة العليا مروراً بالإدارة المتوسطة، ومن ثم أعضاء الموظفين لدى (اسم الجهة)، وستكون (اسم الجهة) مسئولة عن المستويات المختلفة لتنفيذ البرنامج.

### ٤.٢. تحديد الأطراف ذات العلاقة

يجب تحديد جميع الأطراف التي من المرجح أن تتأثر من التنفيذ. ويمكن القيام بذلك من خلال إعداد ورشة عمل تضم ممثلين عن الإدارة العليا والوظائف / الإدارات الرئيسية. ويمكن تعريف مصطلح "أصحاب المصلحة" أو «الطرف ذي العلاقة» أو «الأطراف المعنية» على أنه «أي شخص يتأثر من تنفيذ سياسات وإجراءات أمن المعلومات». وكل طرف معني وله مساهمة ضرورية، ولديه توقعات مناسبة من أجل تحقيقها.

تقوم (اسم الجهة) بتحديد المسئولين عن أصول المعلومات لكل نظام من أنظمة المعلومات التي تشغلها تلك الجهة، بحيث يكون هؤلاء من كبار الموظفين لدى(اسم الجهة) المالكة للنظام. وسيكون هؤلاء مسئولين عن البيانات الخاصة بأنظمة المعلومات تلك التي تعمل ضمن مجالات عملهم،.وسيكونون مسئولين عن الحماية اليومية لأنظمة المعلومات التابعة لهم وعن تأكيد جودة المعلومات في تلك الأصول. كما يتأكد كل مسئول عن أصل معلوماتي من أن متطلبات المؤسسة المتعلقة بتحديد والتبليغ عن وإدارة والاستجابة لحوادث المعلومات تنطبق على أصول المعلومات التي يكون مسئولاً عنها. ويتضمن ذلك آليات تحديد والتخفيف من حدة الحوادث والنقاط التي قد يحتاجون فيها للمساعدة أو إلى تصعيدها.

### ٤.٣. تأسيس لجنة التوجيه

يقوم المسئول عن البرنامج بتأسيس لجنة توجيه تتكون من ممثلين مناسبين مع عناصر الإدارة العليا والأطراف المعنية. وتكون للجنة التوجيه الصلاحية في حل المشاكل والمسائل المتعلقة بالتنفيذ، واتخاذ القرارات حول التغييرات المطلوبة. وستقوم لجنة التوجيه بتحديد أولويات التنفيذ طبقاً لإرشادات هيئة الاتصالات وتقنية المعلومات آخذة في الاعتبار العديد من العوامل مثل المخاطر وتوفر الموارد وغير ذلك.

### ٤.٤. تعيين مدير للبرنامج

تتولى لجنة التوجيه تعيين مدير للبرنامج يتمتع بالخبرات المناسبة، ولديه القدرة على إدارة تنفيذ البرنامج بكفاءة وفاعلية. ويكون مدير البرنامج مسئولا عن جميع مراحل تنفيذ السياسات والإجراءات، ويتبع مباشرة إلى لجنة التوجيه. وفي حال وجود أي تعارض، فيجوز له طلب المشورة من لجنة التوجيه. ويجب أن يكون مدير البرنامج ملماً بالمؤسسة، وثقافتها، وأنظمتها، وبأمن المعلومات بشكل عام. وينبغي أن يتمتع بمعرفة قوية بالموارد الذين سيعملون معه، وأن تكون لديه القدرة الفائقة للعمل مع الآخرين، والقدرة على تحفيز الأشخاص الذين يعملون معه على التعاون بشكل جيد.

## ٥. تنفيذ البرنامج

يتطلب التنفيذ الناجح لسياسات وإجراءات أمن المعلومات دعم الإدارة التنفيذية العليا وجميع الأطراف المعنية. وسيساعد برنامج التنفيذ المؤسسة على تحقيق الأهداف المتوخاة التي وضعتها الحكومة السعودية بشأن أمن المعلومات.

وفيما يلي المراحل المختلفة من تنفيذ البرنامج:

### ٥.١. تحديد الأدوار والمسئوليات

بعد إصدار التعليمات، يكون على الإدارة العليا تعيين الأدوار والمسئوليات عن البرنامج التنفيذي، ومن الضروري تعيين الأدوار والمسئوليات قبل البدء بتنفيذ البرنامج. وسيساعد ذلك في برنامج التنفيذ، وذلك لأن كل مرحلة تتطلب مسئوليات وأدوار خاصة بها.

#### ٥.١.١. المسئول عن البرنامج

يضطلع بهذا الدور عموماً المسئول التنفيذي الأعلى لدى الجهة الحكومية.

ويجب أن يقوم المسئول عن البرنامج بالبدء في تنفيذ البرنامج، ويكون مسئولاً عن التنفيذ الكامل للبرنامج، والتأكد من اتباع برنامج التنفيذ بشكل صحيح، ويضطلع بالمسئوليات التالية:

- قيادة البرنامج.
- تقديم اعتمادات الميزانية للبرنامج.
- تقبل المسئولية عن المشاكل التي يتم تصعيدها من مدير البرنامج.
- تحديد أهداف وغايات البرنامج.
- تحديد مؤشرات الأداء الرئيسية المستهدفة.
- تحديد أعضاء لجنة التوجيه.

يجب أن يتمتع المسئول عن البرنامج بمهارات اتصال جيدة، ومهارات تنظيمية، تسهيلية، وقيادية، ومهارات جيدة في حل المشاكل. ويجب أن تكون لديه المعرفة في (اسم الجهة). كما يجب أن يتمتع بالشهرة في قدرته على الضغط داخل المؤسسة للتغلب على المقاومة للبرنامج.

#### ٥.١.٢. لجنة التوجيه

إن الدور الأساسي للجنة التوجيه هو الإشراف على أنشطة إدارة البرنامج التي يؤديها مدير البرنامج.ويشمل ذلك، دون حصر، مراجعة تقييم المتطلبات، تحليل الفجوات، التقارير، اعتماد المبادرات والمشاريع، والمراقبة والمراجعة المستمرة للبرنامج برمته، والمشاريع الفردية. ويجب أن تتأكد لجنة التوجيه من تبليغ كافة الأطراف المعنية عن حالة البرنامج وتقدم سير العمل في تنفيذه. وتتضمن مسئوليات اللجنة ما يلي:

- تحليل مخرجات تقييم المتطلبات والفجوات التي يتم تحديدها.
- التأكد من صحة المبادرات المحددة وتحديد أولوياتها.
- مراجعة التقارير الصادرة عن مدير المشروع.
- مراجعة التقارير مقابل مؤشرات الأداء الرئيسية المستهدفة.
- مراجعة طلبات التغيير المقدمة إلى لجنة التوجيه.
- مراجعة طلبات التغيير وتبليغ المسئول عن التغيير باعتماد/ رفض التغيير.
- اعتماد التغييرات المخططة الجوهرية والرئيسية الناشئة عن تنفيذ السياسات والإجراءات.
- المشاركة في المراجعة التي تتم عقب التنفيذ حسب المطلوب.
- مراجعة تقارير المراجعة بعد التنفيذ، حسب الحاجة.

#### ٥. ١. ٢. ١. العضوية

تضم لجنة التوجيه أعضاء دائمين وأعضاء مؤقتين يتم استدعاءهم بناء على جدول اجتماعات اللجنة، وليس من الضروري أن تتشكل اللجنة في جميع الجهات الحكومية من نفس الأعضاء. ولكن يجب حيثما أمكن، أن يكون الأعضاء من نفس المسميات الوظيفية للأعضاء المعينين أو ما يعادلهم.

الأعضاء الدائمون:

- المسئول عن البرنامج (رئيس اللجنة).
- مدير البرنامج.
- مدير تقنية المعلومات.
- مدير أمن المعلومات.
- مكتب المساعدة.
- خدمات الاتصالات.
- خدمات الحاسب الآلي.
- خدمات الأمن.

الأعضاء المؤقتون:

- الحسابات.
- العمليات.
- مقدمو الخدمات حسبما يراه ضرورياً المسئول عن البرنامج أو مدير البرنامج.
- الموردون حسبما يراه ضرورياً المسئول عن البرنامج أو مدير البرنامج.
- أطراف أخرى حسبما يراه ضرورياً المسئول عن البرنامج أو مدير البرنامج.

يجب أن يمتلك أعضاء لجنة التوجيه مهارات اتصال، مهارات تنظيمية، وتسهيلية، وقيادية، مهارات عرض، مهارات تفاوضية، كما يجب أن تكون لديهم معرفة فنية واسعة ومهارات مالية.

### ٥. ١. ٣. مدير البرنامج

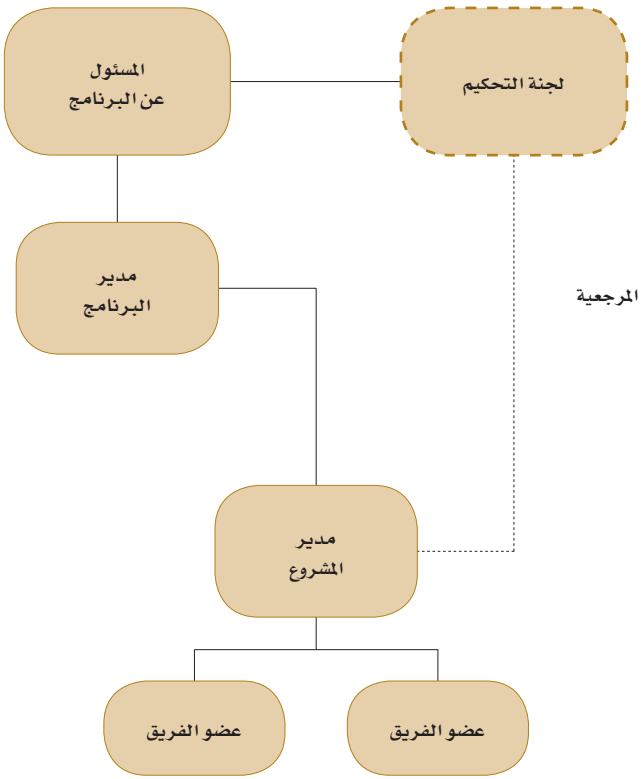
يكون مدير البرنامج مسئولا عن التأكد من إتباع برنامج التنفيذ والالتزام به. وعليه أن يتخذ مبادرات محدده ويحولها إلى مشاريع، وقد يتم تحويل المبادرة الواحدة إلى عدة مشاريع أو مشروع واحد اعتماداً على حجم تلك المبادرة، ويتم تحديد المبادرات المختلفة كمراحل. وتشمل المسئوليات الأخرى لمدير المشروع ما يلي :

- الحفاظ على الأهداف التي حددها المسئول عن المشروع.

- إجـراء تقييم للمتطلبات وإعداد التقارير لعرضها على لجنة التوجيه للمراجعة.
- تقييـم الأثـر المحتمل لبرنامـج التنفيـذ على بيئـة التشغيل الحية.
- تقييم الموارد المطلوبة لبرنامج التنفيذ.
- تقييـم وإعداد الميزانيـة التقديرية (ضمـن الميزانية الأولية المعتمدة) المطلوبة لبرنامج التنفيذ.
- إعـداد المبادرات بناء على الفجوات المحددة في تقرير تقييم المتطلبات.
- وضع أولويات للمبادرات المحددة.
- تعيين مدير المشروع.
- إعداد التقارير الإدارية لتنفيذ البرنامج.
- تحليـل التقارير وتحديد أي توجهـات أو مشاكله واضحة بما في ذلك مقاومة التغيير.
- إجراء مراجعات ما بعد التنفيذ.
- التأكد من الالتزام بالبرنامج.
- التأكد من تمتع الموارد بالمهارات المطلوبة.
- مراقبة وتنفيذ البرنامج للتحسين المستمر.
- الدعـوة إلى وتسهيل عقد اجتماعـات الإدارة العليا لمراجعة التغييرات الرئيسية والتصديق عليها.

تتضمـن المهـارات الأساسية المطلوبة لهذا الـدور ما يلي :مهارات اتصال، مهارات تنظيمية، وتسهيلية، وقيادية، وينبغي أن تكون لديه معرفة بالمؤسسة وتمتلك التأثير، ولديه مهارات في إدارة المشاريع، والعرض، والتفاوض، وخبير في كافـة مجالات أمـن المعلومات، ومهارات قوية في إدارة الموظفي،، وبعض المهارات المالية.

ويبين الإيضاح التالي الأدوار والمسئوليات:



## ٥.٢. تقييم المتطلبات (تحليل الفجوة)

يجب أن يقوم مدير البرنامج بتجميع وتحليل جميع سياسات وإجراءات أمن المعلومات الحالية مقابل سياسات وإجراءات أمن المعلومات المعتمدة. ويتم إظهار أي قيود تعتري تنفيذ السياسات والإجراءات، وينبغي تبليغ القيود والاستثناءات، إن وجدت، إلى الأطراف المعنية.

يجب أن يكون تقرير التقييم الناتج عن مرحلة تطوير المشروع هو المصدر الرئيسي للمعلومات وأساس تقييم المتطلبات هذا (راجع إطار تطوير سياسات ومعايير وإجراءات أمن المعلومات للإطلاع على المزيد من التفاصيل). ويجب أن تحدد الثغرات وجوانب السياسات الناقصة التي تم تحديدها في تلك المرحلة ماذا يجب القيام به لسد هذه الفجوات.

### ٥.٢.١. فهم متطلبات السياسات وأثرها

يجب أن يكون مدير البرنامج فاهماً لوثائق السياسات والإجراءات، وأن يقيّم كيف يمكن لهذه السياسات التأثير على (اسم الجهة). وبناءً على تقرير التقييم الذي تم إعداده كجزء من عملية التطوير، فإن على مدير البرنامج تحديد الفجوات في السياسات والإجراءات المتبعة حالياً، سواء كانت موثقة أم لا. وعليه أن يحدد الجوانب الناقصة التي تحتاج لجهود تنفيذية لما يلي:

- السياسات.
- الإجراءات.
- البنية التحتية.
- الهيكل التنظيمي.
- الموارد.

ينبغي على مدير البرنامج رفع تقرير بالنتائج التي توصل إليها إلى لجنة التوجيه للحصول على اعتمادها.

### ٥.٢.٢. تقييم مخاطر عدم الالتزام

تدل الجوانب الناقصة التي تم تحديدها في مرحلة التحليل على عدم الالتزام بالسياسات المقررة، مما يعد مؤشراً للمخاطر الأمنية التي تواجهها المؤسسة. ويجب تقديم سيناريو قائم على الاحتمالات لإبراز خطورة عدم الالتزام. ويجب على مدير البرنامج كذلك تقييم فيما إذا كانت توجد ضوابط تعويضية لتغطية المخاطر.

### ٥.٢.٣. اعتماد التقييم

تقوم لجنة التوجيه بمراجعة واعتماد نتائج تقرير الجوانب الناقصة والمخاطر المصاحبة لعدم الالتزام بإطار السياسات والإجراءات. وقد لا يوافق أعضاء لجنة التوجيه على النتائج شريطة تقديم مبررات تتعارض مع النتائج. وفي هذه الحالة، يجب أن يتخذ رئيس لجنة التوجيه القرارات الضرورية بشأن قبول التقييم الذي أجراه مدير البرنامج.

## ٥.٣. طرق التنفيذ البديلة

أحد الاعتبارات الرئيسية التي قام عليها إعداد دليل التنفيذ هذا، هو إدراك أن معظم الجهات الحكومية قد لا تتوفر لديها حالياً إدارات أمن معلومات متكاملة، كما قد لا يوجد لديها سياسات وإجراءات أمن معلومات موثقة ومطبقة بصورة جيدة.

وهذا سيؤدي إلى بذل مجهد كبير في مرحلتي التطوير والتنفيذ رئيسية لتحقيق الالتزام بالتوجيهات الحكومية بهذا الصدد. وينصح باتباع منهج تنفيذي يتواكب مع الممارسات الريادية في مجال إدارة المشاريع بهدف تطبيق إدارة منظمة لجميع الجهود المطلوبة لتحقيق الهدف المشترك المتمثل في الالتزام بالتوجيهات الحكومية. وتتضمن الفائدة الأساسية من ذلك التحكم الإداري الكامل ووضوح الصورة إزاء كافة الجهود والاستخدام الأمثل للموارد.

تقوم منهجية هذا البرنامج / المشروع على تحديد مبادرات عديدة ينتج عنها مشروع واحد أو عدة مشاريع واضحة التحديد، تتم إدارتها بعد ذلك من قبل مدير مشروع، وفقاً للممارسات الريادية المتبعة في إدارة المشاريع. وتضم هذه المبادرات والمشاريع مجموعة من الأنشطة / الجهود / الاستثمارات المتشابهة أو المتعلقة ببعضها البعض، والمطلوبة لسد الفجوات الأمنية التي تم تحديدها أثناء التقييم.

ومما تجدر ملاحظته، أن منهج إدارة المشروع الموصوف أعلاه، يتم اختياره اعتماداً على حجم ودرجة تعقيد المجهود المطلوب، وحجم الاستثمار المطلوب من المؤسسة.

في بعض الحالات، قد يكون من الممكن استخدام منهج بديل، إذا كان الأمر لا يتطلب بذل استثمارات ومجهود كبير، وعندما يكون متوقعاً أن ينتج عن الأنشطة البسيطة نسبياً الالتزام بالتوجيهات الحكومية. وفي هذه الحالات، فإن اتباع منهجية تفصيلية في إدارة المشروع قد يعتبر أمراً اختيارياً. وتقوم إدارة الجهة بإعداد مجموعة من الإجراءات التصحيحية وتعيين المهام الفردية ذات العلاقة لموظفيها بما يتوافق مع المجهود المطلوب للالتزام العام بالتوجيهات الحكومية.

وتصف الإجراءات التالية في دليل التنفيذ هذا المنهجية المنظمة في إدارة المشروع بناءً على مشروع واحد محدد أو أكثر كجزء من مشروع متكامل.

## ٥.٤. المبادرات

يقوم مدير المشروع بتحديد وتوثيق الإجراءات اللازمة لتغطية المجالات الناقصة التي تم تحديدها في مرحلة التحليل. وتحتاج هذه المجالات الناقصة إلى مبادرات محددة لتخفيف مخاطر عدم الالتزام المصاحبة لها. ويتم تحديد الموارد الأولية المطلوبة والمتطلبات المسبقة لكل مبادرة قبل تقديمها إلى لجنة التوجيه من مدير المشروع.

ويجب على لجنة التوجيه الحصول على الالتزام من جميع الأعضاء لتخصيص الموارد اللازمة لكل مبادرة:

- يجب أن تخصص لجنة التوجيه وتعتمد الميزانية التقديرية لكل مبادرة، والتي يجب ألا تتجاوز الميزانية الأولية المقررة من المسئول التنفيذي الأعلى.
- يقوم مدير البرنامج بتحديد أولويات المبادرات والأطر الزمنية قبل المضي قدماً في المبادرة إلى مدير المشروع للتنفيذ.
- ينبغي أن يقوم المسئول عن البرنامج باعتماد المبادرات التي يبدؤها مدير البرنامج.

## ٥.٥. المشاريع

بعد تحديد وتوثيق المبادرات، يكون مدير البرنامج مسئولاً عن تحديد مدير مشروع واحد لكل مبادرة (أو مجموعة من المبادرات) كمشاريع مفردة أو متعددة. ويأخذ مدير المشروع كل مبادرة ويتبع دورة إدارة المشروع حسبما ورد في القسم (٥). وعليه أن يتبع أولويات المبادرات حسبما أعطيت له من قبل مدير البرنامج. وعلى مدير المشروع أن يسعى للحصول على التوجيه من مدير البرنامج في جميع المبادرات، والتعاون مع مدير البرنامج في المراحل المختلفة لكل مشروع، وهي مراحل التخطيط، الجدولة، التنفيذ، المراقبة، التحكم، والإغلاق.

## ٦.٥. مخاطر البرنامج الرئيسية

يجب تحديد المخاطر التي ينطوي عليها تنفيذ كل سياسية وإجراء، وتوثيقها، وتحديد خطط التخفيف من آثارها. ومن المهم الأخذ في الاعتبار إلى أي درجة، وبأي السبل، يمكن أن تؤثر محدودية أمن المعلومات على التنفيذ بشكل جوهري.

ما نتائج الفجوات المعلوماتية عندما يبدأ تنفيذ المبادرة على مراحل؟

من أهم مخاطر التنفيذ الشائعة هي الأطر الزمنية المفرطة في الطموح. فالضغوط الزمنية لا تتيح وقتاً كافياً للتعامل مع عوامل النجاح، مثل الخيارات المختلفة من تنفيذ البرنامج، والتشاور مع المنفذين وأصحاب العلاقة، أو الموارد المطلوبة والعقبات التي تعتري التنفيذ. وقد يؤدي ذلك إلى اختلافات جوهرية بين تقديرات تمويل المبادرة والموارد التي سيتم نشرها فعلياً لتنفيذ المبادرة بنجاح.

إذا ما تم تحديد الافتراضات المتعلقة بالمبادرة بشكل واضح، مع حساسيتها للتغيير، فيمكن للجهة الحكومية والأطراف المنفذة للمبادرة الحصول على معرفة أفضل بالمخاطر المحتملة ونتائجها. إن إدراك الأمور غير اليقينية وغير الواضحة يزيد من فرص نجاح التنفيذ، بما في ذلك المبادرات المتعلقة بأمن الشبكة، والبرامج المدفوعة بالطلب، أو المبادرات الجديدة بالكامل، والتي قد تنطوي على توقعات عالية.

قد يتطلب الأمر اتخاذ إجراءات شاملة وجوهرية إذا ما بدأت مخاطر التنفيذ الهامة في التحقق. وإذا اتضح من دراسة المخاطر الناشئة أن المبادرة كبير جداً وطموحة بشكل زائد بالمقارنة مع جدولها الزمني والموارد المستخدمة، فيجب رفع هذا الأمر إلى المحافظ للنظر في الأمر. يمكن الاستجابة بشكل مناسب للمشاكل التي تبدو بشكل ظاهر إذ أنه يمكن إدارتها وتوقعها بشكل أكبر في حال تطوير خطط طوارئ تنفيذية قوية كجزء من إستراتيجية إدارة المخاطر.

ويجب على الإدارة الأخذ في اعتبارها الأدوات والأساليب المختلفة للتغلب على المقاومة للتغيير، أثناء تنفيذ البرنامج. وعليهم استخدام إدارة التغيير عند تنفيذ السياسات والإجراءات لدى (الجهة الحكومية).

## ٧.٥. عوامل النجاح المهمة

يجب تحديد وتوثيق ومراقبة عوامل النجاح المهمة لبرنامج التنفيذ. وتتضمن عوامل النجاح المهمة ما يلي:

### ٥.٧.١. دعم الإدارة

يجب الحصول على دعم الإدارة العليا لأي تغيير تنظيمي بما في ذلك تنفيذ السياسات والإجراءات. ويمكن أن يتضح الدعم الإداري من خلال الثقل الذي يمثله أعضاء لجنة التوجيه، واعتماد لائحة المشروع، وتبليغ الأطراف ذات العلاقة.

### ٥.٧.٢. التوعية والتدريب

من السهولة استغلال الجانب البشري من أمن الحاسب الآلي، وهو ما يتم إغفاله دائماً. وبصرف النظر عن قوة دعائم الأمن الفني المزروع في نظام، أو قوة الأنظمة، أو السياسات، فما يزال هناك إمكانية لكسرها وذلك ببساطة لأن شخصاً ما قام بتخريبها. ومن عوامل النجاح الحساسة رفع درجة الوعي بين الموظفين من خلال برامج التوعية والتدريب. ويجب قياس مستوى وعي الموظف من خلال مقاييس محددة مثل المقاييس التي تنتج عن إجراء مسح

أو استبانة، أو مقايس أخرى مثل عدد حملات التوعية المقدمة، وعدد الأشخاص الذي حضروا أو تمت تغطيتهم بحملات التوعية، إلخ.

ولكـي يتسنـى التنفيذ الناجح للسياسات، فمن الضروري القيام بالتوعية المناسبة بين الأطـراف المعنية، ويجب أن يستخدم مدير البرنامج خطة التوعية النموذجية حسب توجيهات الحكومة السعودية. وتغطي خطة التوعية الجوانب التالية:

- أنشطة التوعية.
- الأطراف المستهدفة.
- احتياجات التوعية الرئيسية للأطراف المستهدفة.
- الأساليب المزمع اتباعها لتنفيذ خطة التوعية.
- مبادرات التوعية مقابل احتياجات التوعية.
- جدول خطة التوعية.

تتوفر وثيقة خطة التوعية بشكل منفصل كجزء من مجموعة الوثائق المستلمة مع الإطار.

### ٥. ٧. ٣. إدارة التغيير

قـد تواجـه عمليات التنفيـذ مقاومة من عدة جوانـب إن لم يكن هنـاك إدارة مناسبة للتغيير، ويتـولى مدير البرنامج تطويـر عملية إدارة التغيـير لبرنامج ومشاريع التنفيذ. وستحدد العمليـة جوانب المقاومة الرئيسية المصاحبة لمبادرات التنفيذ. ويجب أن تشمل الخطة الأدوات والأساليـب اللازمة لإلغاء أو تخفيف النتائج السلبية لتنفيذ سياسات وإجراءات ومعايير أمن المعلومات. ويرد وصف عملية إدارة التغيير في القسم ٧, ١ من هذه الوثيقة.

### ٥. ٧. ٤. الميزانية

إن الميزانيـة هـي أحد الجوانب الهامة لبرنامـج التنفيذ الناجح. ويجب أن يتم تقدير وإعداد الميزانية لمتطلبـات الموارد، والتكاليف، ومبالغ التمويل، والأطر الزمنية بشكل مناسب واعتمادها من قبل لجنة التوجيه.

### ٥. ٧. ٥. إلزامية التنفيذ والتكيُف

يحـدث التنفيـذ الناجح فقط عندما يتم إعداد السياسـات المناسبة، وتنفيذها بشكل فاعل، وقبولها من كافـة الأطراف المعنية، ومراقبتها بشكل منتظم لرصد أية مخالفات أو انحرافات، مع وجود عملية مناسبة للتعامل مع المخالفات والانحرافات. ويمكن اعتبار المسح الذي يتعلق بتوعيـة المستخدمـين وعدد المخالفات المبلغ عنها ضمن فـترة زمنية محددة كمقياس لإلزامية التنفيذ. ويجـب مراقبة جميع هذه المقاييس خلال مرحلة دورة حياة السياسات بهدف تحسينها.

## ٦. إدارة المشروع

عند تعيين مدير المشروع، يتم تحويل المبادرات التي تم تحديدها إلى مشروع بناءً على الأولويات المتعمدة من قبل لجنة التوجيه.

- التخطيط.
- التنفيذ.
- المراقبة والتحكم.
- المراجعة والإغلاق.

### ٦.١. التخطيط

عند استلام المبادرات والمشاريع المعينة، يقوم مدير المشروع بإعداد خطة لتنفيذ كل مشروع.

#### ٦.١.١. تقدير الموارد

يجب أن يقدر مدير المشروع الموارد المطلوبة لتنفيذ السياسات والإجراءات. وتشمل الموارد كلاً من الموارد البشرية والموارد الفنية والبنية التحتية. وبناءً على هذه التقديرات، يُجري مدير المشروع تحليلاً لإظهار توافق الميزانية المتعمدة مع المبادرات المطلوبة لتنفيذ المشروع. ويجب الرجوع إلى المسئول عن برنامج التنفيذ عند الحاجة لإجراء أي تغيير على الميزانية التي سبق وأن تم اعتمادها.

#### ٦.١.٢. إعداد جدول المشروع

بناءً على توفير الموارد، يتم تطوير برنامج التنفيذ لكل مبادرة، ويجب اعتماد الجدول من قبل لجنة التوجيه وتبليغه إلى جميع الأطراف المعنية، ويتم إعداد جدول للمشروع بصيغة (Gantt)، ويفضل أن يكون ذلك باستخدام أداة متابعة المشروع. ويجب أن يصف الجدول كيف يمكن الوصول إلى وتعديل الوسائل المخففة للطوارئ (Contingency buffers) عندما يتراجع الأداء الفعلي عن التقديرات، ويجب أن يصف كيفية ووقت تعديل الجدول وكيفية الاتفاق على والالتزام بالجدول المعدل.

##### ٦.١.٢.١. تحديد التواريخ الهامة

التاريخ الهام، هو حدث رئيسي في المشروع، ويمثل تاريخ انتهاء مجموعة من الأنشطة، وسيكون مدير المشروع مسئولاً عن تحديد التواريخ / الأحداث الهامة التي تعكس بشكل مناسب أهمية وإمكانية تقييم مخرجات كل مرحلة، وذلك عندما ينطوي المشروع على نطاق من الأنشطة المتزامنة أو المتوازية. وفيما يلي مثال بهذا الصدد:

| الحدث الهام | الوصف | تاريخ التسليم |
|---|---|---|
| تشكيل فريق المشروع | إعداد فريق المشروع | يوم / شهر / سنة |

### ٦. ١. ٢. ٢. تحديد الأنشطة

النشـاط هـو «مجموعة من المهـام المطلوبة القيام بها لإنجـاز حدث هام». يقوم مدير المشـروع بالتعاون مع مديـر البرنامج بتجديد جميع الأنشطة المطلوبة لتحقيق الحدث /التاريخ الهام ضمن المشروع. وفيما يلي مثال على ذلك:

| الأنشطة | الوصف | التسلسل |
|---|---|---|
| إعداد قائمة بالموظفين المتاحين | تقديم قائمة بالموظفين الذين لا يشاركون حالياً في مشاريع أخرى | |
| تقييم الموظفين | تقييم الموظفين بناءً على خبراتهم والأهداف المطلوبة وفقاً للائحة المشروع | بعد إعداد قائمة الموظفين |

### ٦. ١. ٢. ٣. تحديد المهام

المهمـة هـي ببساطة «أحد بنـود العمل المطلوب إكمالها ضمن النشـاط». ويقوم مدير المشروع بعد ذلك بتحديد المهـام المطلوبة لكل نشاط. ويحتاج مدير المشروع إلى تحديد المهام التي يمكن قياسها من حيث المجهود المطلوب بذله من قبل الموارد. وفيما يلي مثال على ذلك:

| النشاط | المهمة | التسلسل |
|---|---|---|
| إعداد قائمة بالموظفين المتاحين | الاتصال بمدير الإدارة والحصول منه على قائمة بالموظفين المتاحين | المهمة الأولى |
| إعداد قائمة بالموظفين المتاحين | تجميع القائمة المستلمة من الإدارات المختلفة في وثيقة واحدة | المهمة الثانية |

### ٦. ١. ٢. ٤. تقدير الجهود

سيكون على مدير المشروع، لكل مهمة من المهام المدرجة، تقدير كمية «الجهد» المطلوبة لإكمال المهمة، ويجب توخي العناية أثناء تقدير كمية الجهـد المطلوبـة، وذلك لأن عدم كفاية الوقت المحدد سيضع ضغوطاً على الموارد المعينة، وسيـؤدي إلى تدني جودة العمل، فيما يؤدي تعيين وقـت طويـل إلى تقليل الوقت المخصص لمهمة تحتاج مجهـوداً أكبر، مما يؤدي في النهاية إلى تأخير المشروع عـن الوقت المحدد. وفيما يلي مثال على ذلك:

| المهمة | المجهود |
|---|---|
| الاتصال مع مدير الإدارة والحصول منه على قائمة بالموظفين المتاحين | عدد الأيام |
| تجميع القائمة المستلمة من الإدارات المختلفة في وثيقة واحدة | عدد الأيام |

### ٦. ١. ٢. ٥. تقدير الموارد المطلوبة

يقـوم مديـر المشـروع لكل مهمة من المهـام المدرجة بإعداد قائمـة بالموارد لإنجاز المهمة، ويجـب أن يفهم مدير المشـروع ويتمتع بالمهارات الرئيسية المطلوبة لإنجاز كل مهمة. ويتم ذلك بالتعاون مع مدير الإدارة أو مدير البرنامج. وفيما يلي مثال على ذلك:

| المهمة | الموارد |
|---|---|
| الاتصال مع مدير الإدارة والحصول على قائمة بالموظفين المتاحين | الاسم |
| تجميع القائمة المستلمة من الإدارات المختلفة في وثيقة واحدة | الاسم |

## ٦. ١. ٣. التحكم بالميزانية

يجـب أن يحـدد مدير المشروع آليات التحكـم المستخدمة لقياس تكاليف العمل المنجز، ومقارنة التكاليـف الفعلية مقابل التكاليف المقدرة في الميزانيـة، وتنفيـذ الإجراءات التصحيحية عند انحـراف التكاليف الفعلية بشكل جوهري عن التكاليف المقـدرة في الميزانية. وعليه أن يحدد الفترات أو النقاط التي يتعين التبليغ فيها عن التكلفة، وكذلك الطرق والأدوات التي ستستخدم في إدارة الميزانية. ويكون مدير المشروع مسئولاً عن متابعة الساعات الفعلية والتبليغ عن ساعات المشروع الفعلية والتقديرية إلى لجنة التوجيه بحسب كل تاريخ/حدث هام في المشروع.

## ٦. ١. ٤. معايير وعمليات ومقاييس الجودة

يجب أن تتوافق سياسة وإجراءات التنفيذ مع معايير الجودة لدى (اسم الجهة)، مثل معايير التوثيق. غير أنه يجب تطوير عملية ومقاييس مناسبـة لمراقبـة الفاعليـة والتحسّن أثناء مراحـل التنفيذ والمراقبة. كمـا يجب تحديد آليـات التحكم المستخدم لقياس تقـدم سير العمل والأعمـال المنجـزة ضمن فترة حدث/تاريخ هـام. ويجب كذلك تحديد الطرق والأدوات المستخدمة لمقارنـة التنفيذ الفعلي مقابل المجدول، واستخدام إجراء تصحيحي عند اختلاف التنفيذ الفعلي عن الخطة.

## ٦. ١. ٥. الأدوات والمسئوليات

تزداد احتمالات نجاح المشروع إذا كان هناك مستوى قوي من دعم الإدارة العليا لعمليات تنفيذ السياسات. وبدون الدعم القوي من الإدارة العليا، فأي تغييرات سيفتقر للفاعلية.

### ٦. ١. ٥. ١. لجنة التوجيه (تعمل كلجنة توجيه للمشروع)

يتم إطلاع لجنة التوجيه على حالة المشروع بانتظام، ويتم التعامل مع المسائل الناشئة عن تنفيذ المشروع من قبل اللجنة. وللجنة الصلاحية لاعتماد التغيير في جدول المشروع، والتأكد من توافق ذلك التغيير مع الإطار الزمني المحدد في التوجيهات الحكومية، وقد تم ذكر المزيد من التفاصيل المتعلقة بالدوار لمسئولية اللجنة في القسم ٣, ٢, ٣. ويمكن أن تضم لجنة التوجيه أعضاء من داخل الجهة الحكومية، ويمكن أن توسع عضويتها لتضم أطرافاً معنية، واستشاريين مختصين، أو ممثلين من جهات أخرى.

### ٦. ١. ٥. ٢. مدير المشروع

تحتاج كل مبادرة لمسئول أول عنها لكي تكون فعالة، ويكون مدير المشروع مسئولاً عن التنفيذ الناجح للمشروع، وهو الشخص الذي تطلب منه لجنة التوجيه أو المسئول التنفيذي المعني تقديم تقارير سير العمل. ويجب أن يلعب مدير المشروع دوراً محورياً للتأكد من إشراك الأشخاص المناسبين، وأنهم يؤدون الأعمال المناسبة في الوقت المحدد.

### ٦. ١. ٥. ٣. فريق المشروع

يتعين على مدير المشروع كذلك إعداد أفضل فريق ممكن لتنفيذ المشروع. ويشمل ذلك توفر المهارات المناسبة في أعضاء فريق المشروع. ومن المتطلبات الرئيسية لمدير المشروع أن يقوم بتعيين الأدوار والمسئوليات لأعضاء فريق المشروع، والتأكد من تأدية هذه المهام والمسئوليات بشكل سليم. وينبغي على مدير المشروع اختيار فريق المشروع من بين الأطراف المعنية، آخذاً في الاعتبار المهارات المطلوبة للإشراف على تنفيذ المبادرات. وفي حال عدم توفر المهارات المناسبة لدى أعضاء فريق المشروع، فيجب توخي الحذر عند تعيين المهام للأطراف المعنية للقيام بها.

## ٦. ١. ٦. اقتران الأدوار والمسئوليات

إن خطر التأجيل أو خطر عدم الانتباه للترتيبات الرسمية في المؤسسة يكمن في عدم الاتفاق أو وقوع الارتباك بشأن الأدوار، وقد يظهر هذا الأمر لاحقاً أثناء التنفيذ. ولحل أو تفادي هذا الإشكال يجب إعداد الترتيبات مبكرة، واستكمالها بشكل سريع. وعند إشراك الإدارات الأخرى، يجب النظر في عقد مذكرة تفاهم أو اتفاقية تحدد الأهداف، والأدوار، والمسئوليات، ومتطلبات التقارير للأطراف التي ستعنى بالقيام بهذا المجهود. ويتعين على المسئول عن البرنامج أن يقرن بين كل قسم في السياسة بالأدوار المدرجة في النموذج المرفق. ويستخدم هذا الاقتران للتأكد أن المدراء التنفيذيين لدى (الجهة الحكومية) يفهمون مسئولياتهم التي تمليها السياسة.

وهذا النموذج هو أداة ناجحة في تأسيس وتبليغ المسئوليات والإجراءات المطلوبة على كافة المستويات. ويجب توزيعها على الأفراد المعنيين واستخدامها كوثيقة للمناقشة عند إعداد خطط التنفيذ.

## ٦. ١. ٧. عقد المشروع

يقوم مدير المشروع بتوحيد المعلومات التمهيدية المستلمة من مدير المشروع في وثيقة تسمى دليل المشروع. وتشمل هذه الوثيقة بياناً لنطاق العمل، أهداف المشروع، والمشاركين في المشروع. ويقدم هذا العقد صورة أولية للأدوار والمسئوليات، ويحدد أهداف المشروع، ويحدد كذلك الأطراف المعنية الرئيسية، كما تحدد صلاحيات مدير المشروع. ويمكن أن يستخدم هذا العقد كمرجع أو نموذج يمكن استخدامه للمشاريع الأخرى المختلفة التي قد تنشأ عن المبادرات.

يجب أن يغطي عقد المشروع المجالات التالية بشكل عام:

- لمحة عامة عن التنفيذ.
  - وصف المبادرة / المبادرات.
  - الأهداف المرحلية والنهائية.
  - نطاق العمل.
  - عوامل النجاح الحساسة.
  - الافتراضات.
  - القيود.
- صلاحيات المشروع والتواريخ / الأحداث الهامة.
  - صاحب الصلاحية في التمويل.
  - الجهة المسئولة عن الإشراف على التنفيذ.
  - تواريخ التنفيذ الرئيسية.
- تنظيم المشروع.
  - هيكل المشروع.
  - الأدوار والمسئوليات.
  - مرافق وموارد المشروع.
- نقاط الاتصال.
- المصطلحات الهامة.
- تاريخ التعديلات.
- الملاحق.

### ٦. ١. ٨. الاتصال

يحتاج الاتصال بشأن إحدى السياسات أو إحدى مبادرات البرنامج إلى الالتزام والدعم من الأطراف المعنية بالتنفيذ. ويتضمن ذلك "الرؤية الخارجية الواضحة"، بمعنى أن لا يكون ذلك من منظور الجهة الحكومية فقط، وإنما من منظور الأطراف المعنية أيضا، وخصوصاً فيما يتعلق بكيفية رد فعل الأطراف المستهدفة، وأفضل سبل الاتصال.

يجب أن يكون هدف الاتصال واضحاً (ومتوافقاً مع الهدف الأولي للسياسة). ويمكن المساعدة في ذلك من خلال تطوير إستراتيجية الاتصال التي توفر وسيلة للمساعدة على النجاح أو خلاف ذلك.

يعد الاتصال عنصراً مركزياً في عملية التغيير، وكلما زاد أثر التغيير، كلما زادت الحاجة إلى بيان الأسباب والمبررات التي تقف وراء التغيير بصورة واضحة، والفوائد المتوقعة، وخطط التنفيذ، والآثار المقترحة. وبدون الاتصال الفعال، يمكن للأطراف ذات العلاقة إغفال معلومات هامة، وقد يتعذر عليهم فهم الحاجة إلى التغيير، أو المزايا التي يحصلون عليها من التغيير.

ويهدف الاتصال إلى ما يلي:

- الحفاظ على ارتفاع وتيرة الوعي والالتزام.
- الحفاظ على رسائل متماثلة وثابتة.
- التأكد من عدم خروج التوقعات عن الخط ومخالفة المخرجات المتوخاة.

تعد إدارة وسائل الإعلام من الجوانب الهامة في إستراتيجية الاتصال. وقد يكون من الواجب أن تأخذ الإستراتيجية في الاعتبار الجوانب الاستباقية وردة الفعل لإدارة وسائل الإعلام.

إنه من المهم إتاحة المجال للإدارة العليا للمشاركة في عملية تنفيذ

الإستراتيجيـة، ومناقشـة توقعاتها وتقـديم أي ملاحظات بصدد ذلـك. وسيسهّل ذلك من تحديـد كيفية إمكانيـة انعكاس معايير نجاح المبادرة على الرسائل الرئيسية في إستراتيجية الاتصال.

وقد يتطلب الأمر إجراء تغيير على وسائل الاتصال والأولويات أثناء التنفيـذ للأخذ في الاعتبار المتطلبـات المتزايدة للأطراف المعنية، وخصوصـاً في ظـل تزايد معرفتهـم ونمو الطلب علـى المعلومات. كما أن مراقبـة ردود الأطراف المعنية لوسائل الاتصالات المختلفة تساعـد في تقييم الحاجة لهذا التغيـير، وتساعد كذلك على إدارة التوقعات طوال مراحل التنفيذ.

### ٦.١.٩. خطة الشراء

إذا كان هنـاك حاجـة لتقنيـة جديـدة في المشروع، يجـب أن يتم تحديـد متطلبـات الشراء، وإعـداد خطـة الشراء وفقـاً لسياسة المشتريات لدى (اسم الجهة).

### ٦.١.١٠. اعتماد المشروع

يجـب أن تخضع خطة المشـروع لموافقة لجنة التوجيه، ومن ثم يتم توزيعها وتبليغها إلى الأطراف المعنية.

## ٦.٢. التنفيذ

### ٦.٢.١. اجتماع بدء العمل

يجـب أن يدعو مدير المشروع إلى عقد اجتماع تمهيدي لبدء العمل مع جميع الأطراف المعنيـة، لتوضيح خطة المشروع. وينبغي إعداد محضر ذلك الاجتماع، وتوزيعه، وحفظه في ملف المشروع.

### ٦.٢.٢. تنفيذ خطة المشروع

يجـب تنفيذ المشروع وفقـاً لعقد المشروع المعتمـد وخطة المشروع. ويقوم أعضاء فريق المشروع بتنفيذ المهام المعينة لهم في كل مرحلة مـن مراحل خطة المشـروع. وتقع على عاتق مديـر المشروع ومدير الإدارة مسئوليـة التأكد من أن الموارد التي تم تعيينها تقوم بتنفيذ المهام ضمن الإطار الزمني المحدد.

ويجـب أن يتم التأكـد أثناء عمليـة التنفيذ من القيـام بالأنشطة المخططـة بصـورة فاعلـة وبكفـاءة، والتأكـد في الوقـت ذاتـه مـن استمراريـة تجميـع وتحليـل القياسيـات مقارنـة بالخطط، والمواصفات، ونطاق العمل الأصلـي، والعمل على ذلك طوال دورة حيـاة المشروع. ذلك لأن الافتقار لتعريـف عمليات تنفيذ محددة، يؤدي بالنتيجة إلى استقلال كل فريق بتنفيذ الخطط وفقا لم يراه مناسبا بحسب ممارسات وخـبرات وأساليب أعضاءه، مما يؤدي في النهايـة إلى فقد التحكم بالمشروع والمتابعة وأنشطة الإجراءات التصحيحية.

### ٦. ٢. ٣. تحسين التنفيذ

يتم تحليل التحسينات بناءً على المقاييس المحددة. ويتم تجميع البيانات دورياً من قبل مدير المشروع وتحليلها، حيث تشكل هذه المعلومات جزءاً من التقارير الدورية المرفوعة للجنة التوجيه. وتساعد عوامل النجاح المهمة للقيام بمراجعة مناسبة للتنفيذ. وعنى مدير المشروع بمسئولية القياس عن الأداء، ويشمل ذلك تحديد الاختلافات بين العمل المخطط مقابل العمل الفعلي المنجز، والتكاليف الفعلية مقابل التكاليف المقدرة من الميزانية.

كما يكون مدير المشروع مسئولاً عن تقديم تقرير عن حالة المشروع إلى جميع الأطراف المعنية لإعطائها بيان وصورة واضحة عن سير المشروع. وتكون جميع الأطراف المعنية في المشروع مسئولة عن اتخاذ الإجراءات اللازمة بشأن الاختلافات المذكورة كي يتسنى إكمال المشروع ضمن الوقت والميزانية المحددين.

### ٦. ٢. ٤. تقارير عن حالة سير المشروع

يهدف التقرير عن حالة المشروع إلى تطوير صيغة قياسية لتبادل المعلومات بصفة رسمية فيما يتعلق بتقدم سير العمل في المشروع. ويجب تصميم التقرير عن حالة المشروع بما يتناسب مع المشروع ذاته. ويجب أن يكون التقرير موحداً لجميع أعضاء فريق العمل. ويجب إعداد تقرير الحالة من قبل فريق المشروع، شاملاً الأنشطة، المنجزات، الأحداث / التواريخ الهامة، القضايا والمشاكل المحددة. لذا، يتعين أن يتبع التقرير صيغة محددة، بحيث تستخدم جميع التقارير نفس النموذج.

لقد تم إيراد نموذج تقرير الحالة في الملحق (٨,٢,٨) ويجب استخدامه للتبليغ عن المعلومات الرئيسية، ويشمل ذلك:

- الوضع الحالي للمشروع.
- الأداء.
- الإنجازات الرئيسية خلال الفترة التي يشملها التقرير.
- الأنشطة المجدولة.
- القضايا والمشاكل.

ويمكن إرفاق الوثائق التالية مع تقرير الحالة:

- لوحات بيانية محدثة ومعدة باستخدام نظام Gantt.
- خطط استعادة الأنشطة غير المدرجة في الجدول.
- خطط العمل التصحيحية للمشاكل المتوقعة.
- القرارات المتعلقة ببنود العمل المعينة.

### ٦. ٢. ٥. المشتريات والتنفيذ

قد تطلب (اسم الجهة) أثناء مرحلة التنفيذ شراء منتجات أو خدمات تحتاجها في تنفيذ السياسات والإجراءات، مثل نظام مراقبة الوصول، إلخ. وفي هذه الحالات، يجب تنفيذ خطة الشراء. ويمكن أن يكون لدى الجهة مجموعة محددة من الإرشادات والسياسات التي توفر البنية التحتية لمشتريات المشاريع، والتي يجب دمجها وتكاملها مع خطة الشراء.

وستحدد هذ الإرشادات سياسة طلب المشتريات، اختيار مصدر الشراء، وإدارة عقود الشراء. وعلى الرغم من أن مسئوليات الطلب والتعاقد قد لا تكون دائماً ضمن مسئوليات مدير المشروع، إلا أنه ما زال من المهم أن يكون لدى مدير المشروع الفهم الأساسي لسياسات التعاقد والشراء.

## ٦. ٣. المراقبة والتحكم

تمكّـن المراقبة والمراجعـة الفاعلة للتنفيذ الجهـات الحكومية من التأكد من استمرارية توفر الموارد الكافية للتعامل مع نطاق العمل، والمخاطـر، وحساسيـة المشروع. كمـا تمكن الأطـراف المعنية من تقييـم تقدم سير العمـل في المشروع، وتحديـد ومعالجة المشاكل، ومراجعـة أهميتهـا النسبيـة وأولوياتهـا. ومممـا يعزز مـن كفاءة المراقبـة والمراجعة هو أن يتم القيام بها من قبل موظفين يتمتعون بالمهـارة والمعرفـة في المشـروع الجـاري تنفيذه، ويمتلكـون موارد إدارية كافية لمعالجة بيانات المراقبة الروتينية.

يجـب أن تعكس المراقبة والتقارير أهميـة المبادرة، ومخاطر عدم الالتـزام المتعلقة بتلك المبادرة، وتأخذ في الاعتبار الأعباء الإدارية التي تضعهـا عمليات تجميع البيانات وإعـداد التقارير على فريق المشـروع والمـوارد الأخـرى لدى (اسـم الجهة). وتكـون التقارير أفضـل فاعلية عندما توفر المستوى المناسب من التفاصيل المتعلقة بالمسئوليات على كل مستوى من المستويات لدى (اسم الجهة).

### ٦. ٣. ١. مقاييـس الأداء (مؤشرات الأداء الحساسة)

يساعد التحديد المبكر لمصادر البيانات المناسبة في تأسيس أنشطة مراقبـة موثوقة وفاعلة. فالتبليغ السريـع عن القضايا والتوجهات الرئيسيـة قد يكون له أولوية أعلى من دقة البيانات، وخصوصاً في المبادرات التي تنطوي على درجة مخاطر عالية:

وعندمـا يتضمـن المشروع مبـادرات متعـددة، فمن المهـم تقييم المخـاوف أو الدروس المستفادة من كل مرحلة من مراحل المشروع، وتصعيـد ما لـزم منها، وحلهـا. ويجب التعامل مـع القضايا التي تظهر بشكل مناسب قبل تقدم المشروع إلى المرحلة التالية.

ويمكـن أن يساعد تقييم المشروع على تحديـد إلى أي مدى تسهم المهـام المنفـذة في ذلك المشـروع في تحقيـق المبـادرات المحددة. والدروس الرئيسية المستفادة قد تقـدم مساهمة كبيرة في تنفيذ المبادرات المستقبلية. ويجب أن يهدف التقييم إلى تحديد الدروس المستفادة التي قد تساعد في المستقبل على ما يلي:

- تحسين تنفيذ المشروع وعملية صنع القرار.
- المساعدة في تخصيص الموارد.
- تعزيز المسئوليات من حيث تقييم النتائج التي تم تحقيقها.
- تعزيز التعلم في المؤسسة واتباعها للممارسات الجيدة.

### ٦. ٣. ٢. التحقق من نطاق العمل

يجـب أن يركز التحقق من النطاق على انه يتـم تنفيذ السياسات والإجراءات بشكل صحيح، وأنها تحقق أهداف المؤسسة.

ويتـم التحقـق مـن النطاق من خـلال إجـراء مراجعـات رسمية للتنفيـذ. وعند اكتمـال التنفيذ، تقوم لجنـة التوجيه بعد مراجعة الحالة بتوقيع تقرير اكتمال التنفيذ.

### ٦. ٣. ٣. التوصية بالتغييرات والتصحيحات

يجـب أن تخضـع التغيـيرات والانحرافـات عن الخطـة المعتمدة، إن وجـدت، لعمليات إدارة التغيير، ويجـب أن يقوم مدير المشروع بتقديم طلب توصية إلى لجنة التوجيه بعد تحليل المخاطر وضوابط تخفيفها. وتتخذ لجنة التوجيه قرارها القائم على المعرفة فيما إذا ارتأت اعتماد أو رفض التغيير.

## ٧. مراقبة المخاطر

تحديد المخاطر، ومراقبتها، وحلها تعتبر أدوات أساسية لإنجاز أعمال التنفيذ بنجاح. ويتم البدء بعملية إدارة المخاطر كجزء من تخطيط المشروع، ويتم تحديثها حتى نهاية المشروع وإقفاله. وفيما يلي العناصر الرئيسية لعملية مراقبة المخاطر:

- إعداد مستودع مركزي لمعلومات المخاطر والوثائق المتعلقة ببنود المخاطر وإستراتيجيات الحلول.
- تلخيص المعلومات على نموذج المخاطر.
- تضمين ملخص عن المخاطر في اجتماعات سير العمل المنتظمة.
- تقديم عملية متماثلة ومستمرة لبنود المخاطر وتطوير إستراتيجيات المخاطر:
  - تحديد المخاطر.
  - تقييم المخاطر.
  - تحديد الحل.

### ٧. ٣. ١. تقارير الأداء

ينبغي على مدير المشروع تجميع وتوجيه البيانات المتعلقة بحالة المشروع. ويجب رفع هذه التقارير إلى لجنة التوجيه، التي يتعين عليها مراجعة هذه التقارير خلال اجتماعاتها الأسبوعية لمراجعة الأداء.

### ٧. ٣. ٢. اجتماعات مراجعة سير العمل

يجب أن تعقد لجنة التوجيه اجتماعات مراجعة دورية للأداء لمراجعة حالة التنفيذ. ويتم مناقشة تقارير إدارة المشروع في هذه الاجتماعات، ويتعين أن تتخذ لجنة التوجيه القرارات المتعلقة بطلبات التنفيذ. وتطرح أثناء اجتماعات اللجنة الجوانب التالية على سبيل المثال:

- اختلافات الجدول.
- اختلافات الميزانية.
- تغيير الموارد.
- المخاطر الجديدة / الظروف غير المتوقعة.
- تغييرات الخطة.

يجب إعداد وتوثيق محاضر كافة اجتماعات المراجعة، وحفظها في ملف المشروع.

### ٧.١. الإغلاق

يجب أن يتم إغلاق مشروع تنفيذ سياسات وإجراءات أمن المعلومات رسمياً بعد المراجعة الرسمية للأداء من قبل لجنة التوجيه. وعند اتضاح التنفيذ الناجح، ترفع لجنة التوجيه تقريراً إلى الإدارة العليا لعرض الحالة عليها والحصول على موافقتها الرسمية. عقب ذلك، ينبغي أن تقوم لجنة التوجيه بالتوقيع على إنجاز المشروع، وتخلي سراح الموارد التي كان قد تم تخصيصها للمشروع، وتتضمن عملية الإغلاق الرسمية ما يلي:

- مراجعة التنفيذ.
- الحصول على القبول الرسمي.
- التقرير النهائي.
- الفهرسة، وسجلات الأرشيف.
- تحديث الدروس المستفادة.
- التوقيع النهائي.
- إخلاء الموارد.

الجزء الرابع

# إدارة التغيير

## ١. لمحة عامة

يقـدم هـذا القسم لمحة عامة عـن خطة إدارة التغيـير التي سيتم استخدامهـا من قبـل (اسـم الجهة). وتحـدد الوثيقـة تفاصيل الأدوار والمسئوليات التي سيتم تعبئتها ضمن عملية إدارة التغيير، حسبما يلي:

- المسئول عن عملية التغيير.
- مدير التغيير.
- منشئ التغيير.
- محلل التغيير.
- لجنة التوجيه.

كما تقدم الوثيقة تفاصيل مراحل عملية إدارة التغيير:

- البدء في التغيير.
- تقييم التغيير.
- تحديد فئة التغيير.
- فحص التغيير.
- اعتماد التغيير.
- تخطيط وجدولة التغيير.
- تنفيذ التغيير.
- مراجعة التنفيذ.

تقـدم خطـة إدارة التغيـير الأدوات والأساليـب المطلوبـة لإدارة الأشخاص والفرق والإدارات عند تطبيـق التغيير على بيئة العمل لديهم وقياس فاعليته.

## ٢. الأدوار والمسئوليات

مـن الضروري تعيين الأدوار والمسئوليات قبل البدء في عملية إدارة التغيـير، حيث أن ذلـك سيساعد على تنفيذ العمليـة، نظراً لأنها بحاجـة إلى تحديد مسبـق للمسئوليات وللشخص المسئول عنها. ومـن خلال هـذه الأدوار، سيكون لـدى الإدارة المعنيـة والموظفين فهمـاً واضحـاً لمسئولياتهـم ووظائفهم في كل مرحلـة من مراحل إدارة التغيير.

يتعـين على (اسـم الجهة) تحديـد الأدوار والمسئوليـات المساندة لعملية إدارة التغيير، وسيتم من خلال المسئوليات المحددة التحكم بالتغيير الذي أحدثته سياسات وإجراءات أمن المعلومات.

### ٢.١. المسئول عن عملية التغيير

يجـب تعيين المسئول عـن عملية تغيـير سياسات وإجـراءات أمن المعلومـات من خارج إدارة أمن المعلومـات، لتفادي ورود التعارض في المصالـح. وبالتالي، يتم تعيين المسئـول التنفيذي الأعلى ليكون مسئولاً عن عملية التغيير.

وسيكـون المسئـول عـن التغيير مسئولاً عـن كامل عمليـة التغيير، والتأكـد مـن اتبـاع هـذه العملية بشـكل سليـم. ومـن مسئولياته الأخرى:

- الحفاظ على الغايات والأهداف ضمن العملية.
- تصميم والتوصيه بالمقاييس والتقارير للإدارة.
- تقـديم عمليـة إدارة تغيـير تعمـل بشـكل يكسـب الرضـا للموظفين.
- التأكد من تمتع الموارد المستخدمة بالمهارات المطلوبة.
- الحفاظ على التحسين المستمر للعملية بشكل منتظم.

ومـن المهارات الرئيسية المطلـوب أن يتحلى بها صاحب هذا الدور أن يكـون لـه تأثير على كامـل المؤسسـة، وأن تكون لديـه مهارات اتصال، ومهارات تنظيمية، وتسهيلية، وقيادية، وأن يتمتع بالمعرفة ب (اسـم الجهـة)، وأن تكـون لديـه مهـارات في إدارة المشاريع، ومهـارات تفاوضيـة، ومعرفة فنية عامة، ومهـارات قوية في إدارة الموظفين، ومهارات مالية.

## ٢. ٢. مدير التغيير

يجـب تعيين مدير التغيـير في سياسات وإجـراءات أمن المعلومات مـن إدارة أمن المعلومات، إذ سيكون لديه معرفة أفضل ببيئة أمن المعلومات. ووفقاً للممارسات المعيارية المتبعة في هذا القطاع، يمكن أن يكون هذا الدور هو دور آخر لمدير أمن المعلومات / مسئول أمن المعلومات، ويعتمد ذلك على الهيكل التنظيمي لدى (اسم الجهة). وحسبمـا تم تحديـده في أقسام سابقة من هـذه الوثيقة، فسيكون هذا الشخص كذلك هو مدير برنامج تنفيذ أمن المعلومات.

يكون مدير التغيير مسئول عن اعتماد أو رفض طلبات التغيير بعد مراجعتهـا من لجنة توجيه أمـن المعلومات. وتتضمـن مسئولياته الأخرى ما يلي:

- تقييم الأثر المحتمل للتغيير على بيئة التشغيل الحية.
- تقييم الموارد المطلوبة لتنفيذ التغيير.
- تقييم التكاليف المستمرة للتغيير حسب اللزوم.
- تقييم أثر عدم تنفيذ التغيير.
- اعتمـاد التغييرات المقبولة التي صادقت عليها لجنة التوجيه أو المسئول التنفيذي الأعلى للتغييرات الجوهرية والرئيسية.
- التحقق من صحة أولوية التغيير.
- التأكد من فئة التغيير.
- التأكد من اكتمال التغيير.
- إجراءات المراجعات اللاحقة للتغيير.
- مراجعـة التقاريـر الإداريـة، ومؤشـرات الأداء الرئيسيـة (التأكد مـن تحقيق الغايـات المستهدفة)، وإصـدار تدابير تصحيحية بشأن الأهداف غير القابلة للتحقيق).
- تحليـل سجـلات التغيـير لتحديـد التوجهـات أو المشـاكل الظاهرة التي تحدث بما في ذلك مقاومة التغيير.
- تحديـد التغييرات في الوثائق التي تجاوزت / لم تلتزم بعملية إدارة التغيـير، وتقـديم معلومـات إلى المسئـول عـن عملية التغيير للتعامل مع متطلبات الالتزام.
- مساعـدة المسئـول عـن عمليـة الالتـزام في تحديـد ووضع أولويات التحسينات المطلوبة على العملية.
- التأكد من الالتزام بالعملية.
- الدعـوة إلى وتسهيل عقد اجتماعـات الإدارة العليا لمراجعة التغييرات الرئيسية والتي تم التصديق عليها.
- إحالـة التغيـيرات الجوهريـة والرئيسية إلى لجنـة التوجيه أو المسئول التنفيذي الأعلى للمراجعة.
- التواصـل مع كافة الأطـراف الضرورية لتنسيق عمليات بناء واختبار وتنفيذ التغييرات.
- تحديث سجـل التغيير بكافة المعلومـات المتعلقة بتقديم سير العمل.
- مراجعـة التغييرات المعلقـة التي تنتظر البت فيهـا أو اتخاذ الإجراء اللازم نحوها.

تتضمن المهارات الرئيسية المطلوبة في هذا الدور مهارات الاتصال، المهارات التنظيمية، والتسهيلية، والقيادية، والمعرفة بـ(اسم الجهة)، والقدرة على التأثير، ومهارات في إدارة المشاريع، ومهارات في العرض، ومهارات تفاوضية، والخبرة في كافة جوانب أمن المعلومات، ومهارات إدارة قوية للموظفين، وبعض المهارات المالية.

## ٢.٣. منشئ التغيير

منشئ التغيير لإحداث تغيير في سياسات وإجراءات أمن المعلومات يمكن أن يتم تعيينه من إدارة أمن المعلومات نظراً لأنه سيكون لديه فهم أفضل ببيئة أمن المعلومات. ووفقاً للممارسات المعيارية المتعبة في هذا المجال، فإن هذا الدور يمكن أن يكون دوراً إضافياً لأحد الموظفين المعنيين بإدارة أمن المعلومات / إدارة تقنية المعلومات، ويعتمد ذلك على الهيكل التنظيمي لـ(اسم الجهة).

تتمثل المسئولية الأساسية لمنشئي التغيير في استلام إشعارات التغيير من مدير/ مدراء المشاريع وتسجيلها في طلب تغيير، وهنا يتعين على منشئ التغيير استكمال كافة المعلومات الإلزامية المتعلقة بالتغيير.

تتضمن المهارات الرئيسية المطلوبة في منشئ التغيير ما يلي:

- مهارات اتصالات.
- المعرفة بـ (اسم الجهة).
- المعرفة بأمن المعلومات.

## ٢.٤. محلل التغيير

يجب أن يتم تعيين محلل التغيير في سياسات وإجراءات أمن المعلومات من داخل إدارة أمن المعلومات نظراً لأنه سيكون لديه فهم أفضل في بيئة أمن المعلومات.

يقوم محلل التغيير باستلام طلبات التغيير مع سياسات وإجراءات أمن المعلومات المطلوب تنفيذها. وتكون مسئوليته الأساسية تقييم الحالة الراهنة للسياسات والإجراءات وفحصها مقابل السياسات والإجراءات الجديدة، وإعداد تحليل الفجوة بين الحالتين. كما يتعين على محلل التغيير إجراء تحليل لمواطن القوة والضعف والفرص والتهديدات (SWOT) للسياسات والإجراءات التي تم إعدادها حديثاً، ويشمل ذلك تحديد مواطن القوة في تنفيذ السياسات والإجراءات، وتحديد نقاط الضعف التي يغطيها تنفيذ السياسات والإجراءات، وما هي الفرص التي ستتوفر لـ (اسم الجهة) من خلال تنفيذ السياسات والإجراءات، وما هي التحديات/ التهديدات التي قد تواجهها (اسم الجهة) من خلال تنفيذ هذه السياسات والإجراءات. وقد تم تضمين مثال نموذجي لتحليل الثغرة وتحليل مواطن القوة والضعف والفرص والتحديات في الملحق.

وتتضمن المسئوليات الأخرى لمحلل التغيير ما يلي:

- التقييم الأولي لطلبات التغيير، وإعادة طلبات التغيير غير المكتملة إلى منشئيها.
- المشاركة في المراجعة اللاحقة للتنفيذ حسب اللزوم.
- المشاركة في اجتماعات لجنة التوجيه حسب الحاجة.

المهارات الرئيسية المطلوبة لهذا الدور:

- مهارات في الاتصال.

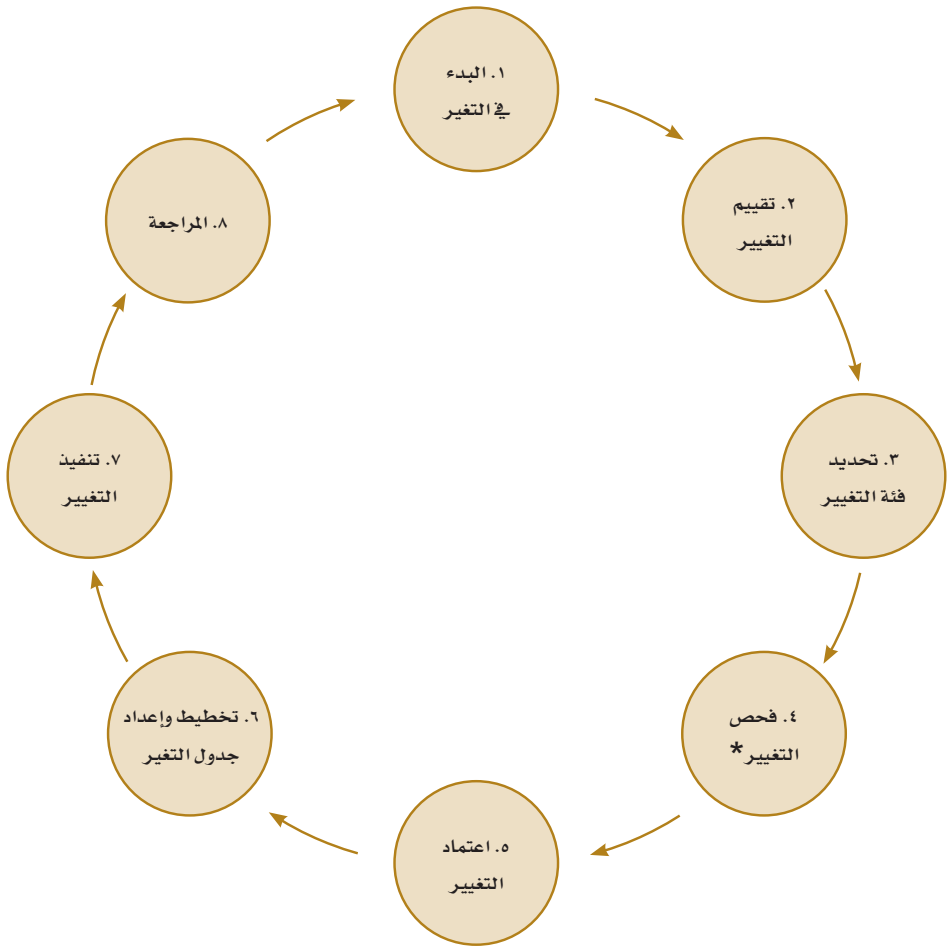
- مهارات تنظيمية.
- المعرفة في (اسم الجهة).
- مهارات تحليلية قوية.
- خبرة / مهارات في تجميع البيانات.
- مهارات فنية قوية في مجال أمن المعلومات وبشكل محدد في بيئة النظام، والأنظمة المساندة.

### ٢.٥. المجلس الاستشاري للتغيير (تعمل لجنة أمن المعلومات بمثابة مجلس استشاري للتغيير)

ستعمل لجنة التوجيه بمثابة مجلس استشاري لتغيير السياسات والإجراءات التي تم إعدادها حديثاً. والوظيفة الأساسية للجنة التوجيه هي مراجعة التغييرات المقترحة والتأكد من أنها متوافقة مع إطار سياسات وإجراءات أمن المعلومات. وتتضمن مسئوليات لجنة التوجيه ما يلي:

- مراجعة طلبات التغيير المقدمة إلى لجنة التوجيه.
- تقييم التغيرات الجوهرية والرئيسية التي تم تعديلها من حيث أثرها على البرنامج.
- المشاركة في جدولة التغييرات الجوهرية والرئيسية.
- التأكد من صحة أولويات وفئات التغيير.
- مراجعة طلبات التغير، وتقديم المشورة إلى مدير التغيير باعتماد / رفض الطلب.
- النظر في جميع التغييرات على جدول الأعمال، وتقديم المشورة إلى مدير التغيير بشأن الطلبات الواجب اعتمادها.
- المشاركة في المراجعة اللاحقة للتنفيذ حسب الحاجة.
- مراجعة المراجعات اللاحقة للتنفيذ حسب الحاجة.

## ٣. عملية إدارة التغيير




*ملاحظة: في بعض الحالات يكون الفحص مطلوباً للتأكد من أن التغييرات الجاري تنفيذها لا تؤثر سلبياً على لأنظمة والتطبيقات لدى (اسم الجهة) وأعمالها اليومية.

تهـدف إدارة التغيير بشكل أساسي إلى تسجيل، وتقييم، واعتماد، وتحديـد أولويات، وتخطيط، وفحص، وتنفيـذ، وتوثيق، ومراجعة التغيـير في سياسات ومعايـير وإجراءات أمـن المعلومات بطريقة قابلـة للتحكـم. أما الهـدف الثانوي لإدارة التغيـير فهو من إتمام الفـترة الانتقاليـة بشـكل سلس، ممـا يعنـي عمومـاً التعامل مع القضايـا والإشكالات المتعلقة بمقاومـة التغيير. ويتعين على (اسم الجهة) اتباع عمليـة إدارة التغيير التالية من أجل تغيير سياسات وإجراءات أمن المعلومات الحالية لديها.

### ٣.١. البدء في التغيير

بمجـرد استلام منشئ التغيـير إشعاراً رسميـاً بالتغيير المطلوب، فعليـه تقديم طلب التغيير للبدء في عملية إدارة التغيير. يتم إحالة طلب التغيير بعد ذلك إلى محلل التغيير لتقييم التغيير. وفيما يلي الخطوات المتبعة في هذه المرحلة:

- يقوم منشئ التغيير بإرسال طلب التغيير.
- يقـوم منشئ التغيـير بتسجيـل البيانـات الأساسيـة (اسم الإدارة، المستخدمين المتأثرين).
- إحالة طلب التغيير إلى محلل التغيير.

### ٣.٢. تقييم التغيير

يقـوم محلـل التغيير بتقييـم التغيير المطلـوب بالتعـاون مع مدير التغيير، ويشمل ذلك الجوانب التالية:

- المالية.
- الفنية.
- الأثر على النشاط.

يؤخذ في الاعتبار أثناء التقييم كذلك توفر الموارد والجدولة. وعقب التقييم، يتم إبلاغ مدير التغيير فيما إذا كان ينصح باعتماد طلب التغيير. وإذا اعتمد طلب التغيـير، يتم إحالته للتخطيط والتنفيذ والاختبـار. أمـا في حال عدم اعتماده، يتم الـرد على منشئ طلب التغيير مع إيضاح سبب الرفض.

يقبل التغيير بناءً على اكتمال معلومات طلب التغيير. وتعاد طلبات التغيـير المرفوضـة إلى منشئيهـا مـع إيضاح الرفض. وفيما يلي الخطوات المتبعة في هذه المرحلة.

- مراجعة طلب التغيير للتأكد من اكتمال معلوماته.
- قبـول أو رفض طلـب التغيـير بناءً علـى اكتمـال المعلومات الإلزامية.
- توقـع وجـود مقاومـة للتغيـير، واستخـدام أدوات وأساليـب لمكافحة المقاومة للتغيير (فضلاً راجع الملحق-٢ للإطلاع على الأدوات والأساليب المستخدمة في مكافحة المقاومة للتغيير).

### ٣.٣. تحديد فئات التغيير

يقـوم محلـل التغيـير بتقييـم التغيير بالتعـاون مع مديـر التغيير لتحديـد فئـة التغيير، (طفيـف، أو جوهـري، أو رئيسي). ويمكن تحديد ذلك بطرح عدد من الأسئلة مثل:

- مـا هي السياسـة التي سيتـم تغييرها، أي تحديـد فيما إذا كانت السياسة موجودة.
- مـن هم المستخدمون الذين سيتأثرون من هذه السياسة، أي هل هم مدراء أم موظفين.
- ما هـو الإجراء الذي سيتم تغيـيره، أي تحديد فيما إذا كان الإجراء موجود بالفعل.
- مـن هم المستخدمون الذين سيتأثـرون من هذا الإجراء، أي هل هم مدراء أم موظفين.

- مـا هي التغييرات التقنية المطلوب تنفيذها ضمن الإعدادات الحالية لتقنية المعلومات.
- هـل سيتم تنفيـذ الأجهزة (العتـاد) و/أو البرامـج في بيئة الإنتـاج كمتطلـب سابـق لدعـم السياسـات والإجـراءات الجديدة.

## ٣.٤. اختبار التغيير

يتعين اختبار التغيير في حالات معينة عندما يتعلق الأمر بتطبيقات وأنظمة. ويستخدم محلل التغيير بيئة اختبار بمساعدة إدارة تقنية المعلومات لنشـر التغييرات المطلوبة الراميـة إلى تطبيق سياسات وإجراءات معينة.

وسيؤدي اختبار التغيير إلى حصول المحلل على المخرجات التالية:

- المشاكل المحتملة.
- أوجه القصور في الأجهزة.
- أوجه القصور في البرنامج.
- مرئيات وردود المستخدمين.

## ٣.٥. اعتماد التغيير

تكـون لجنة التوجيـه مسئولة عن الأخذ في الاعتبـار المخاطر التي قـد تلحـق بـ (اسم الجهـة) جـراء أي تغيير. وفي سيـاق الأعمال الاعتياديـة، يقـوم مديـر التغيـير بتعيين فئـة التغيـير (طفيف، جوهـري، رئيسي) وذلـك بالتعاون مع محلـل التغيير. وتحدد فئة التغيير المستـوى الإداري المشمول في تقييم التغيير. وبعد التقييم، يتـم إبلاغ لجنة التوجيه فيمـا إذا كان يتعين اعتماد التغيير. ويتم إمـا قبـول التغيير والمضـي قدماً فيـه، أو رفضه وإيضـاح أسباب الرفض لمنشئ التغيير.

- يقـوم مديـر التغيير بتقييم المـوارد وأثر التغيـير على البنية التحتيـة لتقنية المعلومات بالرجـوع إلى السياسات، وجدولة التغيـير مـن الفئـة الطفيفـة بنـاءً علـى اتفاقيـات مستوى الخدمة، وتبليغ لجنة التوجيه بالإجراء المتخذ.
- يقـوم مدير التغيـير بتمرير طلب التغيير علـى أعضاء لجنة التوجيه لتقييمه قبل الاجتماع الرسمي للجنة.
- يحيل مدير التغيير طلب التغيير إلى المسئول التنفيذي الأعلى لتقييمـه من ناحية النشاط ومن الناحية المالية، ويقوم مدير التغيير كذلك بإبلاغ لجنة التوجيه.
- يقـوم المسئـول التنفيـذي الأعلـى بالمصادقـة علـى طلـب التغيـير الذي فئته (جوهـري أو رئيسي) أو رفضه. إذا تمت المصادقـة على طلب التغيـير، يتم إرسالـه إلى لجنة توجيه أمن المعلومات.
- يقوم أعضـاء اللجنة بتقييم الموارد وأثـر التغيير على البنية التحتيـة لتقنيـة المعلومـات بالرجـوع إلى قاعـدة بيانـات الإعدادات واتفاقيات مستوى الخدمة، حسب اللزوم.
- تبلّغ لجنـة التوجيه مدير التغيير بقبـول التغيير على البيئة، وبدرجة أولويته، وجدول التنفيذ.
- أما إذا تم رفض طلب التغيير، فيتم إقفاله وتسجيله مع ذكر أسبـاب الرفـض. ويكون لمنشئ التغيير الحـق في الاعتراض والاستئناف.

### ٣.٦. تغيير الخطة والجدول

تعـاد التغيـيرات المعتمدة إلى مديـر المشروع من أجـل التخطيط والتنفيـذ. يساعد مدير التغيير في تنسيق، وتبليغ، وجدولة التغيير المعتمـد. ويتأكد كذلك مـن الإعـداد والتوثيق المسبـق لإجراءات التراجـع عـن التغيـير أو خطـط التصحيـح والإصـلاح. بعد أن يستكمـل مديـر المشروع التخطيـط والجدولة بمـا في ذلك إعداد جـداول العمـل للتغيـير، فـإن عليه الحصـول علـى مصادقة من مديـر التغيير أو لجنـة التوجيه قبل التنفيذ الفعلـي للخطة. وبعد المصادقـة على خطة المشروع يقـوم مدير المشـروع بتوزيعها على جميع الأطراف المعنية، ويبلّغ عن البدء في تنفيذ التغيير.

### ٣.٧. تنفيذ التغيير

يتم تعيـين مهمة محددة لـكل موظف مشـارك في العملية، ويكون مديـر المشـروع مسئولاً عـن التأكد مـن تنفيذ جميع المهـام وفقاً للخطة، ويجـب التبليغ عن أية مخالفات أو خروج على الخطة إلى لجنة التوجيه.

تراقـب لجنـة التوجيه تقـدم سير العمـل في طلـب التغيير طوال هـذه العملية، وتشرف على كامل عمليـة التنفيذ، فيما يقوم مدير المشروع بالتشاور مع مدير التغيير أثناء عملية التنفيذ لتحديد أية خروج عن خطة تنفيذ طلب التغيير المعتمد.

وبعـد التنفيـذ، يقـرر مديـر التغيـير فيمـا إذا تحققـت النتائج المتوخـاة، ويقـرر مديـر التغيير فيمـا إذا كان سيتـم تفعيل خطة التراجع عن التغيير.

### ٣.٨. المراجعة

يراجـع مدير التغيير طلب التغيير وفقـاً لسياسة مراجعة الأعمال بعد تنفيذها:

- بعد فترة محددة مسبقاً، يجري مدير التغيير مراجعة ما بعد التنفيـذ طبقاً لسياسة مراجعة الأعمـال بعد تنفيذها. ويتم تدويـن النتائج في طلب التغيير، وعرضها على لجنة التوجيه للإطلاع والمراجعة.
- تستخـدم النتائج كمدخلات لأنشطـة التحسين لعملية إدارة التغيير.
- إذا لم تكـن نتائـج مراجعـة الأعمال بعد تنفيذهـا مرضية، يقـوم أعضـاء لجنـة التوجيه بإعـادة فحص طلـب التغيير الأصلـي، ويقرروا الإجراءات المتعـين اتخاذها. وقد تتضمن تلـك الإجـراءات طلب تقديم طلـب تغيير جديد بعـد إقفال طلب التغيير الأصلي.
- أمـا إذا كانت النتائج مرضية، فيتم تغيير حالة طلب التغيير إلى «مقفل».

## ٤. مقاومة التغيير – الأدوات والأساليب المستخدمة في إدارة التغيير

عنـد تنفيذ أي برنامج ضخم، فإن مقاومة التغيير قد تنطوي على تهديد كبير لنجاح التغيير المزمع. وفي معظم الحالات، فإن مفتاح التغلب على المقاومة و/أو إدارة التغيير هو تحقيق أهداف التغيير.

أدكار (ADKAR) هـو أحـد أنظمـة مقاومـة التغيـير القائم على تحقيـق الأهداف، ويتيح لفرق إدارة التغيـير تركيز أنشطتها على تحقيـق نتائج محـددة للجهة الحكوميـة. هذا علمـاً أن الأهداف والنتائـج المحددة في نظام (أدكار) هي تسلسلية وتراكمية. ويجب

على مدير التغيير الحصـول على كل عنصر بالتسلسل كي يتسنى تنفيذ التغيـير والحفاظ على استمراريته. ويمكـن استخدام هذا النظـام لتحديد الفجوات في عمليـة إدارة التغيير، وتقديم تدريب فاعل لموظفي الجهة. ويمكن استخدام نظام (أدكار) فيما يلي:

- تشخيص مقاومة الموظفين للتغيير.
- مساعدة انتقال الموظفين عبر عملية التغيير.
- إعـداد خطة عمل ناجحة للتقـدم الشخصي والوظيفي أثناء التغيير.
- تطوير خطة إدارة التغيير للموظفين.

ولـدى نظـام (أدكار) القـدرة على تحديـد سبب انعـدام فاعلية التغيير، والمساعدة على اتخاذ الخطوات اللازمة لإنجاح التغيير.

### ٤.١. التوعية

تهـدف التوعية إلى إيصال جميع الموظفين من كافة المستويات إلى إدراك سبـب الحاجـة إلى التغيير. ويجـب أن يفهم موظفو الجهة أن التغيير المنفذ يهدف إلى تحسين مستوى أمن أصول المعلومات، وهو ما يؤدي في نهاية المطاف إلى النجاح.

### ٤.٢. الرغبة

تلتـزم الإدارة بتشجيع الرغبة لـدى موظفيها لدعم التغيير المزمع والمشاركـة فيه بفاعلية، بصـرف النظر عما إذا كانت العمليات أو الإجراءات الجديدة تبدو جذابة أو براقة.

### ٤.٣. المعرفة

يجـب أن تقـدم الإدارة التدريـب والتعليـم لموظفيها بشـأن طرق التغيـير إلى السياسـات والإجـراءات الجديـدة ووظيفـة أمـن المعلومـات الجديدة. هذا علماً بأنه لا طائـل من تحقيق مستويات عالية من الوعي والرغبة إذا لم تكن مصحوبة بالمعرفة الضرورية لكيفية تأثير التغيير على تحقيق الأهداف المرجوة.

### ٤.٤. القدرة

إلى جانـب المعرفـة بكيفيـة إحـداث التغيـير الناجـح، فيتعين أن يحصـل كل شخـص مشـارك في العمليـة علـى التدريـب المحدد والمعلومـات اللازمة لتحقيق النجاح في تنفيـذ التغييرات المحددة بالتفصيل. وتُعَد ورش العمل والتدريب عبر الإنترنت من العناصر الهامـة لتقديم التعليم للموظفين الذين هم بحاجة لذلك من أجل إنجاح التغييرات.

### ٤.٥. التعزيز

لكـي يتسنـى تنفيـذ التغيـير بنجـاح، ينبغـي علـى الإدارة العليا استخـدام أسلـوب التكـرار والتعزيـز، فـإذا كرر الموظـف المهمة أو العمـل لفـترة طويلة، مثـلاً لمدة شهـر بشكل دقيـق، فستصبح لديه عادة، وتعزيـز "العادات" الجديـدة للموظفين سيحسن من نجـاح التغييرات المنفـذة. ويمكن تحقيق هـذا التعزيز من خلال الترقيات، والتقييم، واتباع أساليب تحفيزية مختلفة.

إن التركيـز علـى التوعيـة، والرغبـة، والمعرفة هـي القاعدة التي تشـكل أساسـاً لقبـول التغيـير والقـدرة علـى تنفيـذ السياسات والإجـراءات الجديدة بنجاح. وباستخدام تلك القاعدة الأساسية والمتابعة، والتعزيز، يمكن التغلب على التردد في قبول التغيير الذي يعتبر من السمات الشخصية الإنسانية، وهو الأمر الذي من شأنه خلق جهود جماعية قوية للقيام بالأعمال التطويرية القادمة بشكل سلس وبغاية النجـاح. إن تطبيق نظـام (أدكار) بشـكل مناسب يـؤدي في العـادة إلى إدارة التغيـير بشـكل يخلـو مـن الصدمات والضغوط والإحباطات.

الجزء الخامس

# الخطة التوعوية لسياسات وإجراءات أمن المعلومات

## ١. مقدمة

يعــزز برنامــج التوعية بأمن المعلومات من فاعلية الضوابط الأمنية التي تم إنشاؤها وتنفيذها مسبقًا، ولا شك أن وعي الموظفين بالمسئوليات الأمنية الملقاة على عاتقهم يشكل رادعا قويا ضد التهديدات المعروفة والمجهولة على حدٍ سواء.

تعرض هــذه الوثيقة العملية والمنهج اللــذان يجب على (اسم الجهة) إتباعهما عنــد تنفيذ ومتابعة برنامج التوعيــة الأمنية. وتبيّن الوثيقة الأدوار والمسئوليات في إطار برنامج التوعية الأمنية، كما تبين عناصر وجداول النماذج الخاصة بالبرنامج.

## ٢. نظرة عامة

يشكل برنامج التوعية بأمن المعلومات عنصرًا مهمًا لنجاح تنفيذ برنامج أمن المعلومات.

يجب أن تسير خطة التوعية التي وضعها المسئول برنامج التوعية بأمن المعلومات في (اسم الجهة) على خطى النهج السليم لإدارة المشاريع بغية تحقيق أفضل النتائج. يتألف البرنامج من المراحل الخمسة الموضحة أدناه:

- بدء برنامج التوعية بأمن المعلومات.
- التخطيط لبرنامج التوعية بأمن المعلومات.
- تنفيذ برنامج التوعية بأمن المعلومات.
- المراقبة والتحكم في برنامج التوعية بأمن المعلومات.
- إنهاء برنامج التوعية بأمن المعلومات واستعراض النتائج.

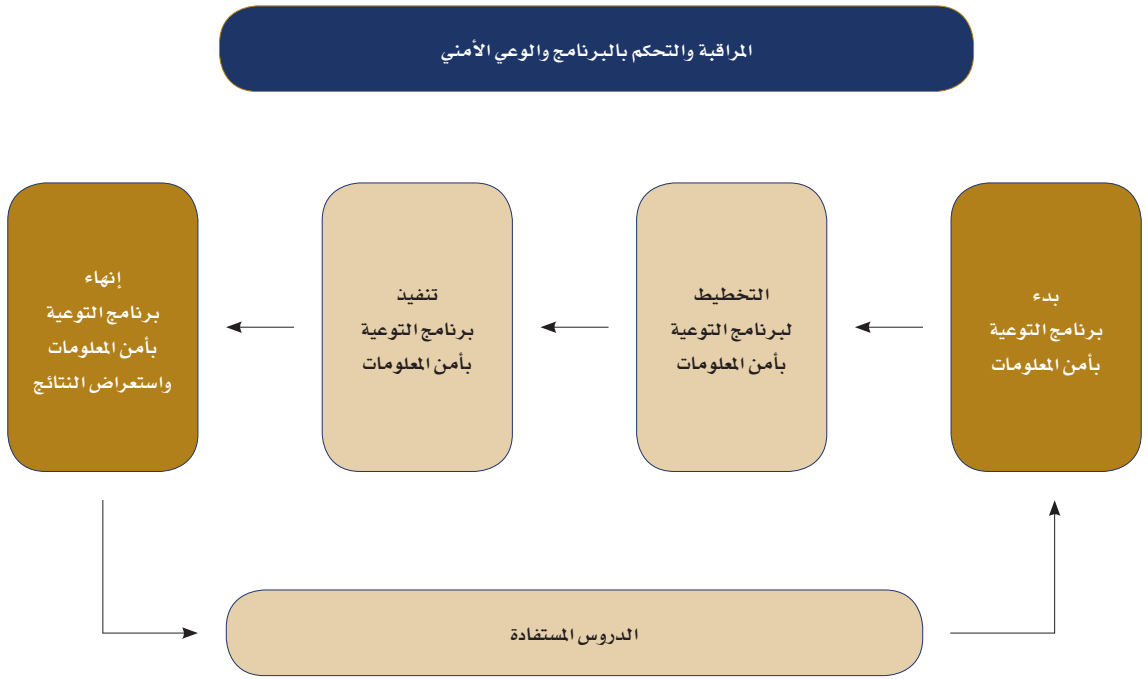
يتيح هذا النهج لـ (اسم الجهة) وضع برامج تدريبية تتفق مع متطلباتها لأقصى قدر ممكن، فضلاً عن تقديم منتجات ذات جودة عالية في موعد زمني محدد، ومراقبة مدى فاعلية برنامج التوعية بأمن المعلومات.

## ٣. منهج برنامج التوعية بأمن المعلومات

يوضح هذا القسم مجريات العملية الإجمالية والعمليات الفرعية الخاصة بتعميم برنامج التوعية بأمن المعلومات، علمًا بأنه ينبغي إتباع نهج سليم لإدارة المشاريع لتنفيذ البرنامج وتعميمه في إطار زمني محدد.

بمـا أن التوعيـة بأمن المعلومات عملية مستمرة بطبيعتها، فـإن البرنامج يعمل ضمن خطة تشغيلية لمدة ١٢ شهـرًا، حيث تستعرض النتائج بصفة مستمرة، وتحدد التعديلات / التحسينات المطلوبة بالنظر إلى أهداف خطة التوعية ونطاقها في المرحلة التالية من عملية التوعية.

الشكل (١)



## ٣.١. بدء برنامج التوعية بأمن المعلومات

تمثـل هذه المرحلة بداية البرنامــج، والهدف الرئيسي منها هو تحديد النطاق والأهداف والقيود، وتحديـد الأدوار والمسئوليات ذات الصلة ببرنامج التوعية بأمن المعلومات. ويعتبر عنصر "إدارة المشاريع" أحد أهم عوامل النجاح في هذه المرحلة.

### ٣.١.١. تحديد الأدوار والمسئوليات

يجب تحديد الأدوار والمسئوليات وتعيينها بوضوح تام. يرجى الرجوع إلى المحلق ١ للاطلاع على المزيد من التفاصيل.

### ٣.١.٢. تحديد مدير المشروع

يتـولى مديـر المشروع إدارة جميـع مراحل المشروع، ويدخل في مهام عملـه تحديد نطاق البرنامج وميزانيته وخطـة إدارته. كما يقوم مدير المشروع برصد معدل تقدم البرنامج واستيعاب القيود التي قد تعرقل إدارة البرنامج بسلاسة. كما تتضمن مهامه البدء في عملية الحصول على الموافقات المطلوبة للبرنامج.

### ٣.١.٣. تحديد متطلبات برنامج التوعية بأمن المعلومات لدى الجهة

تتوقف متطلبات برنامج التوعية بأمن المعلومات على تحديد الاحتياجات وتقويم الجهود وترتيب الأولويات بالنسبة لخطط التدريب:

#### ٣.١.٣.١. تحديد الاحتياجات

ينبغـي رصـد نتائج البرامج المطبقة مسبقًا أو تقييم الوضع الحالي استنادًا إلى الوضع الأساسي أمن المعلومات. ويعقب ذلك إعداد برنامج تدريبي مكثف لمعالجة القصور المعرفي.

مثـال علـى ذلك، المعرفة الأمنية في مجال محـدد مثل (التحكم في الوصول) تقل عن الحد الأدنى لقيمة الوضـع الأساسي. أو مثال آخر أن عمليات التدقيق الداخلية/ الخارجية الأخيرة كشفت عن نتائج بالغة الأهمية في مجالات السياسية شديدة المخاطر.

ينبغـي تحديـد أهم السياسات بناء على الأثر المترتب على الافتقار إلى التوعية بأمن المعلومات، وستتضمن الموضوعات –على سبيل المثال لا الحصر– المجالات التالية:

الجدول ١

| إدارة الأمن | تصنيف المعلومات | إدارة المخاطر | الأمن المادي (والبيئي) |
|---|---|---|---|
| أمن الموظفين | التدريب للتوعية بأمن المعلومات | الاستجابة للحوادث الأمنية | مراقبة مستوى الأمن |
| أمن الشبكة | أمن محطات العمل / الحواسيب الشخصية | الدعم والأمن التشغيلي ذي الصلة | التشفير وسرية المعلومات |
| أمن الوسائط | آليات الكشف عن الهوية والتحقق | أمن دورة الحياة بالنظم المختلفة | التخطيط لاستدامة الأعمال |

### ٣. ١. ٣. ٢. ترتيب أولويات مجالات التوعية

يجب أن ترتب (اسم الجهة) أولوياتها من حيث مجالات التدريب، ويتضمن التدريب مستويين هما: أساسي ومكثف. أما التدريب الأساسي فيشمل جميع أعضاء فريق العمل ومقاولو الطرف الثالث وقسم الموارد البشرية / الإدارة. وأما التدريب المكثف فيشمل موظفي أمن المعلومات وموظفي عمليات تكنولوجيا المعلومات، إضافة إلى تدريب الموردين و/أو تدريب آخر للمتخصصين.

يرجى الرجوع إلى الجدول ٢ للاطلاع على مجالات التدريب المكثف.

إنه من الضروري إخضاع موظفي أمن المعلومات للتدريب المكثف قبل الشروع في البرنامج الأساسي أو المكثف للتوعية المقدم لفريق عمل تكنولوجيا المعلومات.

## ٣. ١. ٤. تحديد أهداف البرنامج

تعد أهداف التوعية بأمن المعلومات أهدافًا رفيعة المستوى لتقود البرنامج، وتحدد (اسم الجهة) هذه الأهداف. ويجب أن يركز البرنامج بادئ الأمر على رسائل أمنية محددة تطرح بشكل متسلسل يمكّن العاملين في (اسم الجهة) من إحراز تقدم واضح في تعلم السياسات الأمنية واستيعابها وتطبيقها على أنشطة الأعمال اليومية. يجب أن تكون الأهداف المحددة قابلة للقياس في نهاية البرنامج.

مثال: أن يفهم ويستوعب ٧٠٪ من فريق العمل الرسالة الأهم من حملة "سياسة كلمات المرور".

## ٣. ١. ٥. تحديد نطاق البرنامج

يركز نطاق البرنامج على تحديد الجمهور المستهدف والأدوات المقرر استخدامها في البرنامج.

### ٣. ١. ٥. ١. من هو الجمهور المستهدف؟

إن تحديد الجمهور المستهدف يعد أمرًا مهمًا لأنه يجب إعداد برامج التوعية على نحو يلبي متطلبات محددة وملائمة لهذا الجمهور.

يصنف الجدول التالي الجمهور المستهدف وبيّن المجالات التي يتوجب التركيز عليها في برنامج التوعية لكل مجموعة.وهو ما تحتاجه (اسم الجهة) لتحقيق الأهداف المراد بلوغها من برنامج التوعية بأمن المعلومات.

الجدول ٢

| الجمهور المستهدف | المجال الذي ينبغي التركيز عليه في برنامج التوعية |
|---|---|
| الإدارة العليا | مسئوليات إدارة الأمن، وتأييد المبادرات الأمنية ودعمها، ومراجعة مدى تقدم البرنامج وفاعليته. |
| إدارة أمن المعلومات والموظفون | الإطار والسياسات والإجراءات والمعايير ذات الصلة بأمن المعلومات، وتدقيق أمن المعلومات واستدامة الأعمال ومعالجة الكوارث. |
| الجمهور العام | السياسات الأمنية لدى (اسم الجهة)، وسياسة الاستخدام المقبول والإبلاغ عن الحوادث. |
| إدارة عمليات تكنولوجيا المعلومات وموظفو تكنولوجيا المعلومات | المسئوليات الأمنية، واختبار خطة الحفاظ على استمرارية العمل وإجراءات التعافي من الكوارث. |
| المقاولون / الاستشاريون | المسئوليات الأمنية. |
| إدارة قسم الإدارة والموظفون | سياسات السلامة المادية وإجراءاتها، وإجراءات الحفاظ على استمرارية العمل. |
| إدارة قسم الموارد البشرية والموظفون | المسئوليات الأمنية، وإجراءات التعيين الوظيفي/ إنهاء التوظيف، والإجراءات التأديبية. |

### ٣. ١. ٥. ٢. ما الأدوات المقرر استخدامها في البرنامج؟

ثمة عدد من الأدوات التي يمكن إدراجها في برنامج التوعية بأمن المعلومات كما هو موضح في الجدول ٣. وعلى المدى البعيد، يجب الاستعانة بمجموعة من الأدوات لأي نطاق من نطاقات السياسات بغية المحافظة على مصلحة المستخدم النهائي وتحسين إمكانية التعلم.

تصف الجداول التالية مختلف الأدوات وتكلفتها النسبية، فضلاً عن المعدل المقترح لتكرار استخدامها.

جدول ٣

| المكونات | الوصف |
|---|---|
| أدوات التوعية في عموم الجهة الحكومية | ينبغي تصميم أدوات التوعية التالية المقرر استخدامها في عموم الجهة وتنفيذها:<br>• **رسالة المحافظ:** توضح هذه الوثيقة ما تترقبه (اسم الجهة) من موظفيها فيما يتعلق بأمن المعلومات.<br>• **كتيب الموظف:** تقدم هذه الوثيقة الإرشادات الأساسية لأمن المعلومات لجميع موظفي (اسم الجهة).<br>• **وحدة التعلم الإلكتروني:** بناء على متطلبات أمن المعلومات لدى (اسم الجهة)، يمكن استحداث وحدة تعليمية إلكترونية، على أن تقدم هذه الوحدة معلومات مفصلة حول العديد من الموضوعات المتعلقة بأمن المعلومات مثل النسخ الاحتياطي والبريد الإلكتروني وإدارة الحوادث واستخدام الإنترنت والحماية من الفيروسات وسرية البيانات، إلخ.<br>• **الأسئلة الشائعة:** ستشكل الأسئلة الشائعة مرجعا سريعا ليحصل الموظفون على معلومات للاستفسارات المتعلقة بأمن المعلومات. يجب استخدام موقع على شبكة الإنترانت للجهة يتم فيه استضافة هذه الأسئلة الشائعة لتصبح في متناول الجميع. |
| المطبوعات الداخلية | يمكن أن تقوم (اسم الجهة) بنشر رسائل التوعية من خلال مجموعة من المطبوعات الداخلية المتعلقة بالموضوعات التي تحظى بأكبر قدر من الاهتمام.<br>أما المنشورات الداخلية التي يمكن تصميمها لهذا الغرض، فهي كالتالي:<br>• **الملصقات وشاشات التوقف:** تجذب الملصقات وشاشات التوقف انتباه الموظفين إلى الأمور الأساسية المتعلقة بأمن المعلومات، وينبغي أن تخضع الملصقات للتغيير باستمرار حتى يستمر الأثر المرجو منها. إضافة إلى ذلك، يجب أن تتمتع الملصقات بقدر من الاحترافية في عرضها وتتوافق مع الملصقات الأخرى الموجودة بالمؤسسة.<br>• **الكتيبات والمنشورات:** ينبغي أن تُعد (اسم الجهة) الكتيبات والمنشورات بحيث تضم رسائل مختصرة تجذب الانتباه فيما يتعلق بأمن المعلومات.<br>• **نشرة إخبارية لأمن المعلومات:** يمكن تصميم «نشرات إخبارية لأمن المعلومات» وإعدادها لنشر المعرفة المتعلقة بمختلف قضايا أمن المعلومات. مثال: أحدث ملصقات منشورة والتنبيهات الخاصة بوجود فيروسات / برمجيات ضارة وتنفيذ ضوابط أمنية جديدة في (اسم الجهة). |

| المكونات | الوصف |
|---|---|
| بوابة الإنترانت | تعد صفحة الويب على الإنترانت إحدى الآليات الجيدة التي تعرّف فريق العمل / المقاول بسياسات أمن المعلومات وإجراءاتها ومعاييرها والأسئلة المتكررة حولها والفحوص الخاصة بها.<br>يضاف إلى ذلك توفير جميع النشرات الداخلية سالفة الذكر على بوابة الإنترانت. |
| أدوات تقييم التوعية بأمن المعلومات | يجب على (اسم الجهة) تصميم نماذج أدوات التقييم وتنفيذها حتى يسهل قياس مستوى وعي الموظفين بأمن المعلومات بانتظام. ويجب إعداد نماذج الأدوات التالية باعتبارها جزءًا من هذه المرحلة:<br>• **الاستفتاءات:** تتضمن الاستفتاءات أسئلة تتعلق بأمن المعلومات إلى جانب السياسات والإجراءات المتبعة لدى (اسم الجهة) فيما يتعلق بأمن المعلومات في مجالات بعينها.<br>• **الأسئلة والألغاز:** ترتبط الأسئلة والألغاز بالمجالات المتعلقة بأمن المعلومات، ومن شأنها مساعدة (اسم الجهة) في قياس مستوى وعي الموظفين بأمن المعلومات.<br>• **نماذج الأوضاع الأساسية:** تعد النماذج كبطاقات قياس الأداء التي تستخدم لقياس مستوى وعي الموظفين بأمن المعلومات. وسيتم استخدام هذه النماذج قبل تنفيذ البرنامج وبعده لقياس مدى فاعليته.<br>ويمكن استخدام بوابة الإنترانت استخدامًا مكثفًا لهذا الغرض. |
| العروض التقديمية | ستتولى (اسم الجهة) تصميم محتوى دورة التوعية بأمن المعلومات وإعداده بحيث يشمل فئات الجمهور المستهدف التالية:<br>• الإدارة العليا: يتضمن العرض التقديمي للإدارة العليا رسائل أكثر شمولاً وإيجازًا للتوعية بأمن المعلومات.<br>• الأعضاء الجدد: يتضمن هذا العرض التقديمي أساسيات أمن المعلومات وممارسات أمن المعلومات المعمول بها لدى (اسم الجهة).<br>• المدربين: يراد من هذا العرض التقديمي تدريب المدرب حتى يتسنى له تعليم جميع موظفي (اسم الجهة) بصفة مستمرة.<br>• ويمكن استخدام بوابة الإنترانت بصورة فعالة للمحافظة على الأرشيف المتاح على الشبكة الخاص بهذه العروض التقديمية حتى يتسنى الرجوع إليها لاحقا. |

## طرق التقديم

الجدول ٤

| الأدوات والأساليب | مستوى التكلفة المتوقعة | معدل التكرار المقترح | أمثلة |
|---|---|---|---|
| الملصقات | منخفض | سنويا | إتاحة مجموعة من الملصقات وتجديدها سنويًا.<br>وينبغي عرض مجموعة من الملصقات المصممة بعناية بحيث تضم ما قل ودل فيما يخص مجموعة متنوعة من قضايا أمن الحاسوب. وستؤتي الملصقات الغرض المرجو منها عند وضعها في الأروقة والمطاعم ولوحات النشرات والاستراحات الخاصة بالمؤسسة، إلخ. |
| النشرات الإخبارية/ المقالات | متوسط | شهريا | تخصيص نشرات إخبارية شهرية لمواضيع أمن المعلومات، ويمكن تخصيصها بحيث تحمل اسم وشعار (اسم الجهة). |
| شبكة الإنترانت | منخفض | تحديث أسبوعي | موقع الإنترانت (البوابة الداخلية) يمثل مصدرًا مفيدًا لتعميم سياسات أمن المعلومات المعمول بها لدى (اسم الجهة). |
| البريد الإلكتروني والصوتي | منخفض | ربع سنوي | نشر رسائل بسيطة المحتوى عبر البريد الإلكتروني (أو البريد الصوتي) لتنبيه العاملين إلى القضايا المرتبطة بأمن المعلومات داخل الأماكن المختارة أو المباني أو المكاتب. |
| المواد الترويجية | متوسط | غير محدد | طباعة شعارات أو رسائل برامج التوعية بأمن المعلومات مثل بعض المواد الترويجية مثل لوحات الماوس والأقلام والأكواب والكؤوس البلاستيكية، إلخ. |
| مواد التوعية الداخلية | منخفض | غير محدد | طابعة شعار برنامج التوعية بأمن المعلومات على الدفاتر / المفكرات / بعض الوثائق المطبوعة والخاصة بـ (اسم الجهة)، مثل كشف المرتب. |
| العروض التقديمية / دورات التوعية | منخفض | مرتان شهريًا أو سنويًا | يكمن عقد دورات التوعية بأمن المعلومات مرة أو مرتين شهريًا حسب عدد الحضور، علمًا بأن حضور الموظفين الجدد أمر إلزامي.<br>ويتعين حضور الموظفين الحاليين مرة واحدة في العام. |

## ٣. ٢. التخطيط للتوعية بأمن المعلومات

يحين تشكيل فريق المشروع وإعداد الميزانية والجداول الزمنية أثناء هذه المرحلة، إلى جانب استحداث مقياس الوضع الأساسي القائم.

### ٣. ٢. ١. تشكيل فريق لتنفيذ برنامج التوعية بأمن المعلومات

يجب أن يكون أعضاء الفريق الذين يقع عليهم الاختيار على دراية جيدة بأمن المعلومات، كما يجب أن يتحلوا بمهارات العرض وحسن التعامل مع الآخرين.

سيعتمد اختيار الكوادر المناسبة لفريق التنفيذ على الأسلوب المحدد لتقديم التوعية، وفيما يلي بيان بالمهارات والكفاءات التي يجب توفرها في الكوادر.

الجدول ٥

| مجموعة المهارات / الكفاءة | الوصف |
|---|---|
| المعرفة بأمن المعلومات | خبير في جميع مجالات أمن المعلومات. |
| مهارة المراجعة / تحليل الجودة | ضمان جودة جميع المسودات بتحليل الأخطاء اللغوية والفنية. |
| مهارات الوسائط الإلكترونية (الاستعانة بجهات خارجية إذا لزم الأمر) | المهارات المطلوبة لإعداد الوثائق والتصاميم ووسائط الفلاش ومحتوى البريد الإلكتروني وشاشات التوقف ومقاطع الفيديو. |
| الوسائط المطبوعة (الاستعانة بجهات خارجية إذا لزم الأمر) | المهارات المطلوبة لإعداد الكتيبات والملصقات والتقاويم، إلخ. |

#### ٣. ٢. ١. ١. تطوير الأوضاع الأساسية

يجب تطوير الأوضاع الأساسية والتي يُستَند إليها كآلية لاختبار مدى كفاءة الوسائل المحددة لتقديم التوعية الأمنية. على سبيل المثال، أعرب ٧٠٪ من الموظفين الجدد الذين حضروا دورات التوعية بأمن المعلومات عن انطباعات إيجابية.

### ٣.٢.١.٢. وضع خطة للتوعية بأمن المعلومات (في شكل جدول زمني)

يجب وضع جدول زمني يحتوي على مراحل واضحة فيما يتعلق ببرامج التدريب بتوعية أمن المعلومات / والرسائل المقرر تعميمها على مختلف أصناف المستهدفين بالتوعية (على النحو المحدد أعلاه)، وتكرار الرسائل وتوقيتها والمحتوى التوعوي والقناة المستخدمة في ذلك. وينبغي تحديد كلٍ من هذه العوامل بعناية بالغة في ضوء مستوى التكلفة المتوقعة على ميزانية التوعية الخاصة بالجهة الحكومية.

نموذج خطة التوعية مرفق بالملحق ١

### ٣.٢.١.٣. وضع ميزانية التوعية بأمن المعلومات

يجب على مدير المشروع إعداد ميزانية في حدود المخصصات المالية السنوية لأنشطة التوعية بأمن المعلومات.

يقدم الجدول ٦ مثالاً توضيحياً للميزانية (هذا المثال للتوضيح ولا يمثل التكاليف الفعلية)

الجدول ٦

| عنصر الميزانية | عدد الوحدات | تكلفة الوحدة | إجمالي التكلفة |
|---|---|---|---|
| مقاطع الفيديو الخاصة بالتوعية بأمن المعلومات | ٩٩ | ٩٩٩ ريال سعودي | ٩٩٩٩٩ ريال سعودي |
| ملصقات التوعية بأمن المعلومات | ٩٩ | ٩٩٩ ريال سعودي | ٩٩٩٩٩ ريال سعودي |
| نشرات إخبارية ربع سنوية حول أمن المعلومات – ٤ نسخ | ٩٩ | ٩٩٩ ريال سعودي | ٩٩٩٩٩ ريال سعودي |
| التصميم المبدئي للمواد التي ستعرض على الموقع الخاص بأمن المعلومات | ٩٩ ساعة من العمل بنظام الدوام الكامل | | ٩٩٩٩٩ ريال سعودي |
| عضوية منظمة أمن نظم المعلومات لـ ٩٩ من فريق العمل المركزي و٩٩ موظف من فريق العمل الإقليمي. | ٩٩ | ٩٩٩ ريال سعودي | ٩٩٩٩٩ ريال سعودي |
| إرسال بريد إلكتروني ذو محتوى أمني أسبوعيًا بالمجان من خلال معهد (SANS) | | | ٠ ريال سعودي |
| بدل المواصلات المستحق لفريق أمن المعلومات المركزي مقابل زيارة المواقع البعيدة لتقديم المساعدة في الدورات التدريبية | ٩٩ | ٩٩٩ ريال سعودي | ٩٩٩٩٩ ريال سعودي |
| جهود الموارد البشرية (الداخلية) | ٩٩٩٩ ساعة من العمل بنظام الدوام الكامل | | ٩٩٩٩٩ ريال سعودي |
| التدريب المتخصص | | | ٩٩٩٩٩ ريال سعودي |
| إجمالي النفقات المقدرة | | | ٩٩٩٩٩ ريال سعودي |

### ٣.٢.١.٤. الإعلام ببدء البرنامج

إعلام راعي المشروع بالموعد الرسمي لبدء البرنامج.

## ٣.٣. تنفيذ التوعية بأمن المعلومات

يتخلل هذه المرحلة إعداد جميع مواد التدريب ونشرها حسب الجدول الزمني. وفيما يلي بيان الأنشطة الرئيسة:

- إعداد مواد التدريب الخاصة بالبرنامج.
- مراجعة محتوى المادة وتعديلها إذا لزم الأمر.
- إجراء مراجعة على المسودات لضمان الجودة وتعديلها إذا لزم الأمر.
- تحديد النسخة النهائية لتعميمها.
- تقديم المواد بالوسائط والأدوات التي تم اختيارها.
- إجراء مراجعة نهائية لضمان الجودة واعتماد النسخة النهائية.
- تطبيق أداة تقديم التوعية.

### ٣.٤. المراقبة والتحكم في التوعية بأمن المعلومات

يخضع المشروع للمراقبة والتحكم طوال مرحلتي التخطيط والتنفيذ لبرنامج التوعية بأمن المعلومات، لذلك يجب رصد أية مشكلات أو عراقيل قد تخل بالجدول الزمني للبرنامج أو تعيق تحقيق أهدافه، واتخاذ الإجراءات التصحيحية المناسبة. ويجب إخطار لجنة التوجيه الخاصة بأمن المعلومات في حال رصدت أية مشكلات مستعصية. وفيما يلي بيان بعض الأنشطة الرئيسة في المراقبة والتحكم في التوعية بأمن المعلومات:

- رصد التقدم في البرنامج مقارنةً بقائمة المراحل الرئيسة للخطة.
- رصد العراقيل واتخاذ الإجراءات التصحيحية.
- تسهيل حل النزاعات وإخطار راعي البرنامج /لجنة التوجيه الخاصة بأمن المعلومات إذا تطلب الأمر مساعدة إضافية.
- تقديم تقرير عن حالة البرنامج بصفة شهرية لجميع الأطراف المعنية.

### ٣.٥. انتهاء برنامج التوعية بأمن المعلومات واستعراض النتائج

يتخلل هذه المرحلة الانتهاء من البرنامج وقياس مدى فعاليته مقارنة بالحد الأدنى الذي تحدد أثناء مرحلة التخطيط لبرنامج التوعية الأمنية. تتضمن الأنشطة الرئيسة لهذه المرحلة قياس مدى فاعلية التوعية وتحديثها وفقًا للدروس المستفادة.

### ٣. ٥. ١. قياس الفاعلية

الجدول ٧

| | |
|---|---|
| طريقة الاستفتاء | **اختيار حجم العينة**<br>يجب أن تغطي العينة ما لا يقل عن ١٥ – ٢٠٪ من حجم فريق العمل. |
| | **تحديد الموضوعات ذات الخطورة التي يجب أن يشملها الاستفتاء**<br>اختيار مجالات تتسم سياساتها بالمخاطر الشديدة أو الموضوعات التي تتسم بقلة مستوى وعي موظفي الجهة أو العاملين بها. |
| | إعداد الاستفتاء والحصول على الاعتماد من المسئول عن برنامج التوعية بأمن المعلومات. |
| | إجراء الاستفتاء وتحليل النتائج ومقارنتها بمقياس الحد الأدنى. |
| | **نشر النتائج**<br>يتولى المسئول عن برنامج التوعية بأمن المعلومات توزيع نتائج الاستفتاء على الأشخاص المعنيين وبسرية تامة. |
| | **إجراءات المتابعة**<br>تجميع كل النتائج باعتبارها ركيزة لتخطيط برنامج التوعية بأمن المعلومات في الأعوام القادمة. |
| الأساليب الأخرى | **تدقيق أمن المعلومات**<br>إجراء مراجعة للمكاتب لملاحظة ما إذا كانت كلمات المرور مكتوبة ومرسلة إلى الوحدات الطرفية الحاسوبية، وما إذا كانت الملفات السرية متروكة من دون ضوابط أمنية. |
| | **الهندسة الاجتماعية (Social Engineering)**<br>استخدام تقنيات الهندسة الاجتماعية مثل التنكر، واختبار ما إذا كان مكتب المساعدة أو الدعم الفني أو مكتب الاستقبال يتبع الإرشادات الأمنية أثناء تقديم المساعدة للعملاء. |

### ٣. ٥. ٢. تحديث الدروس المستفادة

على فريق المشروع بحث ومناقشة جميع الدروس المستفادة أثناء البرنامج، ودراستها بُغية الارتقاء بفاعلية التوعية بأمن المعلومات.

الجزء السادس

# خيارات تعيين موقع لإدارة أمن المعلومات في الهيكل التنظيمي

## ١. المقدمة

تقدم هذه الوثيقة خيارات تعيين موقع لإدارة أمن المعلومات في الهيكل التنظيمي. وتوضح الجوانب المختلفة التي تحدد ماهية وظيفة أمن المعلومات، والأدوار والمسئوليات الضرورية المطلوبة لتأسيس إدارة فاعلة لأمن المعلومات وفقاً للمعايير العالمية المتبعة.

## ٢. نظرة عامة

تقدم هذه الوثيقة نظرة عامة بخصوص الخيارات المختلفة والمتعلقة بتأسيس إدارة أمن المعلومات لدى (اسم الجهة)، وتوثق بالتفصيل الأدوار والمسئوليات المطلوبة ضمن إدارة أمن المعلومات، كما توضح هذه الوثيقة العمليات المطلوبة لتأسيس إدارة أمن المعلومات والتي تشمل المراحل التالية:

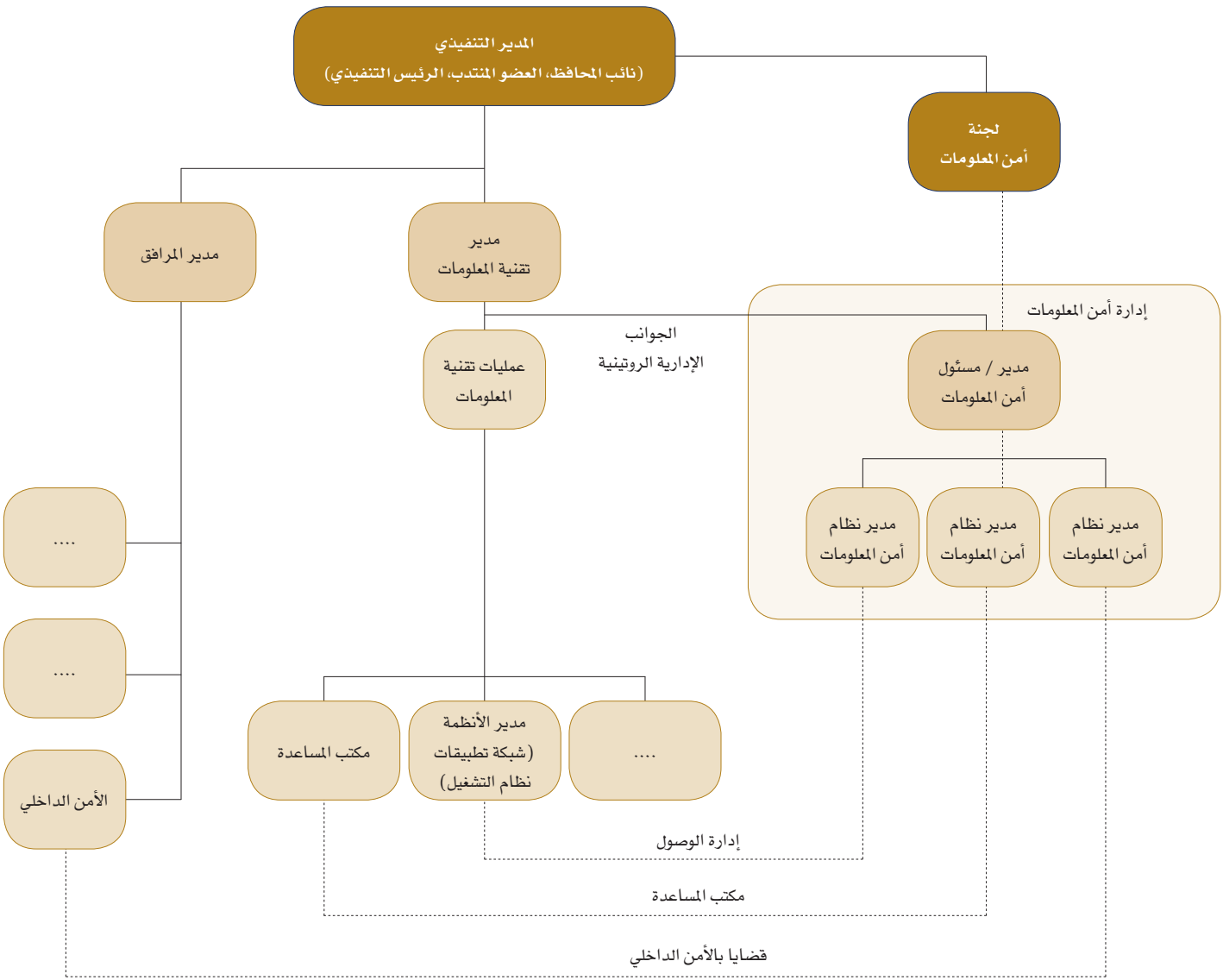
- البدء.
- التخطيط.
- التنفيذ.
- المراقبة والتحكم.

في ظل البيئة المعقدة لأنظمة المعلومات السائدة في هذه الأيام، تلعب عمليات أمن المعلومات دوراً هاماً من أجل التأكد من تكامل وسرية وتوفر البيانات الحساسة. وإن التوسع المتسارع في ترابط أنظمه الحاسب الآلي، والزيادة المضطردة في استخدام تقنيات الإنترنت قد أوجدا تغيير إيجابي في طريقة تواصل الجهات الحكومية ومزاولتها لأعمالها. غير أنه مع هذا التقدم التقني، فقد ظهرت ثغرات أمنية تسببت في زيادة مخاطر فقدان المعلومات الحساسة. وبالنظر لهذه المخاطر، ينبغي أن تدرك الجهات الحكومية حاجتها لوجود إدارة أمن معلومات لتراقب وتتحكم بالمخاطر والتهديدات المحيطة بأمن المعلومات. وكما هو الحال في الإدارات والأقسام الأخرى، فإن أمن المعلومات ينطوي على مهمات وظيفية رئيسية ينبغي تخطيطها وتطويرها وتنفيذها ومراقبتها والتحكم بها.

## ٣. خيارات تعيين موقع لإدارة أمن المعلومات في الهيكل التنظيمي

بناءً على حجم ودرجة تعقيد الجهة الحكومية، توجد ثلاثة خيارات متاحة لتعيين موقع لإدارة أمن المعلومات في الهيكل التنظيمي. وقد تم تضمين الوصف التفصيلي والإيجابيات والسلبيات لكل من هذه الخيارات. كما تم تضمين التوصية المتعلقة بكل خيار، وعلى الجهة المعنية قراءة وفهم هذه التوصيات بعناية.

## ٣.١. الخيار الأول



يلائم تصميم ووضع هيكلة الخيار الأول الجهات صغيرة الحجم ذات المخاطر المتدنية. ويجب بذل العناية اللازمة عند اختيار هذه الهيكلية لأنها قد تسبب تضارباً في المصالح. ويجب تحديد الفصل في المهام مع الأخذ في الاعتبار القيود المتعلقة بالحجم والميزانية لدى الجهة ذات العلاقة.

ضمن هذا الخيار، يكون مدير أمن المعلومات تابعاً للجنة أمن المعلومات، فيما تدار الجوانب الإدارية لأمن المعلومات تحت إشراف مدير تقنية المعلومات. ويمثل الخطوط الملونة المتقطعة الترابط المطلوب للتشاور بين الإدارات المختلفة ووظيفة أمن المعلومات.

وقد تم تقديم المزيد من الإيضاحات للأدوار المشمولة في الخيار الأول ضمن القسم ٤,١,١. وفيما يلي الإيجابيات والسلبيات الرئيسية لهذا الخيار :

### ٣.١.١. جدول: الإيجابيات مقابل السلبيات

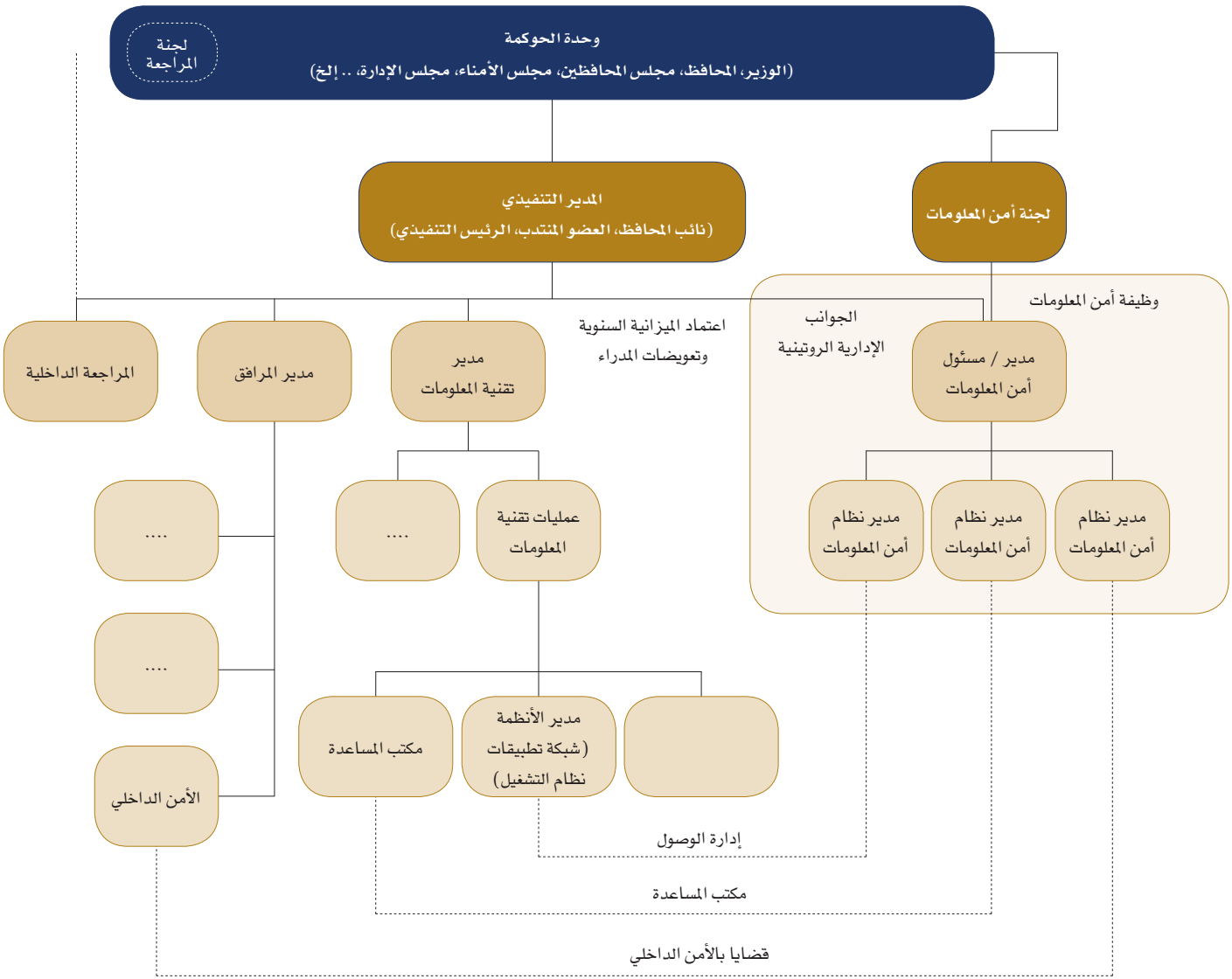
| الإيجابيات | السلبيات (على إدارة أمن المعلومات) |
|---|---|
| خفض التكاليف الكلية | انعدام الاستقلالية |
| خفض مقاومة التغيير | عدم دقة / عدم اكتمال التقارير والتبعية الإدارية |
| | عدم وجود فصل في المهام والواجبات |
| | أعباء عمل إضافية |
| | كفاءة أقل للأعمال |
| | قلة الخبرات |

يتضح من مزايا الخيار الأول أنه حل اقتصادي التكلفة، حيث يمكن أن تتشارك إدارتا في تقنية المعلومات وأمن المعلومات في الأدوار الوظيفية. كما ستكون هناك مقاومة أقل للتغيير الناتج عن تفعيل هذا الخيار، حيث أن الهيكل التنظيمي للمستويات العالية لدى الجهة المعنية لن يتغير بصورة كبيرة. غير أن السلبيات تصف إدارة أمن المعلومات على أنها تفتقر للاستقلالية لأنها تقع في ظل إدارة تقنية المعلومات، كما أن التبعية الإدارية تكون غير دقيقة وغير كاملة وذلك لكون التبعية الإدارية الروتينية ترجع إلى مدير تقنية المعلومات، الذي يتبع بدوره المدير التنفيذي. ويمكن لمدير تقنية المعلومات تصفية (حذف وإضافة) واختيار نوعيه التقارير المرفوعة بما تقتضي مصلحته، كما أن مدير امن المعلومات لن تكون لديه الصلاحية اللازمة لاتخاذ القرارات في تشجيع إجراء التغييرات التنظيمية المطلوبة والضرورية لإلزام إنفاذ سياسات وإجراءات أمن المعلومات.

### ٣.١.٢. الخلاصة:

بناءً على الإيجابيات والسلبيات المذكورة أعلاه، فإن الخيار الأول يلائم الجهات الأصغر حجماً والتي تواجه مخاطر عادية.

## ٣. ٢. الخيار الثاني



تم تصميم ووضع هيكلة الخيار الثاني للجهات متوسطة الحجم التي تواجه مخاطر متوسطة. ويجب تحديد فصل واضح للمهام والواجبات مع الأخذ في الاعتبار القيود التي تتعلق بحجم وميزانية الجهة المعنية.

في هذا الخيار، تكون تبعية مدير أمن المعلومات مباشرة للجنة أمن المعلومات، بينما يمكن إدارة الجوانب الإدارية لأمن المعلومات تحت إشراف المدير التنفيذي. ويكون المدير التنفيذي مسئولاً عن اعتماد الميزانية السنوية وتعويضات المدراء التنفيذيين. ويمثل الخط الملون المتقطع متطلبات التشاور بين الإدارات المختلفة وإدارة أمن المعلومات.

وقد تم إيضاح الأدوار المشمولة في الخيار الثاني ضمن القسم ٤,١,١. وهناك عدد من الإيجابيات والسلبيات الرئيسية التي ينطوي عليها الخيار الثاني.

### ٣.٢.١. جدول الإيجابيات مقابل السلبيات

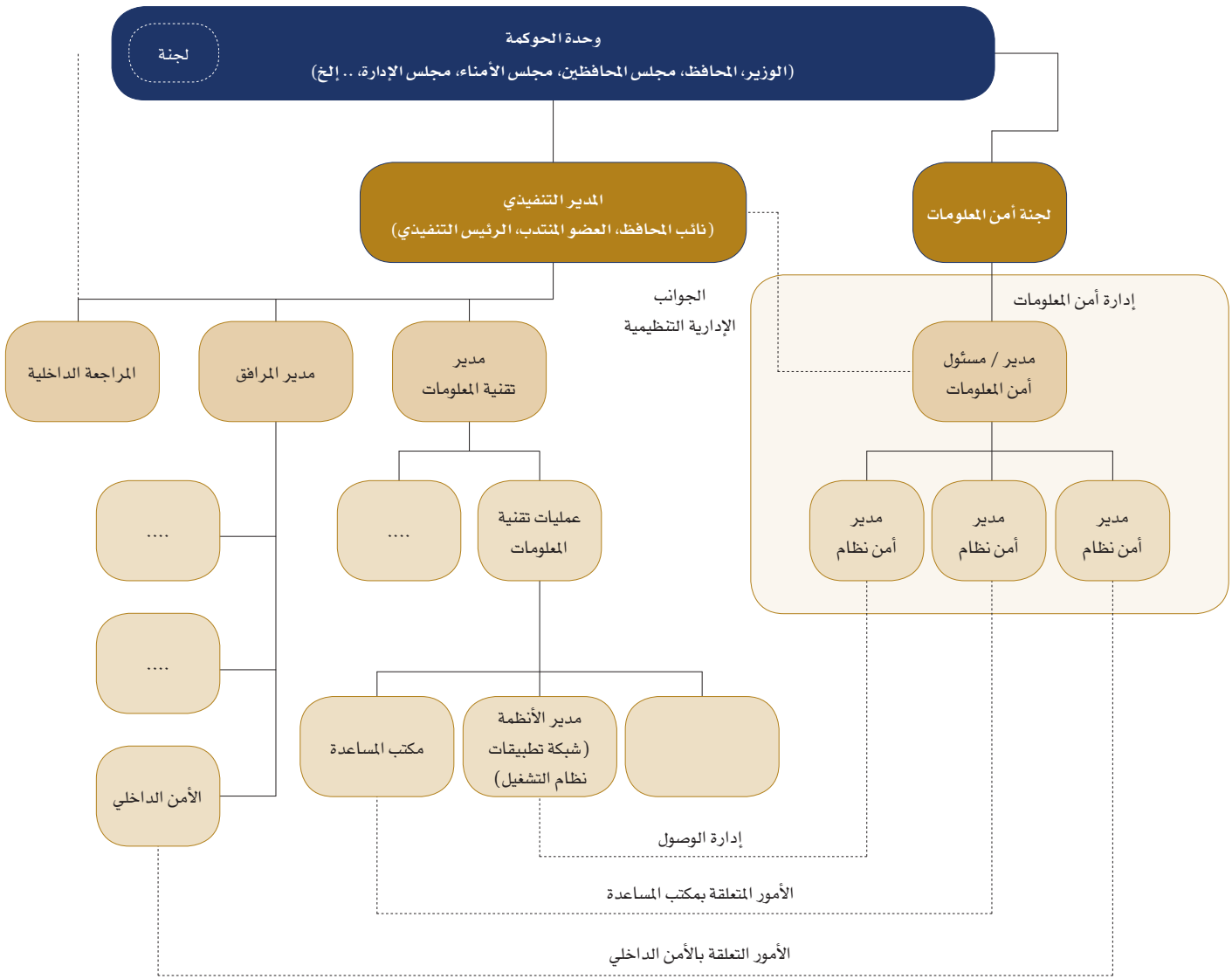
| الإيجابيات | السلبيات |
|---|---|
| كفاءة توزيع أعباء العمل | زيادة التكلفة |
| فصل المهام والواجبات | عدم دقة / عدم اكتمال التقارير والتبعية الإدارية |
| وجود موارد مخصصة | مقاومة التغيير |
| رفع تقارير صحيحة لمستوى المدير التنفيذي | |

يتضح من خلال إيجابيات الخيار الثاني أن إدارة أمن المعلومات تركز على المهام والمسئوليات المتعلقة بأمن المعلومات، حيث يوجد فصل واضح للمهام والواجبات مع وجود موارد مخصصة ومكرسة للقيام بالمهام والوظائف المختلفة لأمن المعلومات. كما أن هذا الخيار يرجع التبعية الإدارية كاملة إلى المدير التنفيذي، حيث يرفع مدير أمن المعلومات تقاريره إلى المدير التنفيذي مباشرة. وبذلك تكون للمدير التنفيذي صلاحيات اتخاذ القرارات لإحداث التغييرات التنظيمية المطلوبة لإلزام إنفاذ سياسات وإجراءات أمن المعلومات. بينما تتضمن سلبيات الخيار الثاني زيادة التكلفة بسبب زيادة عدد الموظفين والمرافق المطلوبة. ورغم أن التبعية الإداري والتقارير ترفع كاملة لمستوى الرئيس التنفيذي، إلا أنه بإمكان المدير التنفيذي في بعض الحالات تصفية (حذف وإضافة) واختيار نوعيه التقارير المرفوعة بما تقتضي مصلحته، وذلك قد يعكس صورة غير دقيقة / غير كاملة لوحدة الحوكمة.

### ٣.٢.٢. الخلاصة

وفقاً للإيجابيات والسلبيات المذكورة أعلاه، فإن الخيار الثاني يناسب الجهات متوسطة الحجم والتي لديها مخاطر متوسطة.

## ٣.٣. الخيار الثالث



تم تصميم وهيكلة الخيار الثالث للجهات الكبيرة الحجم ذات المخاطر العالية والعالية جداً. وفي هذه الحالة يجب الأخذ في الاعتبار الأولويات العليا عند اختيار تعيين الموقع الهرمي لإدارة أمن المعلومات، بحيث تعين دون التنازل عن أي من الأدوار الرئيسية في إدارة أمن المعلومات.

في هـذا الخيـار، يرتبط مدير أمن المعلومـات في المدير التنفيذي في الأمور والمهـام الإدارية الروتينية الخاصة بـإدارة أمن المعلومات بينما يرتبـط مباشـرة بلجنة أمن المعلومات، وهي التي تعتمد الميزانية السنوية وتعويضـات المسئولين التنفيذيين. وتمثل الخطوط الملونة المتقطعة متطلبات التشاور بين الإدارات المختلفة وإدارة أمن المعلومات.

تعمل إدارة أمن المعلومات باستقلالية عن المدير التنفيذي، ويكون لديها أهداف رئيسية وفرعية محددة تتعلق بأمن المعلومات، غير أنه يتعين علـى إدارة أمن المعلومات التفاعل والتعاون بشأن الأمور المتعلقـة بأمن المعلومات مع الإدارات المعنية الأخرى قبل تنفيذ السياسات والمعايير والإجراءات الجديدة.

وقد تم تضمين المزيد من الإيضاحات حول الأدوار المتعلقة في الخيار الثالث ضمن القسم ٤,١,١. وفيما يلي الإيجابيات والسلبيات الرئيسية للخيار المذكور أعلاه:

### ٣.٣.١. جدول الإيجابيات مقابل السلبيات

| الإيجابيات | السلبيات |
|---|---|
| كفاءة توزيع أعباء العمل | زيادة التكلفة |
| فصل المهام والواجبات | |
| وجود موارد مخصصة | |
| تقارير إدارية كاملة | |
| استقلالية واضحة | |

يتضـح من خلال إيجابيـات الخيار الثالث أن إدارة أمن المعلومات تركز على المهام والمسئوليـات المتعلقة بأمن المعلومات، حيث يوجد فصل واضـح في المهـام والواجبات مع وجود موارد مخصصـة ومكرسة للقيام بالمهام والوظائف المختلفة لأمن المعلومـات. وتكون التبعية الإدارية بالكامـل إلى وحـدة الحوكمة، حيث يتبـع مدير أمن المعلومات مباشرة إلى وحـدة الحوكمة. وتتضمن سلبيات الخيـار الثالث زيادة التكلفة بسبب زيادة عدد الموظفين والمرافق المطلوبة.

### ٣.٣.٢. الخلاصة

وفقاً للإيجابيات والسلبيات المذكورة أعلاه، فإن الخيار الثالث يناسب الجهات كبيرة الحجم والتي لديها مخاطر عالية.

### ٤.٣. تعيين الموقع للإدارة في الهيكل التنظيمي استناداً إلى المخاطر

قـد لا تنطبـق الخيارات المذكورة أعلاه على بعض الجهات الحكومية، ومثال ذلك الجهات الكبيرة الحجم ذات المخاطر العادية، أو الجهات المتوسطـة الحجـم ذات المخاطر العاليـة. ويوضح الجدول أدنـاه خيارات مختلفة يمكـن تطبيقها على مختلف الجهـات. يجب الأخذ بعين الاعتبار الإيجابيات والسلبيات المذكورة أعلاه إذ ما زالت تنطبق على كل من الخيارات الواردة في هذا الجدول:

| | مخاطر عالية | مخاطر متوسطة | مخاطر عادية |
|---|---|---|---|
| الجهات الكبيرة الحجم | الخيار الثالث | الخيار الثاني | الخيار الأول |
| الجهات المتوسطة الحجم | الخيار الثاني | الخيار الثاني | الخيار الأول |
| الجهات الصغيرة الحجم | الخيار الثاني | الخيار الثاني | الخيار الأول |

## ٤. الموافقة على الخيار

يجب أيضـا أخذ قيـود الميزانية في الاعتبار عند الاختيار، ممـا يستلزم الحصول على موافقة مـن الإدارة العليا لتكوين وإنشاء إدارة أمن المعلومـات. بعد اختيار خيـار، لا بد من تقديم اقـتراح رسمـي إلى الإدارة العليا مع الميزانية العامـة لإنشاء وظيفة لأمـن المعلومات. يجب على الإدارة العليا الموافقة رسميا على مقترح وظيفة أمن المعلومات قبل البدء في عملية تنفيذ إنشاء الإدارة.

## ٥. عملية تعيين إدارة أمن المعلومات.

### ٥.١. البدء في عملية التعيين

يناقـش هـذا القسم مرحلة البدء في عمليـة التعيين حسب توجيهات الإدارة العليا، حيث يتعين على (اسم الجهة) أن تكون لديها إدارة لأمن المعلومات.

يتـم إجـراء تحليل للثغرات الأمنية المحتملة للمعلومات قبل تأسيس إدارة لأمـن المعلومات. وستحدد نتائج تحليل الثغرات جوانب النقص في إدارة أمـن المعلومـات (وذلك عند إفتراض وجود إدارة تعنى بأمن المعلومات لدى الجهة)، وسيكون من مسئولية الإدارة العليا تأسيس إدارة أمن المعلومات حسبما ورد في هذا الدليل.

الأمـن هـو مسئوليـة جميـع الأشخاص في الجهه، ويكـون جميع المستخدمـين النهائيين مسئولين عن فهـم السياسات والإجراءات المطبقـة علـى أعمالهم ووظائفهـم والالتزام بما هـو متوقع منهم في مجـال المراقبـة الأمنية. ويجـب أن يكـون المستخدمون ملمين بمسئولياتهـم ومدربـين إلى مستـوى كاف للحـد مـن مخاطـر الخسارة.

ورغـم أن المسميـات الوظيفية المحددة ونطـاق مسئولية الموظفين قـد تختلـف من جهـة حكوميـة لأخـرى، إلا أن الأدوار التي سيلي ذكرهـا تدعـم تنفيـذ الضوابـط الأمنية. ومـن الممكـن أن يؤدي موظـف ما عـدة أدوار عندما تحدد العمليات لـدى الجهة المعنية، وذلـك اعتمـاداً علـى القيـود القائمة والهيـكل الوظيفـي للجهة. ومـن المهم الايعاز بمهام وظائف أمـن المعلومات المختلفة وتحديد مسئوليات واضحة للموظفين المعنيـين للتأكد من تنفيذ المهام. إن تبليـغ المسئوليات المتعلقة بكل وظيفة مـن خلال توزيع السياسات، والأوصاف الوظيفيـة، والتدريب، وتوجيهات الإدارة يوفر الأساس لتنفيذ الضوابط الأمنية من قبل فريق العمل.

## ٥. ١. ١. الأدوار والمسئوليات

### ٥. ١. ١. ١. الإدارة العليا

تعنـى الإدارة العليا بالمسئوليـة الكلية عن حماية أصول المعلومات. وتعتمـد أعمال الجهة الحكومية على توفـر ودقة المعلومات المتاحة وحمايتها من الأشخاص الذين لا حاجة لديهم للاطلاع عليها. إذ قـد تتكبد الجهة خسائـر مالية أو تتعلق بسمعتهـا في حال انتهاك سرية ونزاهة وتكامل وتوفر المعلومات. وعلى أعضاء فريق الإدارة أن يدركـوا مصلحـة الجهة حين يقبلون بـأي مخاطر تحيط بأمن معلومـات الجهـة، إذ عليهم أخـذ الحيطة عند اتخـاذ القرارات الدقيقـه، وأيضا مـن القبـول بالمخاطر التي قد تنجـم عند عدم أتخاذهم القـرارات المناسبـة اللازمه لحمايه أمـن المعلومات أو مـن أي إخفاق قد ينتج من عدم فهم طبيعـة المخاطر المتأصلة في العمليات الحالية لأنظمة المعلومات.

### ٥. ١. ١. ٢. مسئول أمن المعلومات

يتـولى مسئول أمن المعلومات توجيـه، وتنسيق، وتخطيط، وتنظيم أنشطـة أمن المعلومات لـدى الجهة. يعمل مسئـول أمن المعلومات مع عدد كبـير من الأشخاص (الموظفين) مثـل الإدارة التنفيذية، إدارات وحـدات العمل، الموظفين الفنيين، والأطـراف الثالثة مثل المراجعين والاستشاريين الخارجيين. ويكون مسئول أمن المعلومات والفريق العامل معه مسئولين عن تقييم، وتنفيذ، وإدارة، ومراجعة السياسـات والمعايير، والإجراءات، والقواعد، والإرشادات الأمنية لدى الجهة.

### ٥. ١. ١. ٣. مراجع أنظمة المعلومات

يقرر مراجع أنظمة المعلومات فيما إذا كانت تلك الأنظمة متوافقة مـع السياسات، والإجـراءات، والمعايير، والقواعـد، والتصاميم، والبنية المعمارية، وتوجيهـات الإدارة، والمتطلبات الأخرى المتعلقة بأمـن المعلومات. ويقوم مراجعو أمن المعلومات بتقديم تطمينات/ تأكيـدات مستقلة إلى الإدارة حول مـدى ملائمة الأهداف الأمنية اعتمـادا على نتائـج المراجعة المستقلة. ويقـوم المراجعون بفحص أنظمـة المعلومـات ويقـررون فيمـا إذا كانـت مصممـة، ومعدة، ومنفـذة، ومشغلـة، ومـدارة بطريقـة تكفـل تحقيـق الأهـداف التنظيميـة. كما يقـدم المراجعون للإدارة العليـا للجهة الحكومية نظـرة مستقلة حول الضوابط المتبعة ومـدى فاعليتها. ويجب أخذ عينات لفحص وجود وفاعلية ضوابط أمن المعلومات.

### ٥. ١. ١. ٤. مدير أمن أنظمة المعلومات

يدير مدير أمن أنظمة المعلومات عمليات طلبات دخول المستخدمين، وعليهم التأكد من إعطاء الصلاحيات للأشخاص الذين تم تفويضهم بالوصـول من قبل الإدارة.و يمتلك الأشخاص المفوضين صلاحيات عاليـة، إذ يمكنهم إنشاء وحذف الحسابات وصلاحيات الوصول. وعلى مـدراء أمـن الأنظمـة إنهاء صلاحيات الوصـول عند ترك الموظفـين لوظائفهم أو نقلهم بين أقسـام الجهة. ويحتفظ مـدراء أمن الأنظمة بسجلات الموافقة كجزء من البيئة الرقابية، ويقدمون تلك السجلات لمراجعي أنظمة المعلومات لإظهار الالتزام بالسياسات.

### ٥. ١. ١. ٥. الأمن الداخلي

يعنـى الموظفـون الذيـن تم ايعاز أدوار الأمن المـادي إليهم بإقامة علاقات عمل مـع الجهات الخارجية المختصة بإلـزام تنفيذ القانون مثل الشرطـة وذلـك للمساعدة في إجراء التحقيقات المتعلقة الحوادث الأمنية. ويدير موظفو الأمن المادي عمليات تركيب، وصيانة، واستمرارية أنظمـة المراقبة عبر الشبكـة التلفزيونية المغلقة، وأنظمة الإنذار بالسرقة، وأنظمة التحكـم بالوصول من خلال قارئ البطاقات. ويتم وضع الحراس حيثما يلزم لمنع الدخول غير المصرح به، ولتوفير السلامة لموظفي الجهة. ويتعاون موظفو الأمن الطبيعي مع أمن الأنظمة، والموارد البشرية، والمرافق، والمناطق القانونية، ومناطق الأعمال للتأكد من تكامل كافة الممارسات المتبعة.

### ٥. ١. ١. ٦. مدير مكتب المساعدة

حسبما يتضح من المسمى، فإن مهمة مكتب المساعدة التعامل مع الاستفسارات الواردة من المستخدمين الذين يبلغون عن مشاكل في النظام عن طريق نظام تعقب المشاكل. ومن ضمن مشاكل أنظمة المعلومات الوارد إبلاغها إلى مكتب المساعدة، الاستجابة البطيئة، احتمال الإصابة بالفيروس، الدخـول غـير المصرح به، عدم القـدرة على الوصول إلى مـوارد النظام، أو الأسئلـة والاستفسارات حـول استخدام البرامج. إن مكتـب المساعـدة مسئـول عن إعادة ضبـط كلمات المرور، إعـادة تزامن/ إعادة إنشاء الرمـوز المميـزة (tokens) والبطاقات الذكية، وحـل المشـاكل الأخرى المتعلقة بالتحكم بالدخول/ الوصـول إلى الأنظمة. ويمكن القيام بهذه الوظائف من خـلال الخدمة الذاتية بواسطة المستخدمين النهائيين أنفسهم، أو من قبل طرف آخر مثل إدارة الأمن أو مدراء الأنظمة، إلخ بدلاً من أن يقوم بها موظفو مكتب المساعدة، ويعتمد ذلك على الهيكل التنظيمي ومبادئ فصل المهام المستخدمة لدى الجهة.

## ٥.٢. تخطيط عملية التعيين

اختيار الموظفين الملائمين هو أحد عوامل نجاح إدارة أمن المعلومات. فبعد تحديد الأدوار والمسئوليات لخيارات التعيين المقترحة، يجب على (اسم الجهة) أن تأخذ في اعتبارها ما يلي:

- إعداد جدول المهارات (انظر النموذج أدناه) الذي يحدد المهارات المطلوبة:

جدول المهارات

| الشهادات | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| المرشح | CISM | CISSP | CISA | CCSP | CPP | CEH | GIAC | ISO 27001 | المؤهلات والتدريبات الأخرى المتعلقة بأنظمة المعلومات |
| الاسم | | | | | | | | | |
| الاسم | | | | | | | | | |
| الاسم | | | | | | | | | |
| الاسم | | | | | | | | | |
| الاسم | | | | | | | | | |
| الاسم | | | | | | | | | |

- تبليغ الموارد البشرية بالمهارات المطلوبة والجداول الزمنية للحاجة إليها.
- بدء عملية التوظيف.
- تجميع السير الذاتية للمرشحين.
- تحديد قائمة نهائية بالمرشحين باختيار من تتوافق مؤهلاته مع الخواص المطلوبة للتوظيف.
- الترتيب لإجراء مقابلات شخصية مع المرشحين المختارين.

### ٣.٥. تنفيذ عملية التعيين

في مرحلة تنفيذ التعيين، ينبغي على (اسم الجهة) أن تبدأ في اتخاذ القرارات المتعلقة بالمرشحين المؤهلين لشغل الوظائف المختلفة بناءً على خيارات التعيين المذكورة آنفاً في هذه الوثيقة.

- يجب توظيف المرشحين وفقاً لعملية التوظيف المتبعة لدى (اسم الجهة).
- عند وصول المرشح إلى (اسم الجهة)، يجب أن يخضع للتوجيه والتعريف للتأكد من البداية السلسة للعمل.

### ٤.٥. المراقبة والتحكم بالتعيين

لضمان استمرارية نجاح إدارة أمن المعلومات، يجب أن تأخذ (اسم الجهة) في اعتبارها ما يلي:

- عمل تقييم سنوي للموظفين.
- تطوير الأوصاف الوظيفية والحفاظ عليها.
- إعداد خطط التطوير الوظيفي والحفاظ عليها.
- إجراء تقييم الضعف في المهارات سنوياً.
- تطوير منهج تدريب يتم تحديثه بانتظام لكل مجموعة مستهدفة من الموظفين مع الأخذ في الاعتبار ما يلي:
- احتياجات وإستراتيجية العمل الحالية والمستقبلية.
- قيم الشركة (القيم الأخلاقية، ثقافة الرقابة والأمن، إلخ).
- تنفيذ بنية تحتية وبرامج جديدة لتقنية المعلومات (أي مجموعات البرامج والتطبيقات).
- المهارات الحالية والمستقبلية، مواصفات الكفاءة، والشهادات، و/أو احتياجات الاعتماد من الهيئات ذات العلاقة، وكذلك إعادة اعتماد الشهادات.
- طرق تقديم الخدمات (مثل الحصص الدراسية أو عبر الويب)، حجم المجموعة المستهدفة، إمكانية الوصول.

الجزء السابع

# عملية مراجعة أمن المعلومات
# (ملخص دليل المراجعة)

## ١. مقدمة

تقـدم هـذه الوثيقة عملية مراجعة أمن المعلومات لدى (اسم الجهة). وتتضمـن عملية المراجعة الأنشطة الرئيسية المتعلقة بتخطيط وتنفيذ وإعداد تقارير مراجعة أمن المعلومات.

## ٢. نظرة عامة

يتم إجراء مراجعة أمن المعلومات للحصول على وجهة نظر مستقلة عن حالة ضوابط أمن المعلومات لدى الجهة الحكومية المعنية، ويستحسن تنفيذ وظيفة المراجعة هذه من قبل:

١. قسم مستقل يختص بمراجعة أمن المعلومات يتبع إدارة المراجعة الداخلية للجهة.

٢. قسم مختص بمراجعة أمن المعلومات يتبع إدارة/ لجنة مركزية مختصة بحوكمة أمن المعلومات لدى الجهات الحكومية الضخمة.

تكون إدارة / وحدة مراجعة أمن المعلومات لدى الجهة الحكومية مسئولة عن العمليات الرئيسية التالية:

١. **تخطيط مراجعة أمن المعلومات:** ويشمل ذلك أنشطة التخطيط المبنية على المخاطر لتحديد أنواع مراجعات أمن المعلومات المزمع إجراؤها للجهة الحكومية.

٢. **تنفيذ مراجعة أمن المعلومات:** ويشمل هذا النشاط القيام بالمراجعات المخططة بناءً على خطة مراجعة محددة لأمن المعلومات.

٣. **إعداد تقارير مراجعة أمن المعلومات:** كجزء من هذا النشاط، يتم تجميع نتائج مراجعات أمن المعلومات وتضمينها في التقارير المعدة لإبلاغ أصحاب الصلاحية المعنيين.

## ٣. عمليات مراجعة أمن المعلومات

يوضـح هـذا القسم بشكل إضافي الإجراءات المحـددة لعمليات مراجعة أمن المعلومات؛ حيث يعرض في البداية إجراءات تخطيط مراجعة أمن المعلومات. ومن ثم يتم عرض إجراءات تنفيذ مراجعات أمن المعلومات وإجراءات إعداد تقارير مراجعة أمن المعلومات نظرا لترابطها أثناء تنفيذ هذه العمليات:

## ٣.١. تخطيط مراجعة أمن المعلومات

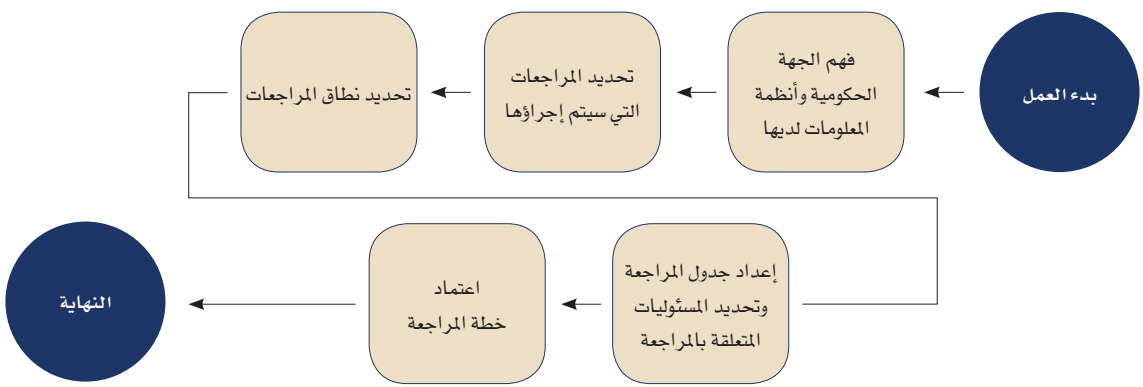
### ٣.١.١. الهدف

يوضح هذا الإجراء الأنشطة الرئيسية للقيام بتخطيط مراجعة أمن المعلومات المبني على المخاطر لدى (اسم الجهة).

### ٣.١.٢. مرجعية الوثيقة

سياسة مراجعة أمن المعلومات.

### ٣.١.٣. الإجراء



### ٣. ١. ٣. ١. فهم الجهة الحكومية وأنظمة المعلومات لديها

١. يقوم (مدير إدارة المراجعة الداخلية) بالتنسيق مع (مدير مراجعة أمن المعلومات لديه) بالبدء في عملية تخطيط مراجعة أمن المعلومات كجزء من التخطيط السنوي للمراجعة الداخلية لدى الجهة الحكومية. ويتم تكليف (مدير مراجعة أمن المعلومات) بالمسئولية الرئيسية عن مراجعة أمن المعلومات.

٢. يقوم (مدير مراجعة أمن المعلومات) بما يلي:

- تطوير/ تحديث مفهومه للأعمال والمهام الفنية المختلفة (خصوصاً تلك المتعلقة بتقنية المعلومات وأمن المعلومات) لدى الجهة الحكومية.
- يقوم (مدير مراجعة أمن المعلومات) بمراجعة قائمة تصنيف أنظمة المعلومات لدى الجهة الحكومية التي تم إعدادها ضمن إجراءات تحديد وتصنيف أنظمة المعلومات.
- يقوم (مدير مراجعة أمن المعلومات) بتعيين التصنيف الأمني للإدارات التقنية والإدارية المحددة آخذاً في الاعتبار التصنيف الأمني لجميع أنظمة المعلومات المستخدمة أو التي يتم إدارتها بواسطة تلك الإدارات، وكذلك آراء (مدير إدارة المراجعة الداخلية) والعوامل الأخرى ذات الصلة.

### ٣. ١. ٣. ٢. تحديد أعمال المراجعات التي سيتم إجراؤها

١. يستخدم (مدير إدارة المراجعة الداخلية) نموذج متطلبات تخطيط مراجعة أمن المعلومات من أجل إدراج الوظائف والأعمال وأنظمة المعلومات التي سيتم مراجعتها.

٢. يُحدد (مدير مراجعة أمن المعلومات) عدد مرات المراجعة لكل من إدارات الأعمال والإدارات الفنية وأنظمة المعلومات كما يلي:

- وظائف/ أنظمة المعلومات عالية المخاطر، وتتم مراجعتها بصورة شاملة سنوياً.
- وظائف/ أنظمة المعلومات متوسطة المخاطر، وتتم مراجعتها بدقة كل سنتين، وتراجع عينات محددة منها سنوياً.
- وظائف/ أنظمة المعلومات عادية المخاطر، وتتم مراجعتها على أساس عينات مختارة سنوياً.

### ٣. ١. ٣. ٣. تحديد نطاق المراجعات

١. يحدد (مدير مراجعة أمن المعلومات) نطاق كل عملية من عمليات المراجعة، كمايلي:

- يتم تحديد نطاق مراجعة كل من إدارات الأعمال والإدارات الفنية من خلال تعريف الجوانب الرئيسية من سياسات وإجراءات أمن المعلومات العامة المتعلقة بتلك الإدارات.
- يتم تحديد نطاق مراجعة أنظمة المعلومات من خلال مراجعة السياسة الأمنية المتعلقة بالنظام المعني. في حالة عدم وجود سياسة محددة تنطبق على النظام، يتم تحديد النطاق من خلال مراجعة الجوانب المطبقة على نظام مشابه استنادا على ما يتناسب من معايير الأنظمة الموثقة لدى الجهة الحكومية، وأفضل الممارسات الدولية المتبعة بهذا الصدد.

٢. يحدد (مدير مراجعة أمن المعلومات) نوع المراجعة التي سيتم أجراؤها حتى يتم تغطية نطاق أعمال المراجعة، مثل:

- مراجعة عمليات أمن المعلومات.
- الهجمات والاختراقات الحاسوبيه.
- تقييم الثغرات الأمنية.
- حساسية أصول المعلومات.
- مراجعة الإعدادات الأمنية.
- وغير ذلك.

### ٣. ١. ٣. ٤. إعداد جدول أعمال المراجعة وتعيين المسئوليات المتعلقة المراجعة

١. يحدد (مدير مراجعة أمن المعلومات) جدولاً محدداً لكل عملية مراجعة كالتالي:

- يحدد الوقت المقدر الذي ستستغرقه كل مراجعة.
- يحدد تاريخ بداية ونهاية كل مراجعة من المراجعات واضعاً في الاعتبار تكرار المراجعات، مدة المراجعة، تواجد وتوفر وقت المعنيين بأعمال الوحدة التي ستتم مراجعتها، والعوامل الأخرى ذات العلاقة.

٢. يقرر (مدير مراجعة أمن المعلومات) بمقتضى المدخلات التي يساهم بها (مدير إدارة المراجعة الداخلية) فيما إذا كان سيتم إجراء المراجعة المتعلقة بأمن المعلومات داخلياً من خلال الموارد البشريه المتاحة في إدارته، أو من خلال مراجعيين خارجيين، أو باستخدام طريقة العمل المشترك بين الموارد المتاحة في إدارته مع موارد من المراجعين الخارجيين.

٣. حيثما ينطبق، يقوم (مدير مراجعة أمن المعلومات) بمدخلات من (مدير إدارة المراجعة الداخلية) بتحديد الشخص المسئول عن إجراء المراجعة من إدارة المراجعة الداخلية.

### ٣. ١. ٣. ٥. اعتماد خطة المراجعة

١. يرسل (مدير مراجعة أمن المعلومات) خطة المراجعة الداخلية إلى (مدير إدارة المراجعة الداخلية) للمراجعة والاعتماد.

٢. يقوم (مدير إدارة المراجعة الداخلية) بمراجعة واعتماد الخطة ويرسلها إلى (لجنة المراجعة) لدى الجهة الحكومية للمراجعة والاعتماد.

٣. عند استلام موافقة (لجنة المراجعة)، يقوم (مدير إدارة المراجعة الداخلية) بما يلي:

- تبليغ خطة المراجعة الأمنية إلى الموظفين المعنيين في (اسم الجهة).
- تنظيم الموارد الداخلية والموارد المزودة من قبل المورد الخارجي للقيام بأعمال المراجعة وفقاً للعمليات المتبعة لدى الجهة الحكومية.

## ٣. ١. ٤. النموذج ذي العلاقة

خطة المراجعة الأمنية.

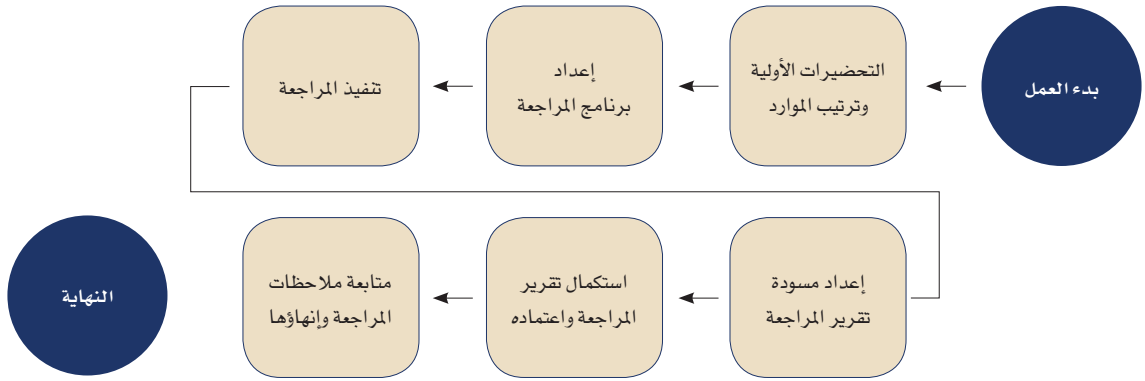
## ٣. ٢. تنفيذ وإعداد التقارير ومتابعة مراجعة أمن المعلومات

### ٣. ٢. ١. الهدف

يوضـح هـذا الإجراء الأنشطة الرئيسية لتنفيذ خطة مراجعة أمن المعلومات التي تم وضعها للجهـة الحكومية وإعداد تقارير المتابعه لنتائج المراجعة والمخاطر والتوصيات إلى المعنيين.

### ٣. ٢. ٢. مرجعية الوثيقة

سياسة مراجعة أمن المعلومات.



## ٣. ٢. ٣. الإجراء

### ٣. ٢. ٣. ١. التحضيرات الأولية وتنظيم الموارد

١. يقوم (مدير مراجعة أمن المعلومات) بتنظيم الموارد البشرية المطلوبة لإجراء المراجعة المجدولة:

- إذا كان سيتم تنفيذ هذه المبادرة داخلياً، يقوم (مدير إدارة المراجعة الداخلية) بالتنسيق مع (مدير إدارة أمن المعلومات) بتحديد الموارد البشرية الداخلية التي يتعين عليها إجراء عملية المراجعة، ويبلغهم بمهام المراجعة التي تم تعيينها لهم.
- أما إذا كان سيتم تنفيذ هذه المبادرة بواسطة مراجعين خارجيينً، فسيقوم (مدير إدارة المراجعة الداخلية) بالتأكد من اختيار طرف ثالث مناسب لذلك، وتوقيع عقد معه لتنفيذ أعمال المراجعة حسب الخطة.

٢. يقوم (مدير إدارة أمن المعلومات) بتبليغ الأشخاص ذوي العلاقة بتاريخ المراجعة المخططة ويطلب منهم التعاون، ويشمل ذلك تبليغ كل من:

- مدير إداراة الأعمال أو الإداره الفنيه التي سيتم مراجعتها.
- المسئول عن نظام المعلومات الذي سيتم مراجعته.
- الأشخاص الآخرين ذوي العلاقة.

### ٣. ٢. ٣. ٢. إعداد برنامج المراجعة

١. قبل البدء في أية عملية مراجعة، يتم إعداد برنامج مراجعة تفصيلي باستخدام نموذج تطوير برنامج المراجعة. ويتم من خلاله توثيق الضوابط المحددة الواجب تقييمها كجزء من المراجعة.

٢. الاعتبارات الرئيسية لتطوير برنامج مراجعة أمن المعلومات هي كالتالي:

- الرجوع إلى السياسة الأمنية الخاصة بنظام المعلومات المعني (أو مجموعة أنظمة المعلومات).
- إذا كانت لا توجد سياسة للمعايير الأمنية لنظام المعلومات (أو مجموعة أنظمة المعلومات)، فيتم الرجوع إلى معيار الأمن المحدد لنظام المعلومات المعني.
- لمراجعة إدارات الأعمال أو الإدارات الفنية، يتم تحديد السياسات والإجراءات العامة المطبقة على تلك الإدارة المراد مراجعتها.
- الرجوع إلى أفضل الممارسات والقواعد.

٣. يقوم فريق المراجعة المعين بتحديد وتوثيق طرق وأساليب المراجعة المناسبة للتأكد من فاعلية الضوابط المحددة في برنامج المراجعة.

### ٣. ٢. ٣. ٣. تنفيذ المراجعة

١. يقوم فريق مراجعة أمن المعلومات بإجراء تقييم لأمن المعلومات وفقاً لبرنامج المراجعة والذي تم إعداده مسبقا، والأساليب التي تم تحديدها لتقييم أمن المعلومات.

٢. يتم تقييم ضوابط الإجراءات كما يلي:

- يقوم فريق مراجعة أمن المعلومات سنوياً بمناقشة الأشخاص المسئولين عن نظام المعلومات بشأن حالة كل ضابط من ضوابط التحكم المشتمل عليها برنامج مراجعة أمن المعلومات.
- بناءً على الرد المستلم، وإذا ما تقرر أن ضابط التحكم غير فعال، يقوم فريق المراجعة بتدوين تلك الملاحظات.
- وإذا تم إبلاغ فريق المراجعة أن الضوابط فعالة، يطلب

الفريـق أدلـة لدعم ومسانـدة صحـة فعاليـة الضوابط، أو يقـوم بنفسه بإجـراء تقييم لضوابط أمـن المعلومات للتأكد من صحـة فعالية الضوابـط. كما يقوم فريـق مراجعة أمن المعلومـات بتدويـن أي نقـاط ضعـف تمـت ملاحظتهـا في ضوابط التحكم كجزء من هذه المراجعة.

٣. بناء على نطاق أعمال مراجعة أمن المعلومات، يجوز لفريق مراجعة أمن المعلومات استخدام الأدوات والأساليب المناسبة لإجراء مراجعات أمن المعلومات، مثل مراجعة إعدادات الأنظمة، تقييم الثغرات الأمنية، فحص الهجمات والاختراق، وغير ذلك. وفي هذه الحالات فإنه:

- يتم أخذ الإذن من الأشخاص المعنيين لتشغيل أدوات وبرامج التقييم الأمني.
- يتم استخـدام طرق تقييم أمنية مناسبـة لإجراء اختبارات التقييم الأمني.
- يتـم تدويـن الملاحظـات ومراجعتهـا لحـذف الملاحظـات الخاطئة منها.

٤. يقوم فريق مراجعة أمن المعلومات بالتأكد من الاحتفاظ بالدليل عن كل ملاحظة تم تحديدها ضمن عملية مراجعة أمن المعلومات.

### ٣. ٢. ٣. ٤. إعداد مسودة تقرير المراجعة

١. يتم توثيق ملاحظات المراجعة بشكل مناسب في مسودة تقرير المراجعة.

٢. يتم توثيق الجوانب التالية لكل ملاحظة من الملاحظات التي ظهرت أثناء المراجعة:

- **نتائـج المراجعـة**: لوصف نقـاط الضعـف في الضوابط التي تمت ملاحظتها أثناء المراجعة.
- **المخاطـر**: لوصف المخاطر التي تتعرض لها الجهة الحكومية حسبمـا تبين من نتائـج المراجعة ودرجـة خطورتها (عالية، متوسطة، متدنية).
- **إجـراءات التخفيـف مـن المخاطـر الموصـى بهـا**: لوصـف الإجـراءات المقـترح اتخاذها مـن قبل الجهـه الحكومية أو المسئول عن المعلومات لمعالجة نقاط الضعف في الضوابط.

٣. يتم إشعار الإدارة التي تمت مراجعتها بمسودة تقرير/ تقارير المراجعة ومناقشة مسئوليها للتأكد من صحة نتائج المراجعة، والمخاطر، والتوصيات.

### ٣. ٢. ٣. ٥. استكمال تقرير المراجعة واعتماده

١. يقوم المُراجع بمناقشة مسودة تقرير المراجعة مع الإدارة التي تمت مراجعتها ويقدم إيضاحات كافية بشأن ملاحظات المراجعة، والمخاطر، والتوصيات التي تم تحديدها أثناء المراجعة. وللإدارة التي تمت مراجعتها أن تتفق أو لا تتفق مع المُراجع فيما تم توثيقه في التقرير. وفي حال عدم موافقتها، يتعين على تلك الإدارة تقديم أدلة داعمة كافية على فاعلية الضوابط لديها.

٢. تقدم الإدارة التي تمت مراجعتها إجابات موثقة للمُراجع بشأن خطتها لمعالجة الملاحظات التي تم تحديدها.

٣. عند الاتفاق على الملاحظات والإجراءات التصحيحية المطلوبة مع الإدارة التي تمت مراجعتها، يتم استكمال تقرير/ تقارير المراجعة ورفعها إلى (مدير إدارة المراجعة الداخلية) لمراجعته واعتماده.

٤. بعد ذلك، يتم رفع ذلك التقرير إلى (لجنة المراجعة) للمراجعة والاعتماد.

### ٣. ٢. ٣. ٦. متابعة ملاحظات المراجعة وإغلاقها

١. يعنى كل مسئول عن أحد أنظمة المعلومات/ مدير الإدارة المعنية بمسئولية معالجة الملاحظات الناشئة عن مراجعة أمن المعلومات المتعلقة بإدارته/ نظامه بالسرعة الواجبة وبشكل فعال.

٢. كل شهر (أو أقل من ذلك حسب الطلب)، يقوم المسئول عن نظام المعلومات/ مدير الإدارة المعنية بإبلاغ (مدير إدارة المراجعة الداخلية) عن وضع الإجراءات التي اتخذها لمعالجة الملاحظات ذات العلاقة والتي تم التعرف عليها أثناء عملية المراجعة.

٣. بناءً على المدخلات المستلمة من الوحدة التي تم تدقيقها، تقوم إدارة المراجعة الداخلية بإعداد تقرير شهري حول حالة تنفيذ توصيات المراجعة، وترسله إلى (لجنة المراجعة).

٤. تراجع (لجنة المراجعة) التقرير المستلم وتتخذ الإجراءات الضرورية للتأكد من تنفيذ الحلول المُرضية لجميع الملاحظات التي ظهرت أثناء مراجعة أمن المعلومات.

## ٣. ٢. ٤. النموذج المستخدم في هذه الحالة:

١. تطوير برنامج المراجعة.

٢. تقرير المراجعة.

## ٤. الاستمارات المساندة

### ٤.١. نموذج خطة مراجعة أمن المعلومات

نموذج خطة المراجعة الخاص بمراجعة إدارات الأعمال والإدارات الفنية

| م | القسم الإداري/ قسم التقنية الذي ستتم مراجعته | تصنيف المخاطر (عالي/ متوسط/ متدني) | مراجعة أمن المعلومات التي سيتم إجراؤها | ملخص نطاق المراجعة | التكرار/ الجدول | الشخص المسئول عن إدارة المراجعة | المهارات المطلوبة | ملاحظات |
|---|---|---|---|---|---|---|---|---|
| ١ | | | | | | | | |
| ٢ | | | | | | | | |
| ٣ | | | | | | | | |
| N | | | | | | | | |

نموذج خطة المراجعة الخاص بمراجعة نظام المعلومات

| م | القسم الإداري/ قسم التقنية الذي ستتم مراجعته | تصنيف المخاطر (عالي/ متوسط/ متدني) | مراجعة أمن المعلومات التي سيتم إجراؤها | ملخص نطاق المراجعة | التكرار/ الجدول | الشخص المسئول عن إدارة المراجعة | المهارات المطلوبة | ملاحظات |
|---|---|---|---|---|---|---|---|---|
| ١ | | | | | | | | |
| ٢ | | | | | | | | |
| ٣ | | | | | | | | |
| N | | | | | | | | |

## ٤. ٢. نموذج برنامج مراجعة أمن المعلومات

يتم تعبئة هذا النموذج لكل نظام معلومات أو مجموعة من أنظمة المعلومات المطلوب مراجعتها.

**اسم نظام/ قسم المعلومات:** (توثيق نظام/ قسم المعلومات المزمع مراجعته)

**اسم نظام/ قسم المعلومات:** (توثيق الرقم المرجعي لنظام/ قسم المعلومات (حيثما ينطبق)).

| رقم الضابط | الرقابة | مراحل التقييم/ أسلوب التقييم | الوثائق المطلوبة/ الأدلة | النتائج | الرقم المرجعي للدليل المستلم | بيانات المراجع |
|---|---|---|---|---|---|---|
| (محور المراجعة) | | | | | | |
| (المحور الفرعي للمراجعة) | | | | | | |
| ١ | | | | | | |
| ٢ | | | | | | |
| ٣ | | | | | | |
| ٤ | | | | | | |

## ٤. ٣. نموذج تقرير مراجعة أمن المعلومات

**القسم (١): الملخص التنفيذي**

(توثيق ملخص عام لملاحظات المراجعة الرئيسية، والمخاطر، والتوصيات، مع التركيز على الملاحظات عالية المخاطر).

**القسم (٢): نطاق المراجعة**

(توثيق النطاق الكلي لأعمال المراجعة).

**القسم (٣): منهجية المراجعة**

(توثيق المنهجية العامة المتبعة في المراجعة).

**القسم (٤): نتائج المراجعة، والمخاطر، والوصيات**

(توثيـق النتائـج المحددة المسجلة أثناء عملية المراجعة، والمخاطر المتعلقة بذلـك والتوصيات. ويستخدم هذا القسم كذلك لتسجيل الخطط الخاصة بالإدارات التي تتم مراجعتها لمعالجة الملاحظات المحددة.

| الرقم | التوصيات والنتائج الرئيسية | |
|---|---|---|
| ١ | (محور المراجعة) | |
| | النتائج ١: | |
| | أثر الخطر: | تصنيف المخاطر<br>(عالية – متوسطة – متدنية) |
| | التوصيات:<br><br>رد الإدارة:<br>موافق ☐ غير موافق ☐<br>خطة عمل الإدارة:<br>(تعنى خطة العمل بتحديد تنفيذ التوصيات أو إجراءات تصحيحية لما ورد من الملاحظات أثناء المراجعة)<br><br>تاريخ التطبيق:<br>(التاريخ)<br>المسئولية:<br>(الاسم، المسمى الوظيفي) | |

الجزء الثامن

# الملاحق

# ا. الملحق (ا): دليل استخدام مستودع سياسات وإجراءات أمن المعلومات

## ا.ا. مقدمة

يصف هذا القسم الهيكل العام للأداة البسيطة المبنية على تطبيق (MS-Access) والتي سيتم استخدامها لتمثيل مستودعات سياسات أمن المعلومات والمعايير الأمنية المتعلقة بأنظمة محددة. ويهدف هذا القسم إلى تحديد الأغراض والهيكل العام لنماذج من مستودعات السياسات التي ستستخدمها الجهات الحكومية في إعداد سياسات وإجراءات أمن المعلومات لديها.

## ا.٢. الغرض

إن الغرض من هذه المستودعات النموذجية هو تكوين تجميعاً جيداً لسياسات أمن المعلومات لدى الجهات الحكومية. وستستخدم هذه العينة من المستودعات من قبل الجهات الحكومية أثناء عملية تطوير سياسات وإجراءات أمن المعلومات.

## ا.٣. نموذج من هيكل المستودعات

يحتوي إطار المستودعات النموذجية على الصفحات المختلفة التالية:

- الصفحة الأولى هي أداة بسيطة مبنية على نظام (MS-Access) الذي يحتوي عينة من سياسات أمن المعلومات العامة.
- الصفحة الثانية هي وثيقة تحتوي على إجراءات أمن المعلومات.
- الصفحة الثالثة هي أداة بسيطة مبنية على نظام (MS-Access) الذي يحتوي عينة من سياسات أمن المعلومات المتعلقة بأنظمة محددة.

### ا.٣.١. نموذج للأداة المبنية على نظام (MS-Access) لسياسات أمن المعلومات العامة

تحتوي الأداة البسيطة المبنية على نظام (MS-Access) لسياسات أمن المعلومات العامة على العناصر التالية:

- الغرض من السياسة: وصف موجز للغرض من السياسة.
- مجال تطبيق السياسة: تحديد الإدارات والجهات المختلفة الداخلية والخارجية وكذلك الأشخاص الذين تنطبق عليهم هذه السياسة.
- المسئول التنفيذي: تحديد الشخص الذي يضطلع بالصلاحية والمسئولية النهائية عن أي تغييرات أو تحديثات تجري على السياسة. يجب اعتماد أي تغييرات أو تحديثات على السياسة من قبل المسئول التنفيذي عن السياسة.
- راعي وثيقة السياسة: الشخص المسئول عن إبقاء وحفظ السياسة وتبليغها وتحديثها بناءً على توجيهات المسئول التنفيذي عن السياسة.
- إلزامية التنفيذ: تحدد تبعات ونتائج أية مخالفة لهذه السياسة.
- قيود سياسة أمن المعلومات: يشتمل هذا القسم وصف لجزئية القيود/الضوابط المتعلقة بالسياسة المحددة.
- الإجراءات ذات العلاقة: يحدد هذا العنصر الإجراءات ذات العلاقة لسياسة معينة، إذا كان ذلك ينطبق.
- تاريخ نفاذ السياسة: يحدد هذا القسم التاريخ الذي يسري فيه تطبيق السياسة، وهو اليوم الذي يجب فيه إتباعها.

### ١. ٣. ٢. نموذج لوثيقة الإجراءات

تحتوي وثيقة الإجراءات على العناصر التالية:

- مرجعية الوثيقة: يحدد هـذا العنصر السياسة ذات العلاقة بالإجراء المحدد.
- الهدف: يذكر هذا العنصر بوضوح الهدف من الإجراء.
- أنشطـة إجراء أمـن المعلومات: يدرج هـذا العنصر ويصف أنشطة الإجراء.
- النمـوذج المطبـق: يحدد هـذا العنصـر اسم النمـوذج ذي العلاقة لإجراء معين إذا كان موجوداً.

### ١. ٣. ٣. نموذج السياسات المتعلقة بأنظمة محددة

تحتـوي الأداة السياسـات المتعلقة بأنظمة محددة علـى العناصر التالية:

- مجـال السياسـة: يحـدد هـذا العنصـر الفئـة الأساسيـة للضوابط الأمنية في السياسة.
- المجال الفرعي للسياسـة: يحدد هذا العنصر الفئة الفرعية للضوابط الأمنية في السياسة.
- تاريـخ النفاذ: يمثل هـذا العنصر التاريخ الـذي يسري فيه تطبيق السياسة، والذي يجب إتباعه حينما يحل.



### ١. ٤. ١. تطوير سياسات أمن المعلومات العامة

فيمـا يلي الخطوات الرئيسية التـي سيتبعها أعضاء فريق المشروع لدى (اسـم الجهة) باستخدام الأداة البسيطـة المبنية على نظام (MS-Access) في تطويـر سياسات أمن المعلومات العامة لإعداد تلك السياسات:

- الخيـار (١): إصدار جميع سياسات أمـن المعلومات العامة في وثيقة واحدة.
  - استبـدال جميـع حقـول (اسـم الجهـة) في الأداة البسيطـة المبنيـة علـى (MS-Access) الخاصـة بسياسـات أمـن المعلومـات العامـة باسـم الجهـة الحكومية، بحيث يتم تعديل سياسات امن المعلومات العامـة لتظهر الاسم الفعلي للجهـة الحكومية ذات العلاقة.
  - استبـدال جميـع المسميـات المتغيـرة (راعـي وثيقة السياسـة والمسئـول التنفيـذي عـن السياسـة) في الأداة المذكورة بالمعلومات المتعلقة بالهيكل التنظيمي للجهة الحكومية.
  - تحديـد تاريخ نفـاذ كل سياسة باستخـدام الحقول الفارغة في الأداة البسيطة المبنية على نظام (MS-Access) الخاصة بسياسات أمن المعلومات.
  - استخـدام نموذج سياسـات أمن المعلومـات العامة الـوارد في الملحـق (٢)، لإدخال المحتـوى الكامل في الأداة البسيطة المبنية على نظام (MS-Access).

- الخيار (٢): إعداد وثيقة منفصلة لكل سياسة من سياسات أمن المعلومات العامة.
  - اختيار مجال السياسة من الأداة البسيطة المبنية على نظام (MS-Access) الخاصة بسياسات أمن المعلومات العامة، ويتم بالتالي تكوين الضوابط المتعلقة بالسياسة.
  - استبدال جميع حقول (اسم الجهة) في الأداة البسيطة المبنية على (MS-Access) الخاصة بسياسات أمن المعلومات العامة باسم الجهة الحكومية، بحيث يتم تعديل سياسات امن المعلومات العامة لتظهر الاسم الفعلي للجهة الحكومية المعنية.
  - استبدال جميع المسميات المتغيرة (راعي وثيقة السياسة والمسئول التنفيذي عن السياسة) في الأداة المذكورة بالمعلومات المتعلقة بالهيكل التنظيمي للجهة الحكومية.
  - تحديد تاريخ نفاذ لمجال السياسة المختارة باستخدام الحقول الفارغة ضمن الأداة البسيطة المبنية على نظام (MS-Access) المتعلقة بسياسات أمن المعلومات العامة.
  - استخدام النماذج الخاصة بسياسات أمن المعلومات العامة المفردة الواردة في المحلق (٢) لإدخال الضوابط المتولدة والحقول الإضافية.
  - إعادة الخطوات أعلاه لكل مجال من مجالات السياسات التي تريد الجهة الحكومية إصدارها.
- الخيار (٣): إصدار سياسات أمن المعلومات العامة المبنية على المستخدمين.
  - اختيار نوع/ فئة المستخدمين من الأداة البسيطة المبنية على نظام (MS-Access) الخاصة بسياسات أمن المعلومات العامة، ويتم بالتالي تكوين الضوابط المتعلقة بفئة المستخدمين المختارة.
  - استبدال جميع حقول (اسم الجهة) في الأداة البسيطة المبنية على (MS-Access) الخاصة بسياسات أمن المعلومات العامة باسم الجهة الحكومية، بحيث يتم تعديل سياسات امن المعلومات العامة لأنواع المستخدمين المختارين لتظهر الاسم الفعلي للجهة الحكومية ذات العلاقة.
  - استبدال جميع المسميات المتغيرة (راعي وثيقة السياسة والمسئول التنفيذي عن السياسة) في الأداة المذكورة بالمعلومات المتعلقة بالهيكل التنظيمي للجهة الحكومية.
  - تحديد تاريخ نفاذ لنوع/فئة المستخدمين المختارة باستخدام الحقول الفارغة ضمن الأداة البسيطة المبنية على نظام (MS-Access) المتعلقة بسياسات أمن المعلومات العامة.
  - استخدام النماذج الخاصة بسياسات أمن المعلومات العامة الواردة في المحلق (٢)، القسم (٣,٢,٣) لإدخال الضوابط المتولدة والحقول الإضافية.
  - إعادة الخطوات أعلاه لكل نوع/فئة من فئات المستخدمين.

### ١. ٤. ٢. تطوير إجراءات أمن المعلومات

فيمـا يلي الخطوات الرئيسية التـي سيتبعها أعضاء فريق المشروع التابـع للجهة الحكومية في استخدام وثيقـة الإجراءات لإعداد و/ أو تعديل إجراءات أمن المعلومات:

٣. استخدام نموذج وثيقة الإجراءات لتعديل إجراءات الجهة الحكومية أو استخدام نموذج إجراءات أمن المعلومات الوارد في الملحق (٢)، لإعداد وتعديل الإجراءات ذات العلاقة لدى الجهة الحكومية من وثيقة الإجراءات المقدمة.

٤. استبدال جميع حقول (اسم الجهة) بالاسم الفعلي للجهة الحكومية بحيث يتم تعديل وثيقة الإجراءات المتكونة لتظهر اسم الجهة.

٥. استبدال جميع المتغيرات في النموذج (وظيفة تقنية المعلومات / أمن المعلومات / الإدارات الأخرى) بالمعلومات المتعلقة بالهيكل التنظيمي للجهة الحكومية.

### ١. ٤. ٣. تطويـر سياسـات أمـن المعلومـات المتعلقة بأنظمة محددة

فيمـا يلي الخطوات الرئيسية التـي سيتبعها أعضاء فريق المشروع التابـع للجهـة الحكومية في استخـدام الأداة البسيطة المبنية على نظـام (MS-Access) والخاصـة بتطوير معايـير أمن المعلومات المتعلقـة بأنظمة محـددة، لإصدار معايير أمـن المعلومات المتعلقة بأنظمة محددة:

١. اختيار عنصر نظام المعلومات (مثل تطبيق قاعدة البيانات، خوادم الأنظمة، الموجهات، غرف الخوادم، إلخ) تحت نوع البنية التحتية لتقنية المعلومات (أي التطبيق، نظام المعلومات، الشبكة، والبنية التحتية المادية) في مستودع السياسات، ويتم تبعاً لذلك توليد الضوابط ذات العلاقة.

٢. اختيار مستوى السرية والتكامل والتوافر (عالي، متوسط، عادي) لعنصر نظام المعلومات المختار لإصدار الضوابط المتعلقة بمستوى السرية والتكامل والتوافر.

٣. استبدال جميع حقول (نظام المعلومات) في الأداة المذكورة باسم عنصر أمن المعلومات ذي العلاقة، بحيث يتم تعديل بنود المعيار لتظهر اسم العنصر.

٤. استبدال جميع حقول (اسم الجهة) في الأداة بالاسم الفعلي للجهة الحكومية بحيث يتم تعديل بنود المعيار لتظهر اسم الجهة.

٥. تحديد تاريخ نفاذ المعيار باستخدام الحقول الفارغة الخاصة بمعايير أمن المعلومات المتعلقة بأنظمة محددة.

٦. استخدام نموذج المعيار الأمني للسياسات المتعلقة بمعيار محدد والمقدم ضمن الملحق (٢)، لإدخال الضوابط المتولدة والحقول الإضافية.

٧. تكرار الخطوات أعلاه لكل عنصر من عناصر أنظمة المعلومات التي تريد الجهة الحكومية استخراجها فيما يتعلق بمعايير أنظمة المعلومات المتعلقة بأنظمة محددة.

### ١.٥. تحديث سياسات وإجراءات أمن المعلومات

فيما يتعلق بتحديث سياسات وإجراءات أمن المعلومات لدى الجهة الحكومية، يفضل الاستماع إلى الإدارات المعنية لفهم الوضع الحالي. إضافة لذلك، فعند تحديث سياسات وإجراءات أمن المعلومات لدى الجهة الحكومية، فمن المهم إجراء التحديثات الضرورية على الحالة الراهنة لبيئة تقنية المعلومات لتمكين الجهة من الالتزام بالسياسات والإجراءات والمعايير التي تتطلبها الحكومة.

ويجب أن يتوافق أي نظام معلومات يتم شراؤه / تطويره من قبل الجهة الحكومية مع سياسة وإجراء شراء وتطوير أنظمة المعلومات، وبالتالي يجب تحديث محتوى/هيكل مستودع العينات تبعاً لذلك.

في حال السياسات الأمنية المتعلقة بأنظمة محددة، فمن المهم بذل جهود يومية لتجميع المعلومات حول الهجمات الجديدة، واستخدامها لتحديث السياسات الأمنية المتعلقة بأنظمة محددة لدى الجهة الحكومية.

عند اكتمال تعديل سياسات وإجراءات أمن المعلومات بناء على نتائج المعاينة والتقييم لأنظمة المعلومات لدى الجهة الحكومية، فيتعين على تلك الجهة تحديث محتوى مستودعات العينات تبعاً لذلك.

## ٢. الملحق (٢): التحكم بالتوثيق

إن الغرض من عملية إدارة التوثيق هو التحكم بجودة وثائق السياسات والإجراءات، والحفاظ على تحديثات وثائق السياسات والإجراءات لتلبية متطلبات الجهات الحكومية.

### ٢.١. المسؤولية عن الإجراءات

- يكون (المسئول عن الوثيقة) مسئولاً عما يلي:
  - تحديد راعي وثيقة السياسة، وكاتبها، ومدير تأييد الجودة.
  - مساعدة راعي وثيقة السياسة عند الحاجة.
  - تصنيف الوثيقة.
  - اعتماد الوثيقة.
- يكون (راعي وثيقة السياسة) مسئولاً عما يلي:
  - مراجعة الوثائق وتحديد الوثائق التي تحتاج لتطوير وتحديث.
  - إصدار نسخ من الوثيقة للتعديل.
  - تحديث الإجراء التصحيحي إذا لم يتم اعتماد الوثيقة.
  - نشر الوثيقة.
  - تحديث سجل الوثيقة.
- يكون (كاتب الوثيقة) مسئولاً عما يلي:
  - اختيار النموذج المناسب للوثيقة.
  - إنشاء وتحديث الوثائق.
- يكون (مدير تأكيد الجودة) مسئولاً عما يلي:
  - المراجعة والتصديق على الوثيقة المنشأة والمحدثة.
- يكون (مسجل الوثيقة) مسئولاً عما يلي:
  - تحديث سجل الوثيقة.
- يكون (أمين حفظ الوثيقة في المكتبة) مسئولاً عما يلي:
  - التأكد من حفظ الوثائق في القسم الصحيح في المكتبة.

## ٢. ٢. الأنشطة المتعلقة بالإجراءات

التخطيط لإنشاء وثيقة جديدة أو تحديث وثيقة قائمة

- لإنشاء وثيقة جديدة، ينبغي على (المسئول عن الوثيقة) تسمية الموظفين الذين سيضطلعون بمسئوليات راعي وثيقة السياسة، كاتب الوثيقة، ومدير تأكيد الجودة.
- يجب على (راعي الوثيقة) بالتنسيق مع (المسئول عن الوثيقة)، إذا لزم الأمر، تحديد نطاق التغيير في الوثيقة الحالية، والعناصر الرئيسية التي ستغطيها في الوثيقة الجديدة.
- يجب على (راعي الوثيقة) بالتنسيق مع(المسئول عن الوثيقة)، إذا لزم الأمر، مراجعة (سجل الوثائق) لتقرير فيما إذا كانت هناك وثيقة قائمة تحتوي على جميع المحتوى المطلوب أو جزء منه. وفي حال وجود وثائق أخرى تغطي الموضوع جزئياً، يجب التنسيق مع الراعين الآخرين للوثائق أو المسئولين الآخرين عن الوثائق، إذا لزم الأمر، لتحديد المرجعية المطلوبة بين الوثائق.
- ينبغي على (راعي الوثيقة) تعبئة التفاصيل المطلوبة في الوثيقة القائمة، إذا كان ينطبق، والوثيقة الجديدة/ المحدثة في نموذج طلب إنشاء/ تغيير وثيقة.

يتوجب على (راعي الوثيقة) أو (مسجل الوثيقة) تحديث التفاصيل التالية في الوثيقة الجديدة/ المحدثة في (سجل الوثيقة):

- مرجعية الوثيقة لدى تقنية المعلومات وفقاً لقواعد المرجعية في نظام (ISMS) وتحديدا في منهجية إدارة التوثيق.
- عنوان الوثيقة.
- رقم النسخة، وفقاً لقواعد ترقيم النسخ في نظام (ISMS) وتحديدا في منهجية إدارة التوثيق.
- المسئول عن الوثيقة.
- راعي الوثيقة.
- كاتب الوثيقة.
- مدير تأكيد الجودة.
- حالة الوثيقة، عندما يجب وضعها «قيد العمل».

### ٢. ٢. ١. إصدار نسخة من الوثيقة

- في حال وجود وثيقة قائمة، يجب على (راعي الوثيقة) أو (مسجل الوثيقة) تحديث حالة الوثيقة الحالية بحيث تصبح "قيد المراجعة".
- وفي حال تحديث الوثيقة، يجب على (راعي الوثيقة)، أو (أمين حفظ الوثيقة في المكتبة) إنشاء نسخة من الوثيقة بحيث تتم إعادة تسميتها لتعكس رقم التعديل التالي. ويجب إصدار نسخة من الوثيقة إلى (كاتب الوثيقة).
- إذا كان سيتم إنشاء وثيقة جديدة، راجع التعليمات المتعلقة بإجراء «اختيار النموذج المناسب».

### ٢. ٢. ٢. اختيار النموذج المناسب

- يجب أن يرجع (كاتب الوثيقة) إلى القواعد المتبعة لدى الجهة من أجل التنسيق القياسي للوثيقة.
- يجب أن يختار (كاتب الوثيقة) النموذج المطلوب.
- في حالة عدم توفر نموذج، فيجب على (كاتب الوثيقة) أن يطلب من (راعي الوثيقة) أو (أمين حفظ الوثيقة في المكتبة) المساعدة في إيجاد وثيقة مشابهة.

### ٢. ٢. ٣. إنشاء / تحديث الوثيقة

- يجب أن يستلم (كاتب الوثيقة) "نموذج طلب إنشاء/ تحديث وثيقة" للإطلاع على متطلبات إنشاء أو تحديث الوثيقة:

- إذا كان سيتم تحديث الوثيقة، فيجب على (كاتب الوثيقة) استلام نسخة من الوثيقة والبدء في تطبيق التحديثات المطلوبة.
- إذا كان سيتم إنشاء وثيقة جديدة، فيجب على (كاتب الوثيقة) الاتفاق على الأقسام الرئيسية مع (راعي الوثيقة)، وتأليف الوثيقة تبعاً لذلك وفقاً للمتطلبات الواردة في نموذج الطلب.

- يجب على (كاتب الوثيقة) تقديم الوثيقة التي تم إنشاؤها/ تحديثها إلى (مدير تأكيد الجودة) المذكور في النموذج.

### ٢.٢.٤. مراجعة الوثيقة

- يجب أن يقوم (مدير تأكيد الجودة) بمراجعة الوثيقة للتأكد من أنه تم تلبية متطلبات الجودة لدى المجموعة، وفيما إذا كان إنشاء/ تحديث الوثيقة تم بناءً على الطلب.
  - إذا أظهرت المراجعة ملاحظات محددة، فيجب تضمينها من قبل (كاتب الوثيقة) وإعادة تقديمها إلى (مدير تأكيد الجودة) للمراجعة.
  - إذا اجتازت الوثيقة عملية المراجعة بنجاح، فيجب على (مدير تأكيد الجودة) التصديق على الوثيقة بتوقيع نموذج الطلب.
- يجب تبليغ (راعي الوثيقة) أو (المسئول عن الوثيقة)، إذا لزم الأمر، بالتغييرات المقترحة من قبل (مدير تأكيد الجودة).
- يجب أن يقوم (راعي الوثيقة) أو (المسئول عن الوثيقة) بتحديث سجل حالة الوثيقة الجديدة/ المحدثة، بحيث تصبح «بانتظار الاعتماد».
- يجب على (مدير تأكيد الجودة) تقديم الوثيقة المراجعة ونموذج الطلب إلى (المسئول عن الوثيقة).

### ٢.٢.٥. تصنيف الوثيقة

يجب أن يقوم (المسئول عن الوثيقة) ببدء إجراء (تصنيف الأصل المعلوماتي) لتحديد مستوى تصنيف مناسب للوثيقة.

### ٢.٢.٦. اعتماد الوثيقة

يجب أن يجري (المسئول عن الوثيقة) مراجعة لمحتوياتها من أجل التوقيع على نموذج الطلب.

- إذا لم يقم (المسئول عن الوثيقة) باعتمادها، ولديه ملاحظات محددة عليها، فيتم الرجوع إلى التعليمات الإجرائية بشأن "تحديد الإجراء التصحيحي".
- إذا اجتازت الوثيقة عملية المراجعة بنجاح، فيتوجب على (المسئول عن الوثيقة) التوقيع على النموذج وإرسال الوثيقة إلى (راعي الوثيقة). ويتوجب على (راعي الوثيقة) أو (مسجل الوثيقة) تعديل حالة الوثيقة في "سجل الوثيقة" لتصبح "معتمدة".

### ٢.٢.٧. تحديد الإجراء التصحيحي

ينبغي على (راعي الوثيقة) تقييم سبب عدم اعتماد الوثيقة، وتقرير العملية الواجب القيام بها لاتخاذ الإجراءات التصحيحية، فإذا احتاجت الوثيقة إلى التعديل، فيتم الرجوع إلى التعليمات الإجرائية المتعلقة بـ«إنشاء/ تحديث الوثيقة».

### ٢.٢.٨. تحديث معلومات الوثيقة

يجب أن يقرر (راعي الوثيقة) مع (المسئول عن الوثيقة) إذا لزم الأمر، التاريخ التالي لتحديث الوثيقة.

يجب أن يقوم (راعي الوثيقة) بتحديث معلومات الوثيقة المدرجة قبل جدول المحتويات وفقاً لمتطلبات منهجية إدارة الوثائق ISMS.

### ٢.٢.٩. نشر الوثيقة

يجب على (راعي الوثيقة) نشر الوثيقة بصيغة (PDF) إلى المستخدمين المعنيين المدرجين في قائمة التوزيع. ويجب أن يتم النشر وفقاً لمنهجيات إدارة وثائق (ISMS) وإدارة أصول المعلومات.

ويجب على (راعي الوثيقة) بالتنسيق مع (أمين حفظ الوثيقة في المكتبة) التأكد من أن النسخة الجديدة من الوثيقة القابلة للتعديل محفوظة في قسم "الجاري" ضمن (مكتبة الوثائق)، وأنه يتم تطبيق ضوابط الوصول الملائمة إلى تلك الوثيقة.

إذا كانت هناك نسخة أقدم من الوثيقة، فيتوجب على (راعي الوثيقة) التأكيد أن (أمين حفظ الوثيقة في المكتبة) قد قام بنقل تلك النسخة إلى قسم "الأرشيف" من (مكتبة الوثائق).

### ٢.٢.١٠. تعديل سجل الوثيقة

ينبغي على (راعي الوثيقة) و(مسجل الوثيقة) التأكد من اكتمال سجلات الوثيقة الجديدة/ المحدثة.

وفي حالة وجود نسخة أقدم من الوثيقة، فيتعين على (راعي الوثيقة) أو (مسجل الوثيقة) تغيير حالة الوثيقة إلى «متوقفة» للتأكد من عدم الرجوع إليها عن طريق الخطأ.

### ٢.٢.١١. المراجعة الدورية للوثيقة

تتم مراجعة الوثيقة بعد مدة من الزمن بناءً على جدول المراجعة الدورية للوثيقة، أو من خلال عمليات أخرى.

- عند قيام (مسجل الوثيقة) باستخراج قائمة ربع سنوية من الوثائق من "سجل الوثائق" التي حل موعد مراجعتها، فإنه يجب إبلاغ (راعي الوثيقة) المعني. أو يجب أن يقوم كل (راعي وثيقة) بمراجعة السجلات الخاصة به بشكل شهري لتحديد الوثائق التي حلت مراجعتها.
- عندما تكون عملية المراجعة ناشئة بفعل تغييرات تستدعي تحديث الوثيقة، فيجب إبلاغ (راعي الوثيقة) عن الأثر الممكن أن تحدثه تلك التغييرات بالوثيقة.

يجب على (راعي الوثيقة)، بالتنسيق مع (المسئول عن الوثيقة) إذا لزم الأمر، القيام بمراجعة أثر التغيير على الوثيقة، وتقرير فيما إذا كان يتعين إجراء أي تغييرات على الوثيقة.

- إذا كان يتعين إجراء تغييرات، يتم الرجوع إلى التعليمات الإجرائية المتعلقة بـ «تخطيط إنشاء وثيقة جديدة/ تحديث وثيقة قائمة».
- إذا لم يتطلب الأمر إجراء أي تغييرات، فيجب على (راعي الوثيقة) تحديث تاريخ التعديل التالي لنسخة الوثيقة إذا لزم الأمر. ويجب

على (راعي الوثيقة) مراجعة الوثيقة مرة أخرى عندما يحل تاريخ التعديل التالي.

| المصطلح | تعريف المصطلح |
|---|---|
| التحكم في الوصول | قبول أو رفض طلبات معينة تختص بـ:<br>• الحصول على (حيازة) معلومات واستخدامها وكذلك الحصول على خدمات تتعلق بمعالجتها<br>• الدخول إلى منشآت مادية محددة مثل المباني الحكومية والمؤسسات العسكرية ونقاط العبور الحدودية. |
| قوائم التحكم في الوصول | سجل يضم :<br>• بيانات المستخدمين (شاملةً المجموعات والمعدات والعمليات) المنوحين إذن باستخدام مورد نظام معين.<br>• أنواع الوصول المُصرَّح لهم. |
| المسؤولية | الهدف الأمني الذي يولد الحاجة لتتبع أعمال جهة بعينها. يدعم ذلك عدم الإنكار، الردع، تشخيص الخطأ، اكتشاف ومنع الاختراق، القدرة على الاسترجاع بعد تنفيذ الفعل، الإجراء القانوني. |
| المعيار المتقدم للتشفير | يحدد المعيار المتقدم للتشفير خوارزمية التشفير الصادر بشأنها موافقة من الحكومة الأمريكية التي يمكن استخدامها لحماية البيانات الالكترونية. وتمثل خوارزمية المعيار المتقدم للتشفير قالب متناظر من الترميز يمكنه تشفير وفك تشفير المعلومات. يحدد هذا المعيار خوارزمية «ريجندايل» وهي تشفير قالب متناظر يمكنها معالجة قوالب بيانات بطول ١٢٨ بت باستخدام مفاتيح ترميز طولها ١٢٨ و١٩٢ و٢٥٦ بت. |
| برامج مكافحة الفيروسات | برنامج يقوم بمراقبة الحاسوب أو الشبكة للتعرف على كل أنواع البرمجيات الخبيثة ومنع أو عزل ما يظهر من حالات (أعراض) تلك البرمجيات الخبيثة. |
| أصل (مورد رئيسي) | تطبيق رئيسي أو نظام دعم عام أو برنامج له تأثير بالغ أو منشأة مادية أو نظام للتعامل مع المهام الحرجة أو مجموعة من الأنظمة المرتبطة منطقياً. |
| الأمين الأصول | الفرد المعين من قبل مالك البيانات لتكون مسؤولة عن إصدار الأحكام واتخاذ القرارات نيابة عن المنظمة فيما يتعلق بالمعلومات الأصول فئة التعيين، واستخدامها وحمايتها، وتقاسم |
| المالك الأصول | الشخص المسؤول عن إصدار الأحكام واتخاذ القرارات نيابة عن المنظمة فيما يتعلق بحساسية الأصول التعيين، واستخدامها وحمايتها، وتقاسم |
| مفاتيح غير متناظرة | مفتاحين مرتبطين أحدهما مفتاح عام والأخر خاص يتم استخدمهما لأداء عمليات متكاملة مثل التشفير وفك التشفير أو إصدار التوقيع والتحقق من صحة التوقيع. |

| المصطلح | تعريف المصطلح |
| --- | --- |
| هجوم والاختراق | اختبار الأمن في التقييم التي تحاكي العالم الحقيقي الهجمات في محاولة لتحديد أساليب للتحايل على ميزات الأمان للتطبيق، نظام، أو الشبكة. |
| التدقيق والفحص | مراجعة مستقلة وفحص للسجلات والأنشطة لتقييم كفاية عناصر تحكم النظام للتأكد من موافقتها للسياسات وإجراءات التشغيل المقررة، وإصدار التوصيات حول ما هو ضروري من تغييرات في عناصر التحكم أو السياسات أو الإجراءات. |
| سجل الفحص والمراجعة | سجل يوضح من قام بالدخول إلى نظام تقنية معلومات والعمليات التي قام بتنفيذها أثناء فترة معينة. |
| يصدِّق على / يتحقق من هوية | التأكد من هوية جهة معينة عند تقديم تلك الهوية. |
| التصديق / التحقق من الهوية | التأكد من صحة هوية الخاصة بأحد المستخدمين أو العمليات أو الأجهزة. يكون ذلك عادة كأحد متطلبات السماح بالوصول إلى الموارد الموجودة في نظام معلومات معين. عملية تأسيس الثقة وتشمل التحقق من صحة الهوية والتحقق من مصدر الرسالة ومحتواها. عملية تهدف إلى تحديد مصدر المعلومات أو هوية جهة ما. |
| برتوكول التحقق من الهوية | عملية تبادل للرسائل محددة بدقة يجري خلالها التحقق من صحة امتلاك احد الرموز المميزة بغرض التحقق عن بعد من هوية الشخص الذي يطلب التعامل مع نظام معين. بعض برتوكولات التصديق تقوم بإنشاء مفاتيح تشفير تُستخدَم لتوفير الحماية طوال فترة التعامل مع النظام ولذلك تكون البيانات المنقولة خلال تلك الفترة محمية بفضل تشفيرها. |
| تصريح | قرار الإدارة الرسمية الصادر من أحد الكوادر العليا لهيئة ما لاعتماد الموافقة على تشغيل نظام معلومات والقبول علانيةً بتعريض عمليات تلك الهيئة للمخاطرة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) أو أصولها أو منسوبيها بناءاً على تنفيذ مجموعة من عناصر التحكم الأمني المتفق عليها. |
| استمرارية توفر الخدمة | التأكد من إمكانية الوصول إلى المعلومات واستخدامها في الوقت المناسب وبشكل يُعتمَد عليه. |
| الوعي بأمن المعلومات | الأنشطة التي تسعى لجذب انتباه الأفراد إلى موضوع أو مجموعة من الموضوعات في أمن المعلومات. |
| نسخة احتياطية | نسخة من الملفات والبرامج لتسهيل عملية الاسترجاع في حالة الضرورة. |
| الحد الأدنى من الأمن | الحد الأدنى من عناصر التحكم الأمنية المطلوبة لحماية نظام معلومات معين بناءاً على الاحتياجات المحددة لحماية سرية وتكامل و/أو استمرارية توفر خدمة هذا النظام. |
| تشفير القالب | خوارزمية تشفير متناظرة تُحوِّل قالب من المعلومات في وقت واحد مستخدمة مفتاح تشفير. من صفات تلك الخوارزمية أن طول قالب المدخلات هو نفس طول قالب المخرجات. |

| المصطلح | تعريف المصطلح |
|---|---|
| طريقة الاستقصاء في الهجوم على كلمة المرور | أسلوب لمحاولة الدخول على أحد الأجهزة التي تمثل عائقاً من خلال إجراء المحاولات باستخدام كلمات مرور متنوعة تجمع عدد من الحروف و/أو الأرقام. |
| إغراق ذاكرة التخزين المؤقت | شرط في قناة الاتصال يمكن من خلاله وضع عدد اكبر من المدخلات في منطقة مخصصة لاحتجاز البيانات بما يفوق قدرتها الاستيعابية لذلك من خلال استبدال المعلومات الموجودة بالكتابة عليها. يستخدم المهاجمون ذلك الشرط لإسقاط النظام أو إدخال شفرات خاصة تم إعدادها بمهارة عالية تسمح لهم بالسيطرة على النظام والتحكم فيه. |
| الهجوم بإغراق ذاكرة التخزين المؤقت | أسلوب التحميل الزائد للبيانات داخل مساحة محددة سلفاً في منطقة حفظ البيانات مما يؤدى إلى احتمالية الكتابة على الكتابة الموجودة في الذاكرة أو تخريبها. |
| خطة الحفاظ على استمرارية العمل | توثيق مجموعة من التعليمات والإجراءات المُعَدَّة سلفاً لوصف كيفية الحفاظ على وظائف العمل داخل منظمة معينة أثناء وبعد حدوث خلل خطير. |
| هيئة التوثيق | كيان موثوق يقوم بإصدار وإلغاء شهادات المفتاح العام. ذلك الكيان الموجودة في البنية التحتية للمفتاح العام حيث يتولى مسئولية إصدار الشهادات والتأكد من الالتزام بسياسة البنية التحتية للمفتاح العام. |
| إدارة التغيير | التخطيط، واختبار، وتنفيذ جميع جوانب عملية الانتقال من هيكل تنظيمي واحد أو عملية تجارية إلى آخر. |
| رئيس قطاع المعلومات | موظف الوكالة المسؤول عن:<br>• إسداء النصيحة ومد يد العون لرئيس الوكالة التنفيذي والآخرين من كوادر الإدارة العليا للتأكد من تحصيل تقنية المعلومات وترتيب موارد البيانات بشكل يتوافق مع القوانين والأوامر التنفيذية والتعليمات والسياسات واللوائح والأولويات التي أرساها رئيس الوكالة.<br>• إعداد وصيانة وتسهيل تطبيق بنية معلوماتية سليمة تتسم بالتكامل داخل الوكالة. |
| معلومات سرية / مصنفة | معلومات تم تصنيفها بناءاً على القرار التنفيذي رقم ١٣٢٩٢ أو أي قرارات تالية بغرض الحماية ضد الكشف غير المصرح به ويتم تميزها للإشارة إلى سريتها عند تحويلها إلى الأرشيف كملفات وثائقية. |
| العميل (برنامج/تطبيق) | أحد مكونات نظام معين عادة ما تكون عملية حاسوبية تعمل نيابة عن أحد العناصر البشرية حيث تستفيد من أحد الخدمات التي يوفرها خادم معين. |
| عناصر التحكم المكافئة | عناصر التحكم الإدارية والتشغيلية والفنية مثل إجراءات الوقاية وعوامل المقاومة التي يتم العمل بها داخل منظمة بدلاً من عناصر التحكم الموصى بها في الحد الأدنى من عناصر التحكم الأمني المنخفض أو المتوسط أو المرتفع بغرض توفير درجة مساوية أو مكافئة من الحماية لنظام معلومات معين. |

| المصطلح | تعريف المصطلح |
| --- | --- |
| حادثة أمن الحاسوب | انتهاك أو تهديد خطير بانتهاك السياسات الأمنية للحاسوب أو سياسات الاستخدام المتفق عليها أو الممارسات القياسية لأمن الحاسوب. |
| التحكم في تهيئة/إعدادات النظام | عملية للتحكم في إجراء التغييرات للأجهزة والبرمجيات وبرامج التشغيل المثبتة في ذاكرة القراءة والوثائق للتأكد من حماية نظام المعلومات ضد التغييرات الخاطئة قبل أو أثناء أو بعد تطبيق النظام. |
| الضوابط | الضوابط التي هي الضمانات أو تنفيذ تدابير للحد من المخاطر الأمنية. |
| ملفات جمع البيانات | معلومة يُرسلها خادم الويب إلى برنامج المتصفح مرفقة بالمورد المطلوب. يقوم المتصفح بتخزين تلك المعلومة مؤقتاً على أن يعيدها لخادم الويب مرة أخرى في الزيارات أو الطلبات التالية. |
| قواعد الارتباط | في الرصد والإبلاغ الأمن عن شروط وقواعد مكتوبة بطريقة أنه كلما منفصلة الأحداث الفريدة تحدث معا هم ذكرت لمزيد من التحقيق. |
| عوامل المقاومة | أعمال أو أدوات أو إجراءات أو أساليب أو معايير أخرى تعمل على تقليل الثغرات الأمنية في نظام المعلومات. تعتبر مرادفاً لعناصر التحكم الأمني وإجراءات الوقاية. |
| التشفير باستخدام دالة الاختزال | دالة تحول سلسلة نصية من وحدات البت ذات الطول العشوائي إلى سلسلة محددة الطول من وحدات البت. تتميز دالة الاختزال الصادر بشأنها موافقة بالمواصفات التالية:<br>• (وحيدة الاتجاه) بمعنى أنه من غير المُمكن رياضياً الحصول على مُدخَل يمكن تحويله إلى مُخرج محددة سلفاً.<br>• (مقاومة للتعارُض) فمن غير الممكن رياضياً الحصول على أي مدخلين مختلفين يتحولان إلى نفس المخرج. |
| مفتاح تشفير | قيمة تُستخدم في العمليات التشفيرية مثل فك التشفير والتشفير وإصدار التوقيع أو التحقق من صحته. معيار يُستَخدم بالاقتران مع خوارزمية تشفير حيث يقوم بتحديد التشغيل المخصص لتلك الخوارزمية. معيار يُستَخدم مقترناً بخوارزمية تشفير لتحديد. تحويل البيانات من النص البسيط إلى نص مُشفر. تحويل النص المشفر إلى نص غير مُشفَّر. حساب التوقيع الالكتروني من البيانات. التحقق من صحة التوقيع الرقمي المحسوب من البيانات. شفرة التصديق المحسوبة من البيانات أو اتفاقية تبادل لأحد الأسرار المشتركة. |

| المصطلح | تعريف المصطلح |
|---|---|
| التشفير | ذلك الفرع من فروع المعرفة الذي يهتم بتقديم مبادئ ووسائل وأساليب تحويل البيانات بغرض إخفاء ما تحويه من دلالات لفظية ومنع استخدامها دون تصريح وكذلك منع تغييرها. ذلك الفرع من المعرفة الذي يهتم بتقديم المبادئ والوسائل والأساليب التي توفر أمن المعلومات بما في ذلك السرية وتكامل البيانات وعدم الإنكار والمصداقية. وينقسم إلى مفتاح سري أو مفتاح عام. تشفير المفتاح السري يعتمد على استخدام مفتاح تشفير واحد مشترك بين طرفين. نفس المفتاح يستخدم في تشفير وفك تشفير البيانات. يحتفظ الطرفين بهذا المفتاح سراً. أما تشفير المفتاح العام فانه يستخدم مفتاحين أحدهما مفتاح عام والأخر مفتاح خاص. كلا المفتاحين مرتبط بالأخر ولكن للمفتاح العام خاصية وهي انه لن يجدي اشتقاق المفتاح الخاص(FIPS 140-1). في نظام تشفير المفتاح العام يمتلك كلا الطرفين زوج يضم مفتاح عام وأخر خاص. المفتاح العام متاح لأي شخص بينما يجب الاحتفاظ بسرية المفتاح الخاص. |
| علم الشفرات | هو ذلك العلم الذي يتعامل مع الاتصالات المخفية والمتنكرة والمشفرة ويضم أمن الاتصالات واستخبارات الاتصالات. |
| خوارزمية تشفير البيانات | محرك تشفير يُستخدَم بواسطة خوارزمية التشفير الثلاثية للبيانات. |
| تكامل البيانات | خاصية عدم تغيير البيانات بطريقة غير مُصرَح بها. يغطى مفهوم التكامل البيانات في مرحلة تخزينها وأثناء معالجتها وأثناء مراحلها الانتقالية. |
| فك التشفير | عملية تحويل نص التشفير إلى نص غير مُشفَّر. عملية تغيير نص تشفير إلى نص غير مُشفَّر باستخدام خوارزمية ومفتاح تشفير. تحويل نص تشفير إلى نص بسيط باستخدام خوارزمية تشفير. |
| منطقة محايدة | شبكة مكونة من بربط اثنين من جدران الحماية. الأنظمة التي يتم الوصول إليها عن بعد ولكنها تحتاج لقدر من الحماية عادة ما توضع في شبكات المنطقة المحايدة. |
| تعطيل الخدمة | منع الوصول المصرح به إلى الموارد أو تأخير العمليات التي يكون فيها الوقت عاملاً حرجاً. (ربما يقاس الوقت عندما يكون عاملاً حرجاً بالملي ثانية أو بالساعات اعتماداً على الخدمة المقدمة). |
| التحكم. المباحث | التحكم. المباحث كشف عن نتائج غير مرغوب فيها، بعد وقوعها. هم أقل فعالية من الضوابط الوقائية. |
| خوارزمية التوقيع الرقمي | خوارزميات غير متناظرة تُستخدَم لتوقيع البيانات رقمياً. |
| خطة معالجة الكوارث | خطة مكتوبة لمعالجة التطبيقات الحرجة في حالة تعطل الأجهزة والبرامج الرئيسية أو تعرض المنشأة للدمار. |
| حجب الخدمة الموزَّع | أسلوب لحجب الخدمة باستخدام العديد من أجهزة المضيف بغرض تنفيذ الهجوم. |
| مجال / نطاق | مجموعة من الأطراف الفاعلة وعناصر معلوماتها بالإضافة إلى سياسة أمن مشترك. |
| حدث | أي حدث يسترعى الملاحظة في الشبكة أو النظام. |

| المصطلح | تعريف المصطلح |
| --- | --- |
| شهادة | المعلومات التي إما وحدها أو عندما تستخدم بالاقتران مع معلومات أخرى تستخدم لإثبات حول حدث أو عمل. ملاحظة – الإثبات لا يثبت بالضرورة الحقيقة أو وجود لشيء إلا أنها تسهم في إقامة الحجة. |
| شفرة الاقتحام | تقنية أو رمز يستخدم الضعف لتوفير نظام الحصول على المهاجم. |
| جدار حماية | بوابة تتحكم في الوصول بين الشبكات طبقاً لسياسة الأمن المحلية. |
| هاكر | فرد مع تقارب لأجهزة الكمبيوتر. قراصنة قبعة بيضاء مفتون بها التحدي الفكري لتمزق أنظمة الكمبيوتر لتحسين أمن الكمبيوتر. قراصنة قبعة سوداء عمدا نظم تحطم الطائرة، سرقة كلمات السر، الخ، وليس بالضرورة لتحقيق مكاسب مالية. |
| دالة الاختزال | دالة تحول سلسلة نصية من وحدات البت ذات الطول غير المحدد إلى سلسلة محددة الطول من وحدات البت. تتميز دالة الاختزال الصادر بشأنها موافقة بالمواصفات التالية:<br>• (وحيدة الاتجاه) بمعنى أنه من غير المُمكن حسابياً يتحول مدخل إلى مخرج محدد سلفاً.<br>• (مقاومة للتعارُض) بمعنى أنه من غير الممكن حسابياً أن يتحول مدخلان مختلفان إلى نفس المخرج. دالة حسابيــة صادر بشأنها موافقة تقوم بتحويل سلسلة نصية ذات طول غير محدد إلى سلسلة نصية محددة الطـول. يمكـن استخدامها لإنتاج مجموع تدقيقـي يُسمّى بـ «قيمة الاختزال» أو «موجـز الرسالة» لسلسلة نصية أو رسالة طويلة. |
| كشف الهوية | إجراءات للتحقق من هوية مستخدم أو عملية أو جهاز تُمثِل عادة أحد الشروط المسبقة للحصول على حق الوصول إلى أحد الموارد في نظام لتقنية المعلومات. إجراءات اكتشاف الهوية الحقيقية (على سبيل المثال المصدر والبيانات التاريخية المبدئية) لشخص أو عنصر من مجموعة تضم أشخاص أو عناصر متشابهة. |
| نظام اكتشاف الاختراقات المعتمد على المضيف | هي نظم اكتشاف الاختراقات التي تعمل على البيانات المُجمَّعة من داخل أحد أنظمة الحاسوب. تمنح تلك الأفضلية أنظمة اكتشاف الاختراقات المعتمدة على المضيف إمكانية أن تحدد بالضبط أي العمليات وأي حسابات المستخدمين التي تورطت في هجوم معين على نظام التشغيل بل وإنه على عكس أنظمة اكتشاف الاختراقات المعتمدة على الشبكة فان تلك الأنظمة تستطيع اكتشاف النتيجة المقصودة من محاولة هجوم معينة لأنها تستطيع الوصول مباشرة ومراقبة ملفات البيانات وعمليات النظام التي عادة ما يتم استهدافها في الهجمات. |
| نظام اكتشاف الاختراقات المعتمد على الشبكة | أنظمة اكتشاف الاختراقات التي تتبع الهجمات من خلال التقاط وتحليل حزم البيانات الموجودة في الشبكة. بالاستماع إلى الإشارات داخل الشبكة أو المُبَدِل يستطيع نظام اكتشاف الاختراقات المعتمد على الشبكة مراقبة تدفق البيانات الذي يؤثر في العديد من أجهزة المضيف المرتبطة بإشارة الشبكة. |

| المصطلح | تعريف المصطلح |
|---|---|
| صورة | نسخة مُحكمة (طبق الأصل) لكل البيانات الالكترونية الموجودة على أحد الأجهزة. يتم عمل تلك النسخة بطريقة تضمن عدم تغير المعلومات. |
| تأثير | حجم الضرر المتوقع أن ينتُج من تداعيات الإفصاح عن البيانات أو تغييرها أو تدميرها دون تصريح أو فقد المعلومات وانقطاع استمرارية توفر نظام المعلومات. |
| حادثة | انتهاك أو تهديد خطير بانتهاك السياسات الأمنية للحاسوب أو سياسات الاستخدام المتفق عليها أو الممارسات القياسية لأمن الحاسوب. حادثة قد تعرض بالفعل أو تجعل من المحتمل تعرض سرية نظام معلومات أو تكامله أو استمرارية توفر خدمته أو عملياته أو مخازن بياناته للخطر أو قد تنقل أو تُشكِّل انتهاكاً أو تهديداً خطيراً لسياسته الأمنية أو إجراءاته الأمنية أو سياسات استخدامه المقبولة. |
| معالجة الحوادث | التخفيف من انتهاكات السياسات الأمنية والتعريف بالممارسات المُوصى بها. |
| خطة معالجة الحوادث | توثيق مجموعة من التعليمات والإجراءات المُعَدّة سلفاً لاكتشاف ومعالجة والحد من تداعيات الهجمات الالكترونية الخبيثة ضد أنظمة تقنية المعلومات الخاصة بأحد المنظمات. |
| مالك المعلومات | موظف يمتلك السلطة القانونية أو التشغيلية لمعلومات محددة والمسئولية عن إنشاء عناصر التحكم الخاصة بإصدارها وتجميعها ومعالجتها ونشرها والتخلص منها. |
| أمن المعلومات | حماية المعلومات وأنظمتها من الوصول أو الاستخدام أو الإفصاح أو الخلل أو التغيير أو التدمير غير المُصرَّح به بهدف توفير سرية تلك المعلومات وتكاملها واستمرارية توفرها. حماية المعلومات وأنظمتها من الوصول أو الاستخدام أو الإعلان أو الخلل أو التغيير أو التدمير غير المصرَّح به لتوفير:<br>• التكامل الذي يعنى الحماية ضد تغيير المعلومات وتدميرها كما يشمل أيضاً التأكد من مصداقية المعلومات وعدم إنكارها.<br>• السرية التي تعني استعمال قيود مرخصة للوصول إلى المعلومات والإعلان عنها بما في ذلك وسائل حماية الخصوصية وحق ملكية المعلومات<br>• استمرارية توفر البيانات بمعنى التأكد من إتاحة الوصول للمعلومات واستخدمها في الحال وبشكل يُعتمد عليه. |
| الحدث معلومات الأمن | حدثا حددت وجود نظام أو خدمة أو شبكة الدولة مما يدل على انتهاك محتمل لسياسة أمن المعلومات أو فشل الضمانات، أو في حالة لم تكن معروفة سابقا الأمنية التي قد تكون ذات صلة |
| مالك نظام المعلومات (أو مدير البرنامج) | موظف مسؤول عن كل عمليات إمدادات نظام المعلومات أو تطويره أو تكامله أو تغييره أو تشغيله أو صيانته. |

| المصطلح | تعريف المصطلح |
| --- | --- |
| تقنية المعلومات | أي جهاز أو نظام مرتبط أو نظام فرعي لجهاز معين تستخدمه وكالة تنفيذية في الحصول على المعلومات أو البيانات آلياً أو تخزينها أو معالجتها أو إدارتها أو تحريكها أو التحكم بها أو عرضها أو توجيهها أو تغييرها أو نقلها أو استقبالها. لتحقيق الأغراض السابقة يتم استخدام الأجهزة بواسطة الوكالة التنفيذية وسواء كان استخدام تلك الأجهزة مباشراً مقبل الوكالة التنفيذية أو بواسطة مقاول بموجب عقد ابرمه مع الوكالة التنفيذية يتطلب ذلك ما يلي:<br>• استخدام تلك الأجهزة.<br>• أن يكون الاستخدام بأكبر قدر في أداء أحد الخدمات أو تزويد أحد المنتجات. يتضمن مصطلح تقنية المعلومات الحواسيب والأجهزة الملحقة والبرامج وبرامج التشغيل المثبتة في ذاكرة القراءة والإجراءات المشابهة والخدمات (شاملةً خدمات الدعم) والموارد المتعلقة بذلك. |
| سياسة أمن المعلومات | مجموعة من التوجيهات واللوائح والقواعد والممارسات التي ترشد إلى كيفية قيام منظمة بإدارة وحماية وتوزيع المعلومات. |
| تصفية حزم البيانات الواردة | عملية رفض لحزم البيانات القادمة والتي يتضح استخدامها لعناوين وهمية لبروتوكول الانترنت مثل عناوين المصدر المحجوزة |
| المبادرات | لغرض هذا الإطار، خطط العمل التي تم تحديدها بوصفها وسيلة لملء الفجوات والحد من المخاطر التي تم تحديدها خلال مرحلة تقييم المخاطر. |
| التكاملية | الحماية ضد تغير المعلومات بشكل خاطئ أو تدميرها وكذلك التأكد من عدم إنكار البيانات والتأكد صحة التصديق. خاصية عدم تعرض البيانات الحساسة للتغيير أو الحذف بطريقة غير مُصرَّح بها ولا يمكن اكتشافها. |
| الملكية الفكرية | ما هو مفيد من معلومات أدبية وتقنية و/أو صناعية ومعرفة أو أفكار تبين الملكية وتتحكم في الاستخدام الملموس أو الافتراضي و/أو طريقة العرض. |
| نظام اكتشاف الاختراقات | برنامج يقوم بالبحث عن الأنشطة المثيرة للريبة وتوجيه تنبيه لمديري النظام. |
| أنظمة منع الاختراقات | أنظمة تستطيع اكتشاف الأنشطة التي تهدف لاختراق النظام وتستطيع أيضاً محاولة وقف تلك الأنشطة قبل الوصول لأهدافها. |
| عنوان بروتوكول الانترنت | هو رقم فريد غير قابل للتكرار يتم تخصيصه للحاسوب بغرض تحديد المكان الذي توجه إليه الرسائل المنقولة عبر الانترنت. عنوان بروتوكول الانترنت يشبه رقم المنزل الذي توجه إليه الرسائل في البريد العادي. |

| المصطلح | تعريف المصطلح |
| --- | --- |
| معيار أمن بروتوكول الانترنت (IPsec) | أحد المعايير الصادرة عن معهد المهندسين الالكترونين والكهربائيين تحت طلب التعليق رقم (٢٤١١) حيث يوفر ذلك البروتوكول إمكانيات الأمن لطبقة الاتصالات في بروتوكول الانترنت. يُستخدَم بروتوكول إدارة المفتاح الخاص بمعيار أمن بروتوكول الانترنت في التفاوض حول المفاتيح السرية التي تحمي الاتصالات عبر الشبكة الخاصة الافتراضية بالإضافة إلى تحديد مستوى ونوع الحماية الأمنية التي تميز الشبكة الخاصة الافتراضية. أكثر بروتوكولات إدارة المفاتيح انتشاراً هو بروتوكول تبادل مفاتيح الانترنت. |
| المخاطر المتعلقة بتقنية المعلومات | التأثير الذي تحدثه الشبكة على الأعمال أو المهام فيما يخص:<br>• احتمالية قيام أحد مصادر التهديد باستغلال أو استهداف الثغرات الأمنية في أحد أنظمة المعلومات.<br>• التأثير الناتج إذا حدث ذلك. تنشأ مخاطر تقنية المعلومات من المسؤولية القانونية أو فقد المهام/الأعمال نتيجة لما يلي على سبيل المثال وليس الحصر: الإفصاح عن المعلومات أو تغييرها أو تدميرها دون تصريح سواء حدث ذلك نتيجة طريقة خبيثة أو غير خبيثة أو مصادفة الأخطاء وعملية الحذف غير الخبيثة. جوانب الخلل التي تصيب تقنية المعلومات نتيجة للكوارث الناتجة عن الطبيعة أو البشر الفشل في توفير الاهتمام والجهد المناسب لتطبيق وتشغيل أنظمة تقنية المعلومات. |
| الوعي بأمن تقنية المعلومات | الغرض من العروض التوعوية هو ببساطة تركيز الانتباه على الأمن حيث تسمح تلك العروض للأفراد بمعرفة شئون أمن تقنية المعلومات وبالتالي الاستجابة لتلك المعرفة. |
| إدارة المفاتيح | هي تلك الأنشطة التي تتطلب معالجة مفاتيح التشفير وما يتعلق بها من معايير أمن أخرى (مثل متجهات بداية التشفير وكلمات المرور) أثناء الدورة الكاملة للمفاتيح شاملة إصدارها وتخزينها وإنشاءها وإدخالها وإخراجها وتحويلها للقيمة الصفرية. |
| زوج مفاتيح | زوج من المفاتيح المرتبطة حسابياً يتميزان بالخواص التالية:<br>• أحد المفتاحين يمكن استخدامه في تشفير أحد الرسائل التي لا يمكن فك تشفيرها إلا بواسطة المفتاح الأخر.<br>• حتى في حالة معرفة أحد المفاتيح يظل اكتشاف المفتاح الأخر غير قابل للتنفيذ رياضياً. أحد المفاتيح العامة وما يتفق معه من المفاتيح الخاصة يمثلان زوج من المفاتيح ذات خوارزمية مفتاح عام. |
| الحد الأدنى من الامتيازات | الهدف الأمني من منح المستخدمين صلاحيات الوصول التي يحتاجونها لتنفيذ مسؤولياتهم الرسمية فقط. |
| التحكم منطقية بالوصول | منع الاستخدام غير المصرح به من الموارد، بما في ذلك منع استخدام الموارد بطريقة غير مشروعة. |

| المصطلح | تعريف المصطلح |
| --- | --- |
| الشفرة الخبيثة | أحد البرامج أو برامج التشغيل المثبتة في ذاكرة القراءة والتي تقوم بتنفيذ عملية غير مصرَّح بها فتُحدِث تأثيراً مضاداً على السرية أو التكاملية أو استمرارية توفر نظام معلومات. أحد البرمجيات الخبيثة التي تصيب جهاز المضيف مثل الفيروس أو الدودة أو حصان طروادة أو غيرها من كيانات المعتمدة على الشفرة. |
| إدارة عناصر التحكم | عناصر التحكم الأمنية مثل إجراءات الوقاية وعوامل المقاومة الخاصة بأحد أنظمة المعلومات والتي تُركِّز على إدارة المخاطر وإدارة النواحي الأمنية المتعلقة بذلك النظام. |
| وسائل نقل البيانات | الوسائل التي تُسجَّل عليها المعلومات أو تُخزَّن أو تُطبَع داخل أحد أنظمة المعلومات مثل الأدوات المادية وأسطح الكتابة التي تشمل على سبيل المثال وليس الحصر الأشرطة الممغنطة والأقراص الضوئية والأقراص الممغنطة وشرائح الذاكرة ذات التكامل واسع النطاق والمطبوعات (لكنها لا تضم وسائل العرض). |
| تطهير البيانات | مصطلح عام يُطلَق على الإجراءات التي يتم اتخاذها لجعل البيانات -المكتوبة على أحد الوسائل- غير قابلة للاسترجاع سواء بواسطة الأدوات المعتادة أو غير المعتادة. |
| مذكرة تفاهم/ مذكرة اتفاق | مستند تم إعداده بين طرفين أو أكثر لتحديد ما يخصهم من مسؤوليات في إنجاز هدف معين أو مهمة معينة. في هذا الدليل تحدد «مذكرة التفاهم/ مذكرة الاتفاق» المسؤوليات الملقاة على طرفين أو أكثر من المنظمات في إقامة وتشغيل وتأمين الوصلات البينية للنظام. |
| الشفرة المتنقلة | برامج أو أجزاء من برامج تُحصَّل من أنظمة معلومات بعيدة وتُنقل عبر شبكة وتُنفَذ على أحد أنظمة المعلومات المحلية دون الحاجة إلى قيام المستقبِل بتثبيتها أو تنفيذها. |
| عدم الإنكار | تأكيد على أن مُرسِل المعلومات حاصل على إثبات لتسليمها وأن متلقي تلك المعلومات قد ورد له إثبات لهوية المُرسِل بحيث لا يستطيع أحدهما إنكار قيامه بمعالجة المعلومات. هي الخدمة الأمنية التي بها لا تستطيع الكيانات المشاركة فيها أحد عمليات الاتصال إنكار تلك المشاركة وبشكل أكثر تفصيلاً فان الكيان المُرسِل لا يستطيع إنكار قيامه بإرسال رسالة (دليل عدم إنكار المصدر) والكيان المستقبل لا يستطيع إنكار تسلمُه لتلك الرسالة (دليل عدم إنكار التسليم). |
| كلمة مرور | سر يحتفظ به مقدم الطلب في ذاكرته ويستخدمه للتصديق على هويته. عادة ما تكون كلمات المرور على شكل سلاسل حرفية و/أو رقمية. هي سلسلة حرفية محمية تُستخدَم في التصديق على هوية مستخدم نظام حاسوب أو التصريح بالوصول إلى موارد النظام. سلسلة حرفية (الحروف الهجائية، الأرقام، والرموز الأخرى) تستخدم للتصديق على الهوية أو التحقق من مشروعية تصريح الوصول. |
| الاصطياد الالكتروني | ممارسة الخداع على الأفراد حتى يكشفوا عن معلومات شخصية حساسة من خلال وسائل خداع تعتمد على الحاسوب. |

| المصطلح | تعريف المصطلح |
|---|---|
| سياسة | وثيقة تبين هيكلية إدارة الأمن وتحدد بوضوح المسؤوليات الأمنية وتضع الأساس اللازم لقياس الأداء ومدى الالتزام بشكل يُعتمد عليه. |
| منفذ | نقطة دخول أو خروج مادية لوحدة تشفير نمطية توفر للإشارات المادية المتمثلة في التدفق المنطقي للمعلومات إمكانية الوصول لتلك الوحدة النمطية (مع العلم بأن المنافذ المنفصلة مادياً لا تتشارك في نفس موضع التركيب أو السلك). |
| فحص المنافذ | استخدام برنامج لتحديد المنافذ المفتوحة في أحد الأنظمة عن بعد (مثلاً لمعرفة هل الأنظمة تسمح بإجراء اتصالات من خلال تلك المنافذ). |
| الخصوصية | تحديد إمكانية الوصول إلى معلومات المشتركين أو الطرف التابع طبقاً للقانونين الحكومية وسياسة الوكالة. |
| المشروع | المشروع هو عبارة عن مسعى المؤقتة المتخذة لخلق منتجات فريدة من نوعها، خدمة أو نتيجة. مشاريع لها تاريخ بداية ونهاية أكيدة. |
| إدارة المشروع | تطبيق المعارف والمهارات والأدوات والتقنيات لتحقيق أهداف المشروع |
| معالم المشروع | الأحداث الهامة في إطار الجدول الزمني للمشروع. |
| خادم الوكيل | خادم يقع بين تطبيق العميل مثل متصفح الويب والخادم الحقيقي حيث يعترض كل الطلبات الموجهة إلى الخادم الحقيقي ليرى ما إذا كانت لديه القدرة على الوفاء بتلك الطلبات بنفسه وإلا فانه يقوم بتوجيهها إلى الخادم الحقيقي. |
| البنية التحتية للمفتاح العام | مجموعة من السياسات والعمليات ومنصات الخادم والبرمجيات والأجهزة تُستخدم بغرض إدارة الشهادات وأزواج المفتاح العام والخاص بما في ذلك القدرة على إصدار والاحتفاظ وإلغاء شهادات المفتاح العام. هيكلية تُستخدم في ربط المفاتيح العامة بالكيانات وتمكين كيانات أخرى من التحقق من صحة روابط المفتاح العام بالإضافة إلى إمكانية سحب تلك الروابط وتوفير خدمات أخرى ذات أهمية لإدارة المفاتيح العامة. |
| الوصول عن بعد | وصول المستخدمين (أو أنظمة معلومات) للاتصال خارجياً بمحيط الأمن الخاص بأحد أنظمة المعلومات. |
| مستودع بيانات | قاعدة بيانات تحتوى على معلومات وبيانات متعلقة بالشهادات كما حددتها سياسة الشهادة. وقد يُشار إلى مستودع البيانات بكونه أشبه بدليل. |
| المخاطر المتبقية | الجزء المتبقي من المخاطر المحتملة بعد تطبيق كافة مقاييس الأمن. توجد دائماً مخاطر متبقية تتعلق بكل تهديد. |

| المصطلح | تعريف المصطلح |
|---|---|
| مخاطرة | مستوى التأثير الذي تتلقاه عمليات الوكالة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) أو أصولها أو منسوبيها نتيجة تشغيل نظام معلومات مع الوضع في الاعتبار التأثير المحتمل لأحد أنواع التهديدات والاحتمالية حدوث ذلك التهديد. |
| تقييم المخاطر | عملية تشخيص المخاطر التي تهدد عمليات الوكالة (بما في ذلك رسالتها ووظائفها ومصداقيتها وسمعتها) أو أصولها أو منسوبيها من خلال تحديد احتمالية حدوث تلك المخاطر والتأثير الناتج عنها وعناصر التحكم الإضافية التي من شأنها تخفيف ذلك التأثير. يعد تقييم المخاطر جزءاً من إدارة المخاطر ومرادفاً لتحليل المخاطر حيث يعمل على تحليل التهديدات والثغرات الأمنية. |
| حذف البيانات نهائياً | عملية لإزالة المعلومات من وسائط التخزين بحيث لا يُمكن استعادتها. يتضمن ذلك نزع كل الملصقات والعلامات وكذلك سجلات النشاط. |
| بروتوكول الاتصال الآمن | بروتوكول للاتصال يوفر حداً مناسباً من حماية السرية والتصديق وتكاملية المحتوى. |
| سجل الأحداث الأمنية | سجل الأحداث الأمنية (مثل تسجيل الدخول/ تسجيل الخروج النجاح أو الفشل، والأحداث الارتباط) التي ترتبط مع طابع تاريخ |
| البقعة الأمنية | رمز البرنامج الذي يحل محل رمز أو تحديثات أخرى. كثيرا ما تستخدم بقع لتصحيح الثغرات الأمنية. |
| سياسة أمنية | بيان بالحماية المطلوبة لعناصر المعلومات. السياسة الأمنية هي توجيهات الإدارة العليا لإنشاء برنامج أمني قائم على الحاسوب وتحديد أهدافه ومسؤولياته. مجموعة من المعايير الخاصة بشروط الخدمات الأمنية حيث تبين وتحدد الأنشطة الخاصة بمنشأة معالجة بيانات بغرض الحفاظ على حالة من الأمن للأنظمة والبيانات. |
| حساسية البيانات | تستخدم في هذا الدليل الإرشادي لتعني مقياس للأهمية المُعطَاة للمعلومات من قِبَل مالكها بغرض إظهار مدى احتياجها للحماية. |
| مستويات الحساسية | نظام تدريجي يمنح علامات (منخفض، معتدل، مرتفع) للمعلومات أو أنظمة معالجة المعلومات بناءاً على التهديدات والمخاطر الناتجة في حالة تنفيذ أحد التهديدات بنجاح. |
| توقيع | نموذج معروف ومُميَّز مرتبط بأحد الهجمات مثل السلسلة الثانية في أحد الفيروسات أو مجموعة معينة من ضربات لوحة المفاتيح التي تُستخدم للحصول على وصول غير مصرح به إلى النظام. |
| الهندسة الاجتماعية | محاولة لخداع شخص لكي يكشف عن معلومات (كلمة مرور مثلاً) بغرض استخدامها في الهجوم على الأنظمة أو الشبكات. |

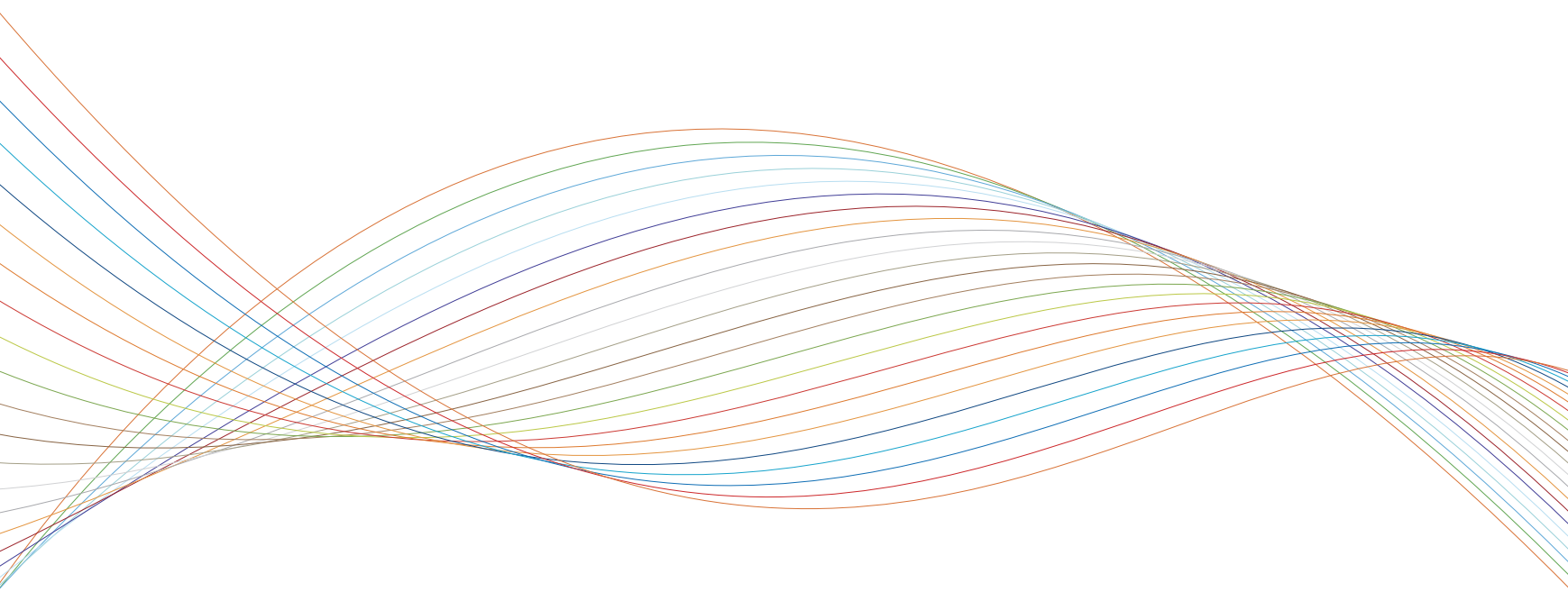
| المصطلح | تعريف المصطلح |
|---|---|
| خداع بروتوكول الانترنت | يشير «خداع بروتوكول الانترنت» إلى إرسال حزمة بيانات عبر شبكة بحيث تبدو إنها تأتى من مصدر غير مصدرها الفعلي ويتضمن ذلك:<br>• القدرة على استقبال رسالة من خلال التنكر كما لو كان هو مقر الوصول الشرعي للتسليم.<br>• التنكر كما لو كان الجهاز المرسل ثم يرسل رسالة إلى أحد جهة الاستلام. |
| برامج تجسس | برامج مثبتة في أحد أنظمة المعلومات سراً أو خلسة لجمع المعلومات عن الأفراد أو المنظمات دون علمهم أي انه أحد أنواع الشفرة الخبيثة. |
| الحقن SQL | نوع من الهجوم نفذ عن طريق الحقن من الشيفرات الخبيثة في الأمر مزود. الحقن يحدث عندما الموفر المستخدم يتم إرسال البيانات إلى مترجم كجزء من قيادة مزود أو الاستعلام. المهاجم الحيل بيانات معادية للمترجم في تنفيذ الأوامر غير مقصودة أو تغيير البيانات. |
| SSID | معرف فريد تستخدم للتمييز بين مختلف الشبكات المحلية اللاسلكية. |
| SSL | نظام التشفير المتقدمة من نتسكيب. خدمة تصميم المواقع يحمي خصوصية البيانات المتبادلة بين الموقع والمستخدمين الفردية. يتم استخدامه من قبل المواقع التي تبدأ مع أسماء https. |
| معيار/ مقياس | بيان منشور حول موضوع يحدد تلك المواصفات –التي عادة تكون قابلة للقياس– الواجب استيفاءها أو تحقيقها للتماشي مع ذلك المعيار. |
| التفتيش Stateful | جدار حماية تقنية التفتيش وذلك بفحص الغرض المرجو من الاتصالات للتأكد من صحتها. على سبيل المثال، في بلاغ يدعي للرد على الطلب مقارنة مع جدول الطلبات المعلقة. |
| مفتاح متناظر | مفتاح تشفير يُستخدم لتنفيذ عملية تشفير ومعكوسها على سبيل المثال القيام بالتشفير وفك التشفير أو إنشاء شفرة رسالة تصديق والتحقق من صحتها. مفتاح تشفير مفرد يُستخدَم مع أحدى خوارزمية مفتاح سري متناظر. |
| نظام | مجموعة من موارد المعلومات المنفصلة مُرتبة بغرض تجميع أو معالجة أو صيانة أو استخدام أو مشاركة أو توزيع أو التخلص من المعلومات. |
| مدير النظام | هو الشخص الذي يدير النواحي التقنية لأحد الأنظمة. |
| دورة حياة النظام | مدى الأنشطة المرتبطة بالنظام والتي تضم إنشاء النظام وتطويره وامتلاكه وتنفيذه وتشغيله وصيانته والتخلص منه بالكامل بحيث يدفع إلى البدء في إنشاء نظام أخر. |

| المصطلح | تعريف المصطلح |
|---|---|
| تكاملية/سلامة/وحدة النظام | هي تلك الميزة التي يمتلكها النظام عند تنفيذه للوظيفة المقصودة منه بطريقة لا يشوبها أي تقصير، بطريقة خالية من أي تلاعب غير مصرح به سواء كان تلاعب مقصود أو غير مقصود. |
| تهديد | أي ظرف أو حدث من المحتمل أن يؤثر تأثيراً معادياً على أعمال الوكالة (بما في ذلك مهمتها أو وظائفها أو مصداقيتها أو سمعتها) أو أصولها أو منسوبيها مستغلاً أحد أنظمة المعلومات عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تغييرها و/أو حجب الخدمة. وأيضاً قدرة مصدر التهديد على النجاح في استغلال أحد نقاط الضعف الخاصة بنظام معلومات معين. |
| اشارة السماح / رمز مُميِّز | شئ (عادة ما يكون مفتاح أو كلمة مرور) يمتلكه مقدم الطلب ويتحكم فيه بحيث يستخدم فى التصديق على هوية مقدم الطلب. |
| معيار التشفير الثلاثي للبيانات | تطبيق لخوارزمية معيار تشفير البيانات باستخدام ثلاث مسارات لخوارزمية معيار تشفير البيانات بدلاً من استخدام واحدة فقط كما في التطبيقات العادية لمعيار تشفير البيانات. يوفر معيار التشفير الثلاثي للبيانات تشفيراً أكثر قوة من المعيار العادي ولكنه أقل أمناً من المعيار المتقدم للتشفير. |
| حصان طروادة | برنامج لا يقوم بنسخ نفسه حيث يتظاهر بكونه ذو أغراض مفيدة ولكنه في الحقيقة يخفى غرض خبيث. |
| المصادقة اثنين عامل | المصادقة تجهيز باستخدام اثنين من العوامل، عادة : لديك شيء وشيء تعرفه. |
| مُستخدَم | أحد الأفراد أو عمليات (النظام) مصرح له الوصول إلى أحد أنظمة المعلومات. أحد الأفراد أو العمليات (طرف فاعل) ينوب عن الشخص الذي له حق الوصول إلى أحد وحدات التشفير النمطية بغرض الحصول على خدمات مُشفرَة. |
| إنشاء مُستخدِم | مرحلة في دورة تكوين مفتاح التشفير بموجبها يقوم المستخدم بإنشاء تطبيقه المُشفَّر (مثلاً تثبيت وإعداد برنامج أو أحد الأجهزة). |
| تسجيل مستخدم | مرحلة في دورة تكوين مفتاح التشفير بموجبها يصبح أحد الكيانات عضواً في أحد النطاقات الأمنية. |
| عنصر بيانات صحيح | البيانات المرسلة عبر الشبكة أو سلسلة البيانات المرفقة أو القيم المؤقتة التي تفي بالقيود الخاصة بوظيفة التنسيق. |
| التحقق من الصلاحية | عملية تبين أن النظام موضع الاهتمام يلبى كافة المواصفات المطلوبة في جميع الجوانب. |
| التحقق من الهوية | التأكد من صحة الهوية التي تم إدعاءها عن طريق المقارنة بين إدعاءات الهوية المقدمة والمعلومات الصحيحة المخزنة سلفاً في بطاقة الهوية أو نظام التحقق من صحة الهوية الشخصية. |

| المصطلح | تعريف المصطلح |
|---|---|
| شبكة خاصة افتراضية | هي شبكة افتراضية مُنشأة في طبقة التطبيق من نموذج نظام الاتصال المفتوح فوق شبكة مادية الموجود بالفعل ولكنها عادة لا تضم كل نقاط الاتصال الموجودة في تلك الشبكة المادية. |
| فيروس | برنامج يقوم بنسخ نفسه ذاتياً بحيث يقوم بالعمل والانتشار عن طريق إحداث تغييرات في برامج وملفات الأخرى. |
| إنذار كاذب | رسالة إنذار عاجل عن فيروس غير موجود. |
| VLAN | شبكات المنطقة المحلية التي تسمح المضيفين على قطاعات مختلفة للاتصال الجسدي كما لو كانت متصلة بجهاز تبديل شبكة واحد. شبكات محلية ظاهرية مساعدة في تحسين الأمن، وشبكة الإدارة غير المرغوب فيها ويقلل من حركة مرور الشبكة |
| ثغرة أمنية | أوجه الضعف في نظام معلومات أو إجراءات أمن النظام أو عناصر التحكم الداخلية أو التنفيذ التي يستغلها أو يستهدفها مصدر تهديد. |
| تقييم الثغرات الأمنية | بيان رسمي وتقييم للثغرات الأمنية في أحد أنظمة المعلومات. |
| بروتوكول التطبيقات اللاسلكية | معيار يوفر لأجهزة التليفون المحمول والاستدعاء عن بعد (Pagers) وغيرها من الأجهزة الكفية المحمولة الوصول الآمن إلى صفحات البريد الالكتروني وصفحات الويب النصية. |
| دودة | برنامج ينسخ نفسه وينتشر ذاتياً مستخدماً آليات التشبيك ولديه القدرة على التخفي من برامج الحماية. |
| شهادة المعيار X.509 | حسب المنظمة الدولية للقياس واتحاد الاتصالات الدولي – قسم المعايير فان المعيار رقم X.509 يحدد نوعين من الشهادات هما شهادات X.509 للمفتاح العام وشهادات X.509 للخصائص. والأكثر شيوعاً حتى في هذا القاموس أن شهادات X.509 تشير إلى النوع الأول وهو شهادات X.509 ذات المفتاح العام. |
| XSS | XSS يشير إلى الضعف الذي يحدث كلما طلب يأخذ المستخدم توفير بيانات ويرسله إلى متصفح الويب من دون التأكد من صحتها أولا أو ترميز هذا المحتوى. XSS تسمح للمهاجمين لتنفيذ البرنامج النصي في متصفح الضحية التي يمكن أن خطف جلسات عمل المستخدم، ومواقع طمر، وربما أعرض الديدان، الخ. |

Sources: Publicly available information in published material from:

- KSU
- PMI (PMBOK)
- ISO ٢٧٠٠١
- US Govt. agencies, etc.



CERT.sa

المركز الوطني الارشادي لامن المعلومات

COMPUTER EMERGENCY RESPONSE TEAM

هيئة الاتصالات وتقنية المعلومات
Communications and Information Technology Commission

ص.ب ٧٥٦٠٦ الرياض ١١٥٨٨ المملكة العربية السعودية
هاتف ٤٦١٨٠٠٠ ١ ٩٦٦+ فاكس ٤٦١٨١٩٠ ١ ٩٦٦+

P.O. Box 75606 Riyadh 11588 Saudi Arabia
Tel.: +966 1 4618000 Fax: +966 1 4618190

www.citc.gov.sa
info@citc.gov.sa