وزارة الاتصالات وتكنولوجيا المعلومات

Ministry of Information and
Communications Technology

البرنامج الوطني للأمن السيبراني

إطار سياسة الأمن السيبراني:
١(د) الامتثال الدولي

جدول المحتويات

الأشكال

١ مقدمة

١-١ الهدف

الأمن السيبراني الوقائي، بما فيه الأمن المادي وأمن الأفراد وأمن المعلومات، متطلب أساسي ويتيح جعل العمل آمنا وأفضل.

هذه السياسة تساند **المجال ١ - الحوكمة وإدارة المخاطر والامتثال** من مجالات إطار السياسة الوطنية للأمن السيبراني، كما هو مبيّن في المستطيل الأحمر في الشكل 1. للاطلاع على القائمة الكاملة لإطار سياسة الأمن السيبراني، يرجى الرجوع إلى **الوثيقة الأساسية لإطار سياسة الأمن السيبراني**.

الشكل 1 - إطار سياسة الأمن السيبراني

١-٢ الاستخدام

هذه السياسة ليس الغرض منها استخدامها كوثيقة مستقلة بمعزل عن غيرها، بل لتكون جزءا لا يتجزأ من المجموعة الكاملة من سياسات إطار سياسة الأمن السيبراني. لمعرفة تفاصيل كيفية انتهاج هذه السياسة، يُرجى الاطلاع على القسم ٥ من **الوثيقة الأساسية لإطار سياسة الأمن السيبراني**.

١-٣ المتطلبات

المتطلبات اللازمة لأجل الامتثال الدولي ضرورية لوضع نهج موحّد ومعتمد للشركات الدولية وتلك العاملة في الخارج. بينما، في سياق العمل ضمن الأردن، تعتبر المعايير الدولية مسألة اختيارية ويُستعان بها فقط كتوجيهات يُسترشد بها أو كسبيل للحصول على اعتماد. لكن لدى العمل على مستوى العالم، تصبح هذه المعايير إلزامية، وخصوصا إن كانت تعتبر معايير تمثل خط الأساس. يتحقق الامتثال الداخلي، سواء كان إلزاميا أم أنه يعتبر من أفضل الممارسات، باتباع ما يلي:

المتطلب أ. تحديد المعايير، وأفضل الممارسات وإمكانية الحصول على اعتماد

المتطلب ب. نشر التوجيهات الإرشادية

المتطلب ج. تطبيق أطر العمل

١-٤ المعنيون

تنطبق هذه السياسة على جميع موظفي الحكومة الأردنية، والمتعاقدين معها، وجميع مستخدمي المعلومات الحكومية وأنظمة المعلومات التي تدعم أعمال وأصول الحكومة. لمزيد من التفاصيل، يُرجى الرجوع إلى **الوثيقة الأساسية لإطار سياسة الأمن السيبراني**.

١-٥ الهيكل

بينما أن كلا من السياسات الأخرى ضمن إطار سياسة الأمن السيبراني تتضمن فقرة خاصة بها بعنوان "المعايير الدولية"، فإن هذه السياسة صيغت بشكل مختلف لتوفر مصدرا واحدا للمعايير الدولية والاعتمادات والتوجيهات بشأن أفضل الممارسات، والتي تعتبر ضرورية أو أكثر صلة وتنطبق على إطار سياسة الأمن السيبراني. لكن هذه القائمة لا تشمل كافة المعايير، وقد تكون هناك بلا شك تحديثات تسبق تاريخ عملية مراجعة وتحديث إطار سياسة الأمن السيبراني، وبالتالي ينبغي الاستعانة بهذه المحتويات مع مراعاة الحرص الواجب.

١-٦ الإيجابيات والسلبيات

الجانب السلبي الأساسي لدى اتباع معيار دولي حين لا يكون هناك لزوم له هو ما يُبذل من وقت وتكاليف لازمة لتطبيقه. وإضافة إلى ذلك، المعيار الدولي قد يحيد بالمؤسسة عن نهجها إن لم يكن مصمما خصيصا ليناسب مجال عملها تحديدا. ومع ذلك، فإن إيجابيات اتباع معيار دولي عديدة وتفوق السلبيات إلى حد كبير، حتى وإن لم تكن هناك حاجة رسمية لاتباعه. من بين هذه الإيجابيات: القدرة على التعلم من تجارب الآخرين والاستماع لتجاربهم ومشاركتها. وعلاوة على ذلك، فإن بلورة استراتيجيات ومقاربات استنادا إلى أسس دولية يفتح المجال أمام جميع أشكال موارد التطبيق الإضافية التي أعدّها آخرون، إلى جانب الإعداد للحصول على اعتماد في حال الحاجة إليه مستقبلا. وبالتالي، فإن المعايير الدولية المشار إليها هنا تعزز، حيثما أمكن، جميع المقاربات تجاه الأمن.

٢ المعايير، وأفضل الممارسات، وإمكانية الحصول على اعتماد

المتطلب أ. المعايير، وأفضل الممارسات، وإمكانية الحصول على اعتماد. ينبغي على المؤسسة تحديد المعايير وأفضل الممارسات التي تنطبق على عملها، وما إن كانت تعتزم الحصول على اعتماد لها.

يجب على المؤسسة تحديد النهج الذي ترغب في اتباعه، واستعانتها بالمعايير الدولية، ونوع الاعتماد الذي تحتاج إليه المؤسسة أو العاملون فيها، وكيفية الاستعانة بتلك المعايير للاستناد إليها في النهج المتبع. القائمة المدرجة أدناه، التي هي على سبيل المثال لا الحصر ولا تشمل كل المعايير، تحدد المعايير الدولية والأوروبية الأساسية المشار إليها كي تستند إليها السياسيات في إطار سياسة الأمن السيبراني.

٢-١ معايير ISO/IEC

ISO/IEC هي اللجنة التقنية المشتركة للمنظمة الدولية لتوحيد المعايير (آيزو ISO) واللجنة الكهربائية التقنية الدولية (IEC).

إن المعايير الدولية، و"أفضل الممارسات" في قطاع ما، والطرق المعترف بها على نطاق واسع تعتبر جميعها مصادر ضرورية للمعلومات بالنسبة لأي مؤسسة تتطلع إلى تحسين وضعها الأمني. وسياسات إطار سياسة الأمن السيبراني هذا تتناول العديد من المعايير والممارسات والطرق الدولية، والتي يُستعان بها لتستند إليها قرارات الإدارة العليا المتعلقة بالسياسات.

من الضروري أن تتدارس المؤسسة المعايير والممارسات والطرق الدولية لدى وضعها لخطط الدعم والتحسين. لكن ليس كل ما هو مدرج أدناه مناسب لجميع المؤسسات، وبالتالي ينبغي على المؤسسة تقييم مدى ملاءمة ما يلي لاحتياجاتها الخاصة.

كما إن الكثير من المعايير الدولية هي أيضا معايير للاعتماد، ويمكن اعتماد المؤسسة بموجبها من قبل منظمة خارجية مؤهلة. لكن قد لا يكون ذلك ضروريا أو مناسبا في جميع الأوقات، وبالتالي يجب اعتبار هذه المعايير أيضا بمثابة مقاييس مرجعية أو أهداف لأفضل الممارسات تستند إليها المؤسسة في صياغة استراتيجية أمنية مُحَسَّنة.

٢-١-١ ISO/IEC 9001

يُعتبر معيار ISO/IEC 9001 أساسا معترف به دوليا لنظام إدارة الجودة وعمليات التدقيق. وهو يوفر مجموعة من المتطلبات التي تساعد في مراقبة وإدارة الجودة باستمرار لكافة قطاعات عمل المؤسسة ويحدد مجالات التحسين. ويُمكن استخدام ISO/IEC 9001 كمجموعة من الإرشادات لتطوير وتنفيذ وإدارة نظام إدارة الجودة.

باستطاعة المؤسسة أن تطلب الامتثال لهذه المعايير لضمان الأداء في تزويد الخدمات. كما إن معيار ISO/IEC 9001 يعطي تفاصيل متطلبات عملية الشراء حين تكون المؤسسة هي العميل.

ISO 10007:2017 ٢-١-٢

معيار ISO 10007:2017 (ويُعرف أيضا بمعيار BS EN ISO 10007) يوفر إرشادات حول إدارة الصورة المتكاملة في المؤسسة، وينطبق على دعم المنتجات والخدمات ابتداء وضع من تصور لها وحتى تقديمها.

نسخة عام ٢٠١٧ هي أحدث إصدار لمعيار BS EN ISO 10007، والغرض منه هو الاستعانة به كوثيقة إرشادية تستعين بها المؤسسة بشأن إدارة الصورة المتكاملة. ويمكن تطبيقه لدى دعم المنتجات ابتداء بمرحلة وضع تصور لها وحتى تقديمها.

ISO/IEC 19770-1:2017 ٣-١-٢

يحدد المعيار ISO/IEC 19770-1:2017 متطلبات محددة تتعلق بإدارة أصول تكنولوجيا المعلومات في المؤسسة. يمكن تطبيق هذا المعيار على جميع أنواع أصول تكنولوجيا المعلومات، ومن قبل المؤسسات بمختلف أنواعها وأحجامها.

يوفر هذا المعيار إطارا من العمليات لضمان الدعم الفعال لإدارة خدمة تكنولوجيا المعلومات، ولتمكين المؤسسة من برهنة أنها تدير أصول البرمجيات وفق معايير عالية بالدرجة الكافية، تماشيا مع أي التزامات قانونية أو حكومية ذات صلة.

ISO/IEC 20000 ٤-١-٢

المعيار ISO/IEC 20000 هو المعيار الدولي لإدارة خدمات تكنولوجيا المعلومات، وقد نُشر لعرض أفضل الممارسات الدولية المشار إليها في العديد من أطر إدارة هذه الخدمات، وأشهرها إطار مكتبة البنية التحتية لتكنولوجيا المعلومات (ITIL) المستخدم عالميا.

معايير ISO/IEC المستخدمة على نطاق واسع في مجموعة السياسات هذه مشار إليها بالتفصيل في الأجزاء التالية.

ISO 22301 ٥-١-٢

ISO 22301 هو المعيار الدولي لاستمرارية العمل، ويشمل مجموعة من المتطلبات لنظام إدارة يهدف إلى الحماية من وقوع حادث، وتقليل احتمال وقوعه، وضمان أن تتعافى المؤسسة وتواصل عملها في حال وقوعه. يمكن الاستعانة بهذا المعيار كوسيلة للاعتماد، لكن ربما تفضل المؤسسة أيضا الاستعانة به لاتباع أفضل الممارسات، وفي عمليات التدقيق الداخلي، حيث أنه يساند مجموعة من التدابير لرفع التقارير للإدارة.

ونهج المؤسسة عموما بشأن استمرارية العمل يجب أن يحكمه نظام لإدارة استمرارية العمل متوافق مع المعيار ISO 22301.

ISO/IEC 27001 - 27002 ٦-١-٢

تتألف سلسلة ISO/IEC 27000 من مجموعة من المعايير المتعلقة بأمن المعلومات، والتي أعدتها ونشرتها آيزو (ISO) بالاشتراك مع IEC. اثنان من هذه المعايير - المعيار ISO/IEC 27001 والمعيار ISO/IEC 27002 - ينطبقان بشكل خاص على موضوع حماية الأرصدة، وهما معا يحددان مجموعة من المتطلبات المتعلقة بأنظمة إدارة أمن المعلومات، ومدونة لقواعد السلوك بشأن ضوابط أمن المعلومات.

المعيار ISO/IEC 27001 هو أفضل معيار معروف لتوفير متطلبات نظام إدارة أمن المعلومات. والمعيار ISO/IEC 27002:2013 يعطي توجيهات إرشادية بشأن معايير أمن المعلومات والممارسات المتعلقة بها في المؤسسة، بما في ذلك اختيار وتطبيق وإدارة ضوابط تأخذ بعين الاعتبار بيئة الخطر الذي يواجه أمن المعلومات في المؤسسة.

سلسلة معايير ISO/IEC 27000 المتعلقة بأمن المعلومات تشمل المعايير التالية:

- ISO/IEC 27000:2018 - تكنولوجيا المعلومات - التقنيات الأمنية - أنظمة إدارة أمن المعلومات - لمحة عامة ومصطلحات؛
- ISO/IEC 27001:2013 - تكنولوجيا المعلومات - التقنيات الأمنية - أنظمة إدارة أمن المعلومات - المتطلبات؛
- ISO/IEC 27002:2013 - تكنولوجيا المعلومات - التقنيات الأمنية - مدونة قواعد السلوك المتعلقة بضوابط أمن المعلومات؛
- ISO/IEC 27003:2017 - تكنولوجيا المعلومات - التقنيات الأمنية - أنظمة إدارة أمن المعلومات - توجيهات إرشادية بشأن التطبيق؛
- ISO/IEC 27004:2016 - تكنولوجيا المعلومات - التقنيات الأمنية - إدارة أمن المعلومات - المراقبة والقياس والتحليل والتقييم؛
- ISO/IEC 27005:2012 - تكنولوجيا المعلومات - التقنيات الأمنية - إدارة مخاطر أمن المعلومات (ISO/IEC 27005:2011)؛
- ISO/IEC 27007:2017 - تكنولوجيا المعلومات - التقنيات الأمنية - توجيهات إرشادية بشأن التدقيق في أنظمة إدارة أمن المعلومات؛

٢-١-٧ ISO/IEC 27031

المعيار ISO/IEC 27031 يوفر مجموعة من المفاهيم والمبادئ حول مدى استعداد تكنولوجيا المعلومات والاتصالات لضمان استمرارية العمل. كما يوفر إطارا لتحديد وتحسين نهج المؤسسة بهذا الصدد.

٢-١-٨ ISO/IEC 28000

المعيار ISO/IEC 2800 يحدد المتطلبات المتعلقة بنظام الإدارة الأمنية لسلسلة التوريد، الأمر الذي يتيح للمؤسسة معرفة الجوانب الحيوية المتعلقة بأمن سلسلة التوريد التي تتعامل معها، وتطبيق السياسات والإجراءات والضوابط اللازمة لإدارة المخاطر الأمنية.

٢-١-٩ ISO 31000

المعيار ISO 31000:2018 يعطي توجيهات إرشادية لإدارة المخاطر، وهذه التوجيهات هي على شكل مبادئ وإطار عمل وعملية لإدارة المخاطر. هذا المعيار مناسب لتستعين به أي مؤسسة، بعض النظر عن حجمها أو نشاطها أو قطاع عملها.

يمكن للمؤسسة الاستعانة بالمعيار ISO 31000 للمساعدة في معرفة الفرص والتهديدات، وتخصيص الموارد اللازمة لمعالجة الخطر. وهو يقدم توجيهات إرشادية، لكن الغرض منه ليس الحصول على اعتماد رسمي؛ بل يمكن للمؤسسة أن تعتبره مؤشرا معترفا به دوليا أو وثيقة تتعلق بأفضل الممارسات.

٢-١-١٠ ISO 55000

معيار ISO 55000 هو معيار دولي يغطي إدارة الأصول المادية. هذه السلسلة من المعايير لإدارة الأصول - والتي كان قد نشرها المعهد البريطاني للمعايير في ٢٠٠٤ باسم الخصائص المتاحة للعامة (PAS 55) - نُشرت في عام ٢٠١٤، وهي تشمل:

- المعيار ISO 55001:2014 - إدارة الأصول - مجموعة دولية جديدة من المعايير التي صُممت لتوفير توجيهات إرشادية حول أفضل الممارسات في إدارة الأصول.

لمزيد من التفاصيل حول هذه المعايير وغيرها من معايير آيزو ISO، يُرجى زيارة www.iso.org

٢-٢ المعايير البريطانية/الأوروبية

المعيار البريطاني (BS) والعرف الأوروبي (EN) والمنظمة الدولية لتوحيد المعايير (آيزو ISO) هي جميعها أجهزة فردية معنية بالمعايير في المملكة المتحدة والاتحاد الأوروبي ودولية على التوالي. إلا أن بعض المعايير قد تمت "ملاءمتها"، أي تبنيها في مناطق عدة.

وفي الكثير من الحالات، تكون المعايير مسبوقة برمزين "BE EN". ذلك يعني أن هذا المعيار هو النسخة البريطانية (باللغة الإنجليزية) عن معيار أوروبي تمت ملاءمته. كما إن من الممكن وجود معايير تمت ملاءمتها في جميع المناطق الثلاث، وفي تلك الحالة يكون المعيار مسبوقا بثلاثة رموز "BE EN ISO". ذلك يشير إلى معيار دولي تبنته أوروبا كمعيار أوروبي.

٢-٢-١ BS EN 1143 (معيار أوروبي معترف به دوليا)

المعيار BS EN 1143 يحدد معيار اختبار الخزنات الآمنة، وخزنات أجهزة الصرف الآلي (ATM)، وأبواب الغرف محكمة الإغلاق والغرف نفسها. ودرجات مقاومة الخزنات مقسمة إلى سبع درجات، وترتفع درجة الأمن بنحو ٥٠% من درجة إلى أخرى.

ويُحسب مستوى الأمن بناء على درجات الأدوات والفترة اللازمة لاختراق خزنة. وبالنسبة لوحدات التخزين الآمن المؤمَّنة وفق هذا المعيار، يجب أن يستوفي نظام قفلها أيضا متطلبات المعيار BE EN 1300.

٢-٢-٢ BS EN 1300 (معيار أوروبي معترف به دوليا)

المعيار BS EN 1300 يحدد مستوى اختبار وحدات التخزين الآمن. وهو يعطي، بالتحديد، تصنيفا للأقفال شديدة الأمان تبعا لدرجة مقاومتها لمحاولة فتحها من قبل شخص غير مصرح له بفتحها.

٢-٢-٣ BS EN 1627 (معيار أوروبي معترف به دوليا)

المعيار BS EN 1627 يحدد درجة مقاومة الدخول غير المصرح به من خلال الأبواب والنوافذ، والأغلفة والشبكات والمغالق الخارجية للمباني. وهو يعتبر عموما خط الأساس لأمن البيوت والمكاتب وغيرها.

٢-٢-٤ PAS 24 (معيار أوروبي معترف به دوليا)

المعيار PAS 24 يستند إلى مبادئ مماثلة لمبادئ المعيار BS EN 1627 (أعلاه)، لكنه يتناول متطلبات أمنية أكثر شدة بالنسبة للأبواب في المواقع الأكثر أمانا.

لمزيد من التفاصيل حول معايير BS وPAS،يمكن زيارة الموقع www.bsigroup.com

٢-٣ اعتماد الأفراد

أغلب المعايير المشار إليها في الأقسام السابقة من هذه السياسة تتعلق بنهج العمل أو المؤسسة، رغم أن بعضها يوفر كذلك سبلا لاعتماد الأفراد. لمزيد من الاعتماد الفردي، فيما يلي قائمة، على سبيل المثال لا الحصر، للسبل المحددة التي يمكن للأفراد اتباعها سعيا للحصول على اعتماد بمجال ممارسة الأمن.

٢-٣-١ IISP

يوفر معهد محترفي أمن المعلومات (IISP) المجال للعضوية وأطرا ومجموعة من الكفاءات المتوقعة من محترفي أمن المعلومات وضمان المعلومات. لمزيد من التفاصيل، يرجى زيارة الموقعwww.iisp.org

٢-٣-٢ SANS

معهد SANS هو معهد عالمي يقدم التدريب لموظفي الأمن المعنيين بإدارة الأنظمة والتدقيق والشبكات والأمن، إلى جانب فرص العضوية فيه. لمزيد من المعلومات، يُرجى زيارة الموقع www.sans.org

٣ التوجيهات الإرشادية

☑ **المتطلب ب. نشر التوجيهات الإرشادية.** يتعين على المؤسسة أن تكون منفتحة على تطبيق التوجيهات وعازمة على استيفاء المعايير ومستويات الاعتماد. لذا عليها أن تنشر كافة أهداف المعايير والاعتماد وأن تدخلها في سجلاتها التي توثق أفضل الممارسات والتوجيهات الإرشادية لكي يتمكن كافة العاملين من تحقيق تلك الأهداف من خلال درايتهم بها.

رغم أن وثائق أفضل الممارسات والإرشادات التوجيهية ليست معايير رسمية، فإن نشرها أصبح مقبولا على نطاق واسع كوسيلة لاطلاع المؤسسة على المنهجيات المُختارة من خلال مطبوعات تعريفية. وحينما يكون ذلك ممكنا، يجب أيضا شمول العودة إلى الأهداف المرجوة للمعايير والاعتماد لكي يكون بالإمكان ضبط الإصدارات والتحديثات، ولنشر الوعي على نطاق أوسع. ورغم أن هذا القسم ليس مستوفيا لكل شيء، فهو يشمل أيضا معايير التشفير الرياضية المقبولة لدى قطاع تكنولوجيا المعلومات كمعيار آمن.

٣-١ معايير ومطبوعات المعهد الوطني للمعايير والتكنولوجيا (NIST)

المعهد الوطني للمعايير والتكنولوجيا (NIST) هو وكالة غير تنظيمية تابعة لوزارة التجارة الأمريكية. يضع المعهد معايير القياس ومواد القياس المرجعية وما شابه، وهو مُعترف به في كافة أنحاء العالم كمنظمة رائدة على مستوى العالم في وضع المعايير وعلوم القياس.

٣-١-١ NIST SP 800-30 (المراجعة ١)

المطبوعة NIST SP 800-30، وهي دليل إجراء تقييم المخاطر، توفر إرشادات توجيهية لأية مؤسسة تُجري تقييما للمخاطر حول أنظمة المعلومات وأمور المؤسسة الأعم. وهي تقدم عرضا مفصلا لأفضل الممارسات في تقييم المخاطر كجزء من عملية تقييم المخاطر عموما. يُعتبر تقييم المخاطر في غاية الأهمية لأية مؤسسة تسعى للتعرف على مجالات الخطر، وإعداد تقارير بالنتائج بطريقة دقيقة ومركزة، وتخطط لكيفية معالجة المخاطر. كما يُمكن استخدام تقييم المخاطر لاستقطاب دعم كبار قيادات المؤسسة عند السعي لتحسين نظام العمل ومعالجة المخاطر.

٣-١-٢ NIST SP 800-53A - تقييم الضوابط الأمنية (المراجعة ٤)

توصي النشرة الخاصة NIST SP 800-53A بمجموعة من الضوابط الفنية وغير الفنية لحماية الأمن والخصوصية من أجل دعم تطوير أنظمة معلومات آمنة وقادرة على الصمود أمام الأخطار.

٣-١-٣ NIST SP 800-60

توفر النشرة الخاصة NIST SP 800-60 توجيهات إرشادية من أجل تصنيف أنواع المعلومات وأنظمة المعلومات بموجب فئات أمنية. والغرض منها مساعدة المؤسسة في أن تضع لنفسها نهجا يحدد مستويات التأثير الأمني على الأصول بشكل دائم، ومن ثم يحمي تلك الأصول بالطريقة المناسبة.

٣-١-٤ NIST SP 800-175A and 800-175B

النشرة الخاصة NIST SP 175 تشمل الجزء 800-175A، وهو مجموعة من التوجيهات والسياسات بشأن استخدام التشفير في حماية البيانات، والجزء 800-175B الذي يعطي شرحا مفصلا لآليات التشفير. ويوفر الجزءان معا توجيهات إرشادية مفيدة من أجل استخدام معايير التشفير في أمن البيانات.

٣-١-٥ NIST AES

معيار التشفير المتقدم (AES) هو معيار مُعتمد من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) وهيئة المعايير الفيدرالية لمعالجة البيانات (FIPS) لخوارزمية التشفير (algorithm)، وهو يُستخدم لحماية البيانات الإلكترونية.

"خوارزمية معيار التشفير المتقدم هي شيفرة من كتل متناسقة يُمكنها تشفير المعلومات وفك الشيفرة. يُحوّل التشفير البيانات إلى نص غير مفهوم يُدعى النص المُشفّر (ciphertext) أما فك شيفرة النص فيعيد البيانات إلى شكلها الأصلي، ويُدعى النص في تلك الحالة النص الواضح. بإمكان خوارزمية معايير التشفير المتقدم استخدام مفاتيح التشفير من فئة ١٢٨، و١٩٢، و٢٥٦ بت (bits) لتشفير البيانات وفك شيفرتها في كتل من ١٢٨ بت" النشرة رقم ١٩٧ للمعهد الوطني للمعايير والتكنولوجيا وهيئة المعايير الفيدرالية لمعالجة البيانات.

٣-١-٦ NIST SP 800-115 - الاختبار والتقييم

توصي النشرة الخاصة NIST SP 800-115 باتباع نهج فني إزاء اختبار وتقييم أمن المعلومات.

٣-١-٧ NIST SP 800-161 - سلسلة الموردين

توصي النشرة الخاصة NIST SP 800-161 باتباع نهج يركز على ضوابط وإرشادات حماية سلسلة المورّدين.

مجموعة ضوابط أمن العاملين

تُستخدم المجموعة التالية من ضوابط أمن العاملين، والمستقاة من المعهد الوطني لمعايير التكنولوجيا (NIST)، لاتخاذ القرارات بشأن ضوابط أمن العمل:

أمن العاملين-١ تدابير أمن العاملين: لا بد لكافة أنظمة العمل الحكومية أن تطور وتتبنى وتلتزم بتدابير رسمية موثقة لحماية العاملين، والتي تعالج كل ما يتعلق بأهداف المؤسسة، ونطاق عملها، والأدوار، والمسؤوليات، وواجبات الإدارة، والتنسيق بين إدارات المؤسسة، والامتثال لأنظمتها.

أمن العاملين-٢ تصنيف شاغلي المناصب: يتوجب على كافة أنظمة العمل الحكومية أن:

- تحدد المسؤوليات عن المخاطر لكافة شاغلي المناصب.
- تضع معايير للفحص الأمني للأفراد الذين يشغلون تلك المناصب.
- تراجع وتعيد النظر بتوزيع المخاطر المتعلقة بالمناصب بمعدل ثلاث مرات في السنة.

أمن العاملين-٣ التدقيق الأمني في العاملين: يتوجب على كافة أنظمة العمل الحكومية أن تُجري تدقيقا أمنيا في خلفيات الأفراد قبل منحهم صلاحية الاطلاع على أصول المعلومات. كما على المؤسسة أن تعيد الدقيق الأمني للأفراد كل سبع سنوات.

أمن العاملين-٤ إنهاء خدمات العاملين: يترتب على كافة أنظمة العمل الحكومية لدى إنهاء خدمات أحد العاملين أن:

- تلغي التصريح له بالاطلاع على أصول المعلومات.

- تُجري معه مقابلة قبل الخروج من الخدمة.
- تسترجع كل ما بحوزته مما يتعلق بأمن المؤسسة وأنظمة معلوماتها.
- تستعيد الدخول إلى معلومات المؤسسة وأصول المعلومات التي كانت سابقا تحت تصرف الموظف الذي أُنهيت خدماته.

أمن العاملين-٥ نقل العاملين: يتعين على كافة أنظمة العمل الحكومية القيام بمراجعة فصلية لصلاحيات الدخول الإلكتروني والمادي إلى أصول ومرافق المؤسسة عندما يُنقل الموظف أو يُعاد تكليفه بوظيفة أخرى داخل المؤسسة.

أمن العاملين-٦ اتفاقيات الدخول إلى البيانات: يجب على كافة أنظمة العمل الحكومية أن تتأكد أن الأفراد الذين يحتاجون الاطلاع على معلومات المؤسسة وأصول المعلومات يوقعون اتفاقية خاصة بذلك قبل منحهم الإذن بذلك. يُضاف إلى ذلك أنه يجب مراجعة تلك الاتفاقيات وتحديثها كل ثلاث سنوات.

أمن العاملين-٧ أمن عاملي الطرف الثالث: يجب على كافة أنظمة العمل الحكومية أن:

- تُحدد متطلبات أمن العاملين، بما في ذلك الأدوار والمسؤوليات الأمنية للمزودين من طرف ثالث.
- تُوثّق متطلبات أمن العاملين.
- تُراقب امتثال المزودين.

أمن العاملين-٨ العقوبات على العاملين: يجب على كافة أنظمة العمل الحكومية أن تُطبّق عقوبات رسمية بحق العاملين الذين لا يلتزمون بسياسات وإجراءات أمن المعلومات المعمول بها.

تنطبق هذه الإجراءات على جميع موظفي الحكومة الأردنية، والمتعاقدين معها، وجميع مستخدمي المعلومات الحكومية وأنظمة المعلومات التي تدعم أعمال وأصول الحكومة.

لمزيد من التفاصيل عما ورد أعلاه وبقية معايير ومنشورات المعهد الوطني للمعايير والتكنولوجيا (NIST) يرجى زيارة الموقع www.nist.gov

٤ أطر العمل

المتطلب ج. تطبيق أطر العمل.
عند الاستعانة بعدد كبير من السياسات والمبادئ، ينبغي استخدام أطر لوضع تصور لكيفية دعم هذه السياسات لبعضها البعض، أو أن تكون هناك إرشادات محددة يجب اتباعها.

إطار العمل هو مجموعة من السياسات والمبادئ الأساسية والأهداف طويلة الأمد التي تشكل أساس صناعة القرارات، وتضع القواعد والتوجيهات الإرشادية، وتوفر التوجيهات العامة من أجل التخطيط والالتزام، وتطور المؤسسة أو العمل. فيما يلي عرض لأطر عمل أفضل الممارسات المُعترف بها دوليا:

٤-١ إطار عمل المعهد الوطني للمعايير والتكنولوجيا (NIST) بشأن إدارة المخاطر

يقدم إطار عمل المعهد الوطني للمعايير والتكنولوجيا بشأن إدارة المخاطر توصيفا للعملية التي تدمج فعاليات الأمن وإدارة المخاطر في دورة تطوير الأنظمة. وتنقسم الفعاليات إلى خطوات على النحو التالي:

- ***الخطوة ١: وضع تصنيف للأنظمة***
- ***الخطوة ٢: تحديد خط الأساس***
- ***الخطوة ٣: تطبيق الضوابط***
- ***الخطوة ٤: تقييم الضوابط***
- ***الخطوة ٥: التصريح بتشغيل الأنظمة***
- ***الخطوة ٦: مراقبة الضوابط***

٤-٢ مكتبة البنية التحتية لتكنولوجيا المعلومات

مكتبة البنية التحتية لتكنولوجيا المعلومات (ITIL) هي مجموعة من ممارسات إدارة خدمات تكنولوجيا المعلومات مُعترف بها دوليا، وهي تركز على تقديم خدمات تكنولوجيا المعلومات بناء على احتياجات المؤسسة. وبالتالي، يتم استغلال العمليات والإجراءات على النحو الأمثل لتسهيل مهمة المؤسسة من خلال تطبيق ممارسات فعالة لتكنولوجيا المعلومات. ورغم أن إطار عمل مكتبة البنية التحتية لتكنولوجيا المعلومات لا يُعتبر معيارا دوليا، فإنه أصبح في السنوات الأخيرة مقبولا على نطاق واسع كمرجع لأفضل الممارسات في مجال إدارة خدمات تكنولوجيا المعلومات. وهذا الإطار يرتبط بوضوح بالمعيار ISO/IEC 20000 كما هو مشار إليه أعلاه في الفقرة ٤.١.٢، وهذا الارتباط مُعتمد من قبل اللجنة الكهربائية التقنية الدولية. وبالتالي يُمكن استخدام هذا الإطار لدعم الاستجابة للمتطلبات المحددة من أجل الحصول على شهادة اعتماد ISO/IEC 20000، إن كانت هناك حاجة إليها.

وقد تم تصميم مكتبة البنية التحتية لتكنولوجيا المعلومات حول دورة حياة الخدمات التي تقدمها، والتي تتألف من الأجزاء التالية:

- استراتيجية الخدمات
- تصميم الخدمات
- نقل الخدمات
- عمليات الخدمات
- التحسين المستمر للخدمات

لمزيد من التفاصيل حول مكتبة البنية التحتية لتكنولوجيا المعلومات، انظر الموقع www.axelos.com

٤-٣ إطار مخاطر تكنولوجيا المعلومات - جمعية تدقيق أنظمة المعلومات وضبطها (***ISACA***)

يقوم إطار مخاطر تكنولوجيا المعلومات ISACA على مجموعة من المبادئ الإرشادية من أجل إدارة فعالة لمخاطر تكنولوجيا المعلومات. ويُمكن للمؤسسة أن تستخدمه للتعرف على مخاطر تكنولوجيا المعلومات والتحكم بها وإدارتها. وهو ينطبق بشكل خاص على المؤسسات التي تعتزم اتباع إطار عمل غايات ضوابط المعلومات والتكنولوجيا (COBIT).

٤-٤ غايات ضوابط المعلومات والتكنولوجيا المصاحبة لها ***COBIT***

إطار عمل COBIT يحدد مجموعة من العمليات العامة لإدارة تكنولوجيا المعلومات، حيث تكون كل عملية محددة مع مدخلاتها ومخرجاتها، وأنشطتها الأساسية، وأهدافها، ومقاييس أدائها، ونموذج أولي عن نضجها. وتشمل مكونات COBIT ما يلي:

٤-٤-١ إطار العمل

تُستخدم أطر العمل لدعم أهداف حوكمة تكنولوجيا المعلومات وأفضل ممارساتها لمساندة النطاقات الإلكترونية (Domains) والعمليات، وذلك من أجل ربطها بمتطلبات العمل.

٤-٤-٢ توصيف العمليات

يتيح توصيف العمليات إيجاد لغة موحدة وعامة تستخدمها كافة إدارات المؤسسة.

٤-٤-٣ غايات الضوابط

توفر غايات الضوابط مجموعة من المتطلبات عالية المستوى التي يجب أن يراعيها صناع القرار في الإدارة لتطبيق ضوابط فعالة في كل عملية.

٤-٤-٤ التوجيهات الإرشادية للإدارة

تحدد التوجيهات الإرشادية مسؤوليات الإدارة، والاتفاق على الغايات، وقياس الأداء، وتوضيح تداخل العلاقة مع العمليات الأخرى.

٤-٤-٥ نماذج النضوج

تفيد نماذج النضوج في تقييم مدى نضوج وقدرة كل عملية لأجل فهم أين تكمن الحاجة للتحسينات، أو

الثغرات الموجودة في العملية/القدرات والتي تحتاج لسدها.

لمزيد من التفاصيل حول ISACA وCOBIT انظر الموقع www.isaca.org

٤-٥ اعتبارات أساسية

- قائمة المعايير هذه لا تشمل كل شيء، بل هي على سبيل المثال لا الحصر. ويتعين على مسؤولي أمن المعلومات (أو من في حُكمهم) داخل المؤسسة أن يكونوا على دراية بالنطاق الأوسع للمعايير، وأن تكون لديهم معرفة حديثة بأية معايير أو إرشادات توجيهية أخرى قابلة للتطبيق.

- إن المنشورات التي تصدرها مؤسسات مثل المعهد الوطني للمعايير والتكنولوجيا (NIST) يُمكن أن تكون مصادر مفيدة للمعلومات بشأن أفضل الممارسات والتوجيهات الإرشادية، وأطر العمل المقبولة على نطاق واسع للممارسات الأمنية.