السياسات العامة لأمن المعلومات
في الجهات الحكومية
مقدمة

2. على كافة الوزارات والجهات الحكومية والمؤسسات والهيئات والوحدات التابعة لها:

أ- العمل وفق وثيقة السياسات العامة لأمن المعلومات في الجهات الحكومية والالتزام بها.

ب- تخصيص وتعيين الشخص والقسم والإدارة المسؤول عن متابعة تنفيذ هذه السياسات لديها وموافاة وزارة الاتصالات وتقنية المعلومات ببيانات ضابط أمن المعلومات المعني بتنفيذها والتقييم الدوري لذلك.

3. على وزارة الاتصالات وتقنية المعلومات تنظيم الورش والندوات التعريفية والتشاورية لتعزيز أمن المعلومات وسياساتها وتحديثها بشكل مستمر.

قرار مجلس الوزراء رقم (٥٩) للعام ٢٠٢٠م بشأن وثيقة السياسات العامة لأمن المعلومات في الجهات الحكومية- متقطفات

مقدمة

- أصبحت تكنولوجيا المعلومات والاتصالات أحد العوامل المؤثرة في نهضة البلدان وازدهارها واستقرارها إلى درجة أنه لا يمكن لأي جهة أو مؤسسة أو شركة حكومية أو خاصة أن تعمل في استغناء عن تكنولوجيا المعلومات والاتصالات، ومع سرعة تعاظم ونمو تكنولوجيا المعلومات والاتّصالات، وتزايد أثرها في تعزيز التّنمية البشرّية والاقتصادّية والاجتماعّية والثّقافّية ودورها في تقديم خدمات الجهات الحكومية والخاصة، ازدادت المخاطر على المنظومات المعلوماتيّة وتنوّعت واختلفت أساليبها ودوافعها.
- وعليه ولأهمية وضرورة تأمين بنية تحتيّة آمنة وموثوقة سواءً لإنجاز الأعمال والمهام أو لتقديم الخدمات الإلكترونيّة، ولزوم توفير البيئة الملائمة لتقليل خطر اختراق المنظومات المعلوماتيّة الحكوميّة، وكشف محاولات الاختراق واتّخاذ الإجراءات اللّازمة بأسرع وقت ممكن في حال حدوثها، فقد أعدت الوزارة وثيقة سياسات أمن المعلومات العامة للجهات الحكومية.

مقدمة

- حيث توفر هذه السياسات مجموعة متكاملة من المتطلبات الأساسية الأدنى وإجراءات الحماية التي يجب توافرها على مستوى جميع الجهات الحكومية لضمان بيئة تشغيل وعمل آمنة للأصول المعلوماتية والمعلومات وبما يضمن ديمومة قيامها بمهامها وأعمالها بسلامة واطمئنان، حيث تعد معلومات هذه الجهات والمعلومات الوطنية وأنظمة دعم تكنولوجيا المعلومات وبيانات المواطنين ونحوها من الأصول المهمة للجهات الحكومية والتي يجب الحفاظ عليها. كما تعنى وزارة الاتصالات وتقنية المعلومات بتقديم الملحقات اللازمة من **أدلة إرشادية ولوائح تفصيلية ومواد تأهيل وتدريب وتوعية** لكافة الجهات الحكومية في مجالات أمن المعلومات.

تعاريف

- **أمن المعلومات**: الوسائل والتّدابير الخاصة المطبقة والمستمرة بشكل دائم بالحفاظ على سرّية، وتوافرية، وسلامة المعلومات، وحمايتها من الأنشطة غير المشروعة وبما يضمن الحماية اللازمة للمعلومات ومنع الوصول إليها من غير ذوي الصلاحية.
- **الأصول المعلوماتية**: هي البيانات والمعلومات والبنية التحتية المحيطة بها من تجهيزات أو برمجيات أو خدمات أو مستخدمين أو مرافق ...الخ.
- **أصالة المعلومات**: خاصّية كون الشيء حقيقياً ويمكن التّحقق منه والثّقة به، وضمان صحة الإرسال، أو الرسالة أو المنشئ داخل المنظومة المعلوماتية.
- **التشفير**: تحويل البيانات (النص عادي) إلى شيفرات (نص مشفر) بشكل يحافظ على المعنى الأصلي لهذه البيانات بهدف منع التعرف عليها أو استخدامها من قبل الغير مخول/ مصرح لهم بذلك.

تعاريف

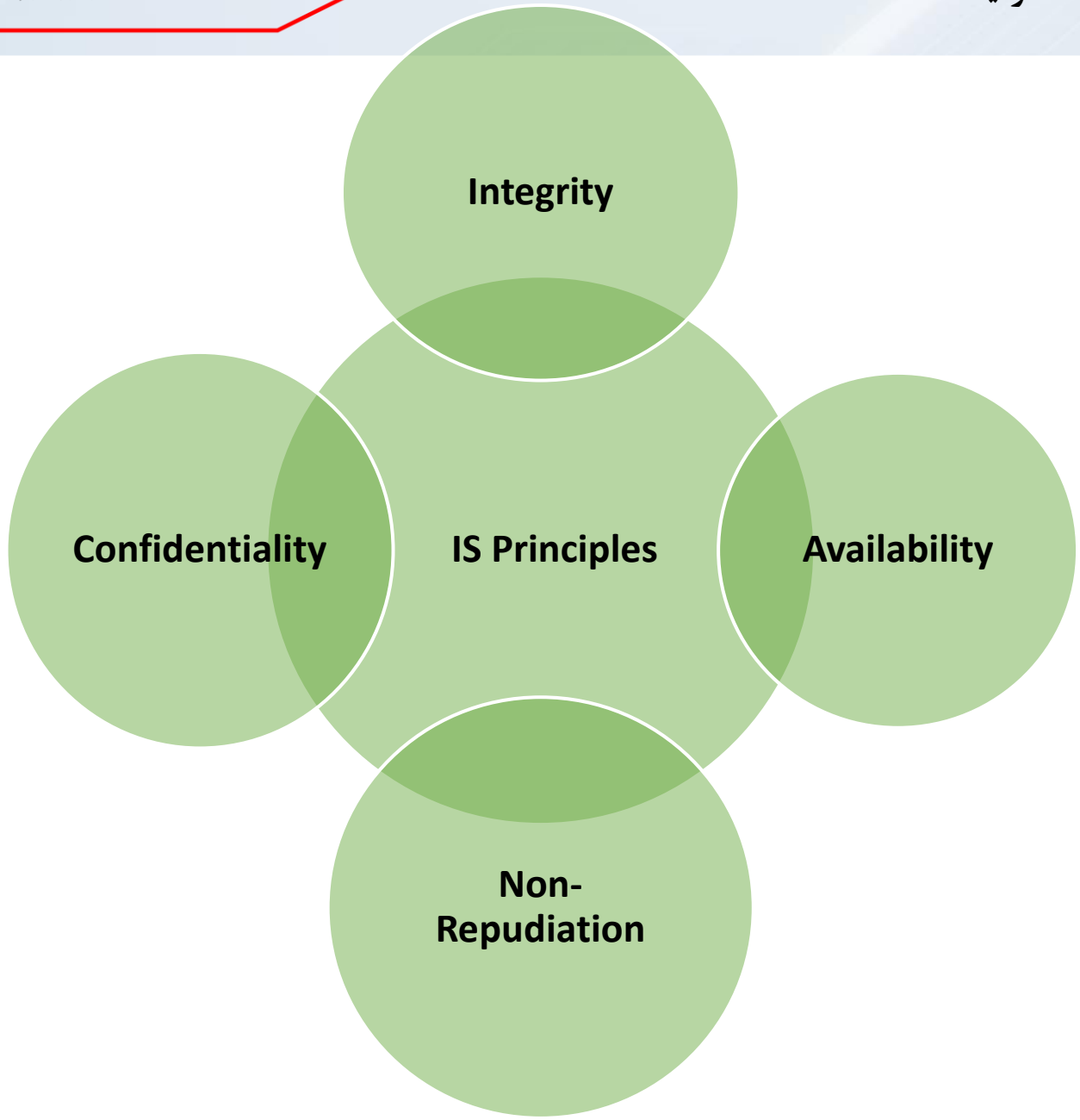
- **سرية المعلومات**: ضمان عدم الكشف عن المعلومات لغير المصرح لهم.
- **سلامة المعلومات**: الحماية من التعديل أو الحذف غير المرخص للمعلومات أو التلف بأي شكل ولأي سبب وضمان أصالة المعلومات.
- **المخاطر**: الخطر هو احتمال وقوع حدث سيء من شأنه المساس بأمن المعلومات والآثار المترتّبة على ذلك.
- **التّهديدات**: أي شيء يمكن أن يسبب ضرراً على المعلومات كفعل أو ظرف أو حدث وذلك من خلال تدميرها أو كشفها أو تعديلها أو إيقاف خدماتها ونحو ذلك.

تعاريف

- **نقاط الضعف/ الثغرات**: خلل يمكن أن يستخدم للإضرار بالأصول المعلوماتية ويمكن أن يتواجد في إجراءات أو تصميم أو تنفيذ أو في الضوابط الداخلية لحماية النظام تحدث بشكل عرضي أو أن يتم استغلالها بشكل مقصود وينتج عنها خرق أمني أو انتهاك لسياسات أمن المعلومات.

- **إدارة المخـــاطـــر**: هي عملية مستمرة ومتكررة لتحديد نقاط الضعف والتهديدات ذات الصلة بالموارد المعلوماتية ومراقبتها والحّد من آثارها. وتتضّمن تقييم المخاطر، ومقارنة المزايا والعيوب، ووضع وتنفيذ واختبار الإجراءات الوقائّية وتقييم مستوى الحماية مع الأخذ بعين الاعتبار الفعالّية والكفاءة والأثر.

- **السياسة**: مجموعة من القواعد الإدارية تستخدم لإدارة وضبط الحالة المرغوبة للكيان الإداري (مثل أمن المعلومات).



المبادئ الأساسية لضمان أمن المعلومات

الأهداف

تهدف وثيقة السياسات العامة ... لوضع أسس عامة لسياسات أمن المعلومات الواجب توافرها وإتباعها والعمل بها في جميع الجهات الحكومية التابعة للجمهورية اليمنية من أجل ضمان الحفاظ على أمن وسرية المعلومات والأصول المعلوماتية وبما يعزز أداء الجهة الحكومية لأعمالها واستمرارها بتقديم خدماتها، وذلك من خلال:

أ. التأكد من أن جميع الموظفين على علم ودراية بمهامهم وأدوارهم ومسؤولياتهم والامتثال الكامل للتشريعات ذات الصلة بأمن المعلومات.

ب. تحديد ووضع المتطلبات الأساسية لأمن المعلومات والإجراءات اللازمة لحماية الأصول المعلوماتية التي تحت سيطرة وتحكم الجهة الحكومية.

ج. وصف مبادئ أمن المعلومات وشرح كيفية تنفيذها في الجهات الحكومية وتوفير مرجعية لكافة النواحي المتعلقة بأمن المعلومات.

د. رفع مستوى الوعي بأهمية وضرورة أمن المعلومات داخل الجهات الحكومية واعتمادها كجزء لا يتجزأ من الأعمال والمهام الدائمة داخل تلك الجهة.

هـ. توفير بيئة آمنة لتقديم وتطوير الخدمات الإلكترونية.

مجال ونطاق تطبيق السياسات

- تسري هذه السياسات على جميع الجهات الحكومية في الجمهورية اليمنية (داخل البلاد وخارجها) وعلى مسؤوليها وقياداتها وموظفيها والعاملين فيها بشكل دائم أو مؤقت، وعلى المتعاقدين معها، وعلى أي جهة أو فرع أو شركة أو وحدة يتم فيها تواجد بيانات ومعلومات خاصة بهذه الجهات الحكومية.
- تطبق على كافة الأصول المعلوماتية وعلى البيانات والمعلومات التي تمتلكها الجهة سواء التي يتم معالجتها واستخدامها داخل الجهات الحكومية أو خارجها.
- فريق أمن المعلومات المختص في الجهة على حسب طبيعة عمل الجهة وحجمها (شخص أو أكثر، أو وحدة مختصة) .
- تعتبر هذه الوثيقة وتعديلاتها أحد المكونات الأساسية للاستراتيجية الوطنية لأمن المعلومات التي يجب وضعها وإقرارها مستقبلاً على المستوى الوطني الشامل.

مدخل لسياسات أمن المعلومات

متطلبات إدارة وتنفيذ أمن المعلومات

يجب وضع خطة شاملة وواضحة لحماية أصول المعلومات التابعة لكل جهة حكومية وبطريقة تتناسب مع قيمة تلك المعلومات وحجم الضرر المتوقع حال فقدانها أو إساءة الاستخدام أو السرقة أو التعديل بطرق غير قانونية، وبما يضمن استخدامها وتخزينها ونقلها وإدارتها بطريقة فعالة، **ويجب أن يراعى في الخطة الاعتبارات التالية:**

1. **خطة إدارة وتنفيذ أمن المعلومات**

يجب أن تكون الخطة موثقة وتتضمن الإجراءات والتعليمات والسياسات الداخلية الواجب تنفيذها من قبل العاملين والمتعاقدين/ المتعهدين لديها، ويجب أن تحظى هذه الخطة بدعم من قيادات الجهة.

٢. تحديد سياسات أمن المعلومات

يجب تحديد سياسات أمن المعلومات في خطة أمن المعلومات للجهة وتعريفها وذلك وفق متطلبات أمن المعلومات، على أن يتم المصادقة عليها من قبل قيادات الجهة ونشرها لجميع المعنيين بتنفيذها، **ويجب أن تتضمن كل سياسة البنود/ الأقسام التالية:**

- تعريف السياسة والغرض منها وأهدافها.
- تحديد (البنود/ الضوابط) والمسئوليات والأدوار على كل شخص أو جهة تابعة لتنفيذ هذه السياسات والرقابة على الالتزام بها.
- إجراءات واضحة لحالات عدم الامتثال للسياسة.

متطلبات إدارة وتنفيذ أمن المعلومات

٢. إدارة وتنفيذ (خطة) أمن المعلومات

يجب أن تقوم الجهة بوضع إطار عمل لإطلاق الخطة والتحكم بآليات التنفيذ، من خلال فريق متخصص وبصلاحيات محددة وفترة زمنية محددة وتطويرها بشكل مستمر بما يشمل:

- تحديد فريق العمل المسئول عن تنفيذ السياسات أو مجموعة السياسات وإعداد تقارير عن مدى الالتزام مع الفترة الزمنية للتنفيذ.
- تحديد الجهات الداخلية (الوحدات الإدارية) أو الجهات الخارجية الملزمين بتنفيذ السياسة.
- وضع آلية واضحة لإبلاغ المعنيين في الجهة في حال حدوث أي طارئ يتعلق بأمن المعلومات، كفقدان للمعلومات أو الخدمات أو أي اختراقات أو نحو ذلك.
- وضع الأدوار والمسئوليات والمهام بين الوحدات الإدارية الداخلية بحيث لا تتعارض واجباتها وبما يضمن تحديد الوحدة الإدارية المسئولة عن عدم تنفيذ السياسات أو عند حدوث أي طارئ.

متطلبات إدارة وتنفيذ أمن المعلومات

٤. متطلبات أمن المعلومات

- تحديد متطلبات أمن المعلومات يختلف باختلاف أهمية المعلومات والبيانات والخدمات الإلكترونية المعتمدة، **ويجري تحديد هذه المتطلبات اعتماداً على ثلاثة مصادر أساسية:**
- تقييم المخاطر التي قد تهدد الجهة الحكومية، مع الأخذ بعين الاعتبار أهدافها والخدمات التي تقدمها ومدى الضرر المتوقع من هذه المخاطر.
- القوانين والأنظمة والتعليمات وغيرها مما يتعلق بعمل الجهة الحكومية، أو المتعلقة بالخدمات الإلكترونية التي تقدمها الجهة.
- متطلبات نجاح الجهة الحكومية في تحقيق أهدافها وتنفيذ مهامها.

متطلبات إدارة وتنفيذ أمن المعلومات

- تطبيق سياسات أمن وحماية المعلومات التي توفر الحد الأدنى للممارسات المتعلقة بأمن وحماية المعلومات في الجهة.
- تعميم السياسات على جميع الموظفين والعاملين في هذه الجهة الحكومية كلاً فيما يخصه وجعلها في متناول المعنيين بشكل مستمر، كون أمن المعلومات هو مسؤولية كل موظف في الجهة الحكومة.
- وضع التعليمات والإجراءات المناسبة لتطبيق السياسات.
- تضمن الجهة أن الحماية الأمنية تكون متلائمة ومتوافقة مع تغيرات البيئة والتكنولوجيا.
- توفر الجهة بند مالي في الموازنة لتغطية احتياجات ومصادر الحماية الأمنية الضرورية.
- حفظ وصيانة البرمجيات وعقود الصيانة والضمانات سارية المفعول بعناية وبشكل سليم.

الأدوار والمسئوليات والواجبات العامة
الجهة الحكومية

- تطبق الجهة سياسات فعالة للفصل بين المهام والواجبات لتجنب تنفيذ كل المهام الأمنية بشكل فردي.
- تعيين ضابط أمن معلومات وتوفير الدعم اللازم له من أجل توفير المهارات والتدريب الكافي للموظفين والعاملين في الجهة والإشراف على فهم وتطبيق السياسات والتعليمات الخاصة بأمن وحماية المعلومات فيها.
- ضمان سرية وسلامة وتوفر المعلومات لنظم المعلومات التابعة لها حتى المدارة من قبل جهات خارجية.
- منح الموظفين أقل الصلاحيات اللازمة على موارد نظم المعلومات بما يضمن سير العمل، بناءً على تصنيف البيانات أو الإدارة التي ينتمي اليها الموظفون وطبيعة عملها ومستوى المسؤولية لكل موظف.
- التدقيق الدوري على مدى الالتزام بهذه السياسات داخل الجهة بهدف تحديد ومعالجة أي قصور أو ثغرات لوحظت فيها.

الأدوار والمسئوليات والواجبات العامة
الجهة الحكومية

- وضع وتوضيح الإجراءات المناسبة لمحاسبة الموظفين والعاملين في الجهة عن أي خلل أو قصور من شأنه الإخلال بأمن وحماية أي من الموارد المعلوماتية في الجهة طبقاً للأنظمة المعمول بها.
- يجب على الجهة إبلاغ الموظفين (الدائمين -المتعاقدين – المؤقتين) أنه في حال انتهاك أي من بنود سياسات أمن المعلومات قد يتعرضون للمحاسبة وإنهاء خدمتهم في الجهة وذلك تبعا لدرجة خطورة الانتهاك.
- يجب اختيار الموظفين المعنيين بمهام وأعمال أنظمة المعلومات/قواعد البيانات بعناية وفق سياسة أمن التوظيف والموظفين.
- يجب على الجهة إعلام الموظفين بمسؤولياتهم فيما يخص أمن المعلومات من بداية تعيينهم وخلال فترة عملهم في الجهة بشكل دوري.

الأدوار والمسئوليات والواجبات العامة الجهة الحكومية

- على كافة مدراء /مسئولي الانظمة والتجهيزات وقواعد البيانات تطبيق التعليمات والإجراءات على جميع الموارد المعلوماتية الموجودة في الجهة الحكومية بالتوافق مع سياسات أمن وحماية المعلومات.
- توفير الدعم الفني الكافي الذي يضمن تطبيق هذه السياسات من قبل المعنيين في الجهة.
- على جميع الموظفين الالتزام بقراءة السياسات وفهمها والرجوع إليها عند الحاجة، والتوقيع بالتقيد على ما جاء فيها.
- على كافة قيادات ومدراء وموظفي الجهات بذل أقصى الجهود الممكنة لتنفيذ السياسات والتعليمات المتعلقة بها في الجهة.
- على كافة الموظفين التعاون مع المختصين في مجال تكنولوجيا وأمن وحماية المعلومات والرجوع إليهم عند الحاجة والتعاون مع مدققي أمن المعلومات للقيام بمهامهم بيسر وسهولة.

الأدوار والمسئوليات والواجبات العامة
الجهة الحكومية

- التأكد من تطبيق سياسات أمن وحماية المعلومات والتعليمات والإجراءات المتعلقة بها في الجهة بشكل دوري والرفع بتقارير عن درجة ومستوى تطبيق السياسات.
- الرفع بالمقترحات والتوصيات اللازمة ومنها الترقيات أو الترتيبات الواجب توفيرها سواءً كانت تجهيزات أو برمجيات أو إدارية أو نحوها.
- التعاون مع جميع العاملين والمتعاملين مع الجهة من أجل تطبيق هذه السياسات والتعليمات والإجراءات بأعلى مستويات الدقة الممكنة.
- القيام بدور التوعية المناسب لتدريب ورفع مستوى مهارات العاملين في الجهة في مجال أمن وحماية المعلومات من خلال تطبيق برامج التوعية الخاصة بأمن وحماية المعلومات، والمشاركة في ورش العمل والندوات ذات العلاقة.
- التدقيق على مدى التزام جميع العاملين والمتعاملين مع الجهة بالسياسات والتعليمات المتعلقة بها.

الأدوار والمسئوليات والواجبات العامة
ضابط أمن المعلومات

- يجب أن يتقيد مزودو الخدمات الخارجية أو البرامج التجارية المتعاملين مع الجهة بسياسات أمن المعلومات في الجهة وأي من متطلبات أمن المعلومات التي تصدرها الحكومة.
- يجب على الجهة الحكومية مراقبة ومراجعة معايير أمن المعلومات المقدمة من مزودي الخدمات والبرامج التجارية لكي تتأكد من إدارتها بشكل صحيح.
- يجب أن يخضع المستشارون الخارجيون والمتعاقدون والموظفون المنتدبون والمؤقتون الذين يعملون مع الجهة الحكومية لنفس الضوابط والمتطلبات والمسؤوليات الخاصة بأمن المعلومات.

الأدوار والمسئوليات والواجبات العامة
الجهات الخارجية


خطة أمن المعلومات
خطة تقييم الأصول المعلوماتية
استراتيجية الإدارة العليا
خطة التدريب والتوعية
الخطة التشغيلية
سياسات وإجراءات أمن المعلومات + المعايير ونماذج العمل
خطة إدارة المخاطر
كشوفات التشييك الخاصة ببنود سياسات أمن المعلومات

إدارة مخاطر أمن المعلومات والتعامل معها

إعداد خطة/ مصفوفة تقييم الأصول المعلوماتية

تحديد التهديدات

تحديد الضوابط الأمنية الحالية

تحديد الثغرات

تحديد وتقدير التأثيرات السلبية

تقدير احتمالية وقوع الحوادث الأمنية

تحليل وتقييم مخاطر أمن المعلومات

التعامل مع مخاطر أمن المعلومات

إعداد خطة تقييم الأصول المعلوماتية

- تحديد الأصول المعلوماتية والمسئول عن كل أصل.
- تقدير الأصول المعلوماتية
- تحديد المعايير التي على أساسها يجب تقدير أهمية وحساسية الأصول المعلوماتية
- تحديد المقياس لتقدير الأصول المعلوماتية
- تحديد الاعتماديات والعلاقات بين الأصول
- مثلاً إذا انضرب نظام التشغيل، وهذا عادة سيؤدي على سبيل المثال إلى تلف للنظام المالي المثبت على نظام التشغيل.

تحديد الأصول المعلوماتية

١. الأصول الرئيسية

- عمليات وأنشطة الجهة.
- بيانات الجهة.

٢. الأصول الداعمة

وهي الأصول المعلوماتية التي تحتوي على ثغرات/ نقاط الضعف والتي يمكن استغلالها عن طريق التهديدات، والتي بالتالي ستؤدي إلى حدوث أضرار على الأصول الرئيسية للجهة أو الأصول الداعمة نفسها.

- المعدات.
- الموظفين.
- البرمجيات.
- المواقع وتجهيزاتها.
- الشبكات.
- الجهة/ التنظيم المؤسسي.

تقدير الأصول المعلوماتية

- يتم تقدير البيانات على حسب أهميتها وحساسيتها، وذلك بتقدير أهمية السرية والتكاملية والتوافر لتلك البيانات وبتقدير حجم الضرر والخسائر المادية وفقاً للمعايير التي تضعها الجهة إذا وقعت أي حادثة أمن معلومات لتلك البيانات.
- عادةً يتم تقدير أهمية وحساسية الأصول المادية والبرمجية بحساب قيمة شرائها أو تقدير قيمة شراء أصول بديلة لها إذا حدث أي تلف لتلك الأصول.
- يمكن استخدام الطريقتين السابقتين لتقدير نفس الأصل.
- يمكن التقدير بالطريقة التي تراها الجهة مناسبة لها.

مقاييس تقدير الأصول- أمثلة

المقياس الكمي	المقياس النوعي
0	منخفض جداً
1	منخفض
2	متوسط
3	عالي
4	عالي جداً أو حساس

المقياس الكمي	المقياس النوعي
0	منخفض
1	متوسط
2	عالي

- ينبغي أن استخدام نفس المدى والنوع عند تقدير الأصول، وتقدير التهديدات (بتقدير درجة احتمالية وقوعها أي وقوع حادث أمني)، وتقدير الثغرات وذلك بتقدير مستوى سهولة استغلالها من قبل التهديدات لإحداث تأثيرات سلبية على الأصول المعلوماتية.
- ما عدا تقدير المخاطر فقد يصل مدى القياس إلى 12

تقدير الأصول المعلوماتية- مثال

نوع الأصل	اسم الأصل	درجة السرية	درجة التكامل	درجة التوافر	الخسائر المالية أو توقف العمل	خصوصية البيانات الشخصية	المشاكل القانونية	المشاكل مع الأطراف الخارجية وفقدان الثقة	الأمن والأمان المادي للأشخاص	قيمة الأصل (المعدل)
المعدات	السيرفر الرئيسي	4	4	4	3	3	0	1	0	3
	الراوترات									
البرمجيات	النظام المالي									
الشبكات	الشبكة الداخلية									
الأشخاص	المهندسين									

التهديدات	الثغرات	التأثيرات السلبية
اختراق أو هجوم محتمل لأمن المعلومات باستغلال ثغرة ما. وقد تكون بشرية من داخل الجهة (الموظفين) أو من خارجها (المخترقين والأطراف الخارجية)، فقد تكون متعمدة أو غير متعمدة، أو قد تكون تهديدات طبيعية/ بيئية	نقطة ضعف في أي أصل معلوماتي.	العواقب الوخيمة أو الأضرار التي قد تحدث على الأصول المعلوماتية أو الجهة أو الأشخاص وذلك وفقاً لمستوى الثغرة/الثغرات التي يمكن استغلالها
يتم تقدير احتمالية وقوع التهديدات (الحوادث الأمنية) وفقاً للعوامل التالية: - عدد مرات حدوث الحادثة (التهديد) سابقاً- سواءً داخل أو خارج الجهة. - درجة سهولة استغلال الثغرات الموجودة (من قبل التهديدات). - الضوابط الحالية ومدى فاعليتها في تقليل مستوى الثغرات، وبالتالي تقليل فرصة نجاح التهديد لإحداث تأثيرات سلبية.	قد تكون هناك نقاط ضعف تقنية (المعدات والبرمجيات) أو في السياسات أو إدارية أو بيئية أو في الموظفين أو الأطراف الخارجية.	يتم تحديد التأثيرات السلبية لجميع التهديدات/الحوادث المحتملة وفقاً للعوامل الخاصة بتقدير الأصول إضافة إلى العوامل التالية: - الوقت والتكاليف المالية المستغرقة للتحليل والتدقيق وإصلاح الضرر. - العمل أو الوقت الضائع والفرص المفقودة.

الثغرات والتهديدات والتأثيرات السلبية

أصناف التهديدات
Threats –

- **الأضرار المادية:** مثل الحرائق ومشاكل المياه والغبار وتآكل الأجهزة وتدمير/تلف المعدات، التعرض للقصف/الحروب الخ.
- **الحوادث الطبيعية/ البيئية:** مثل الظواهر المناخية (الحرارة أو الرطوبة الشديدة...) والفيضانات والزلازل والبراكين، الخ.
- **خلل في الأجهزة الخدمية أو الخدمات الأساسية:** مثل خلل أو انقطاع التكييف أو الطاقة/ الكهرباء، أو فشل في معدات الشبكة والاتصالات.
- **خروقات لأمن البيانات:** مثل التجسس عن بعد أو التنصت أو كشف البيانات الغير مصرح به أو سرقة المستندات أو سرقة وسائط التخزين أو المعدات.
- **الأعطال/ الخلل التقني:** مثل تعطل المعدات أو فشل في أداء وظائف المعدات.
- **الأنشطة الغير مصرح بها:** مثل استخدام غير مصرح به للمعدات أو إتلاف البيانات.
- **مشاكل في الوظائف/ العمليات:** مثل أخطاء في الاستخدام أو انتهاك للحقوق الملكية أو الفكرية أو عدم تواجد الموظفين.
- **الإشعاعات:** مثل الإشعاعات الكهرومغناطيسية أو الحرارية، أو النبضات الكهرومغناطيسية، الخ.

تحديد الضوابط الأمنية المطبقة حالياً

- بعد تحديد التهديدات الأمنية يجب تحديد الضوابط والإجراءات والمعايير الأمنية المطبقة حالياً في الجهة، سواءً كانت إدارية أو تقنية، وذلك لتجنب القيام بأي عمل مكرر وغير ضروري وتجنب التكلفة الغير ضرورية .
- يجب التأكد من أن الضوابط الحالية مطبقة وفعالة لأن الضوابط الغير فعالة تؤدي إلى ثغرات أمنية.
- وإذا لم تكن الضوابط فعالة، فيجب عند إعداد خطة التعامل مع المخاطر (الحلول) تحديد أنه سيتم تحديد الحلول لذلك مثل تحديث أو تغيير تلك الضوابط.
- ويتم معرفة أن الضوابط غير فعالة بأنها لا تؤدي النتائج المطلوبة، أي أن الحوادث الأمنية لا زالت تحدث.

أنواع الأصول والثغرات والتهديدات المرتبطة بها مع تأثيراتها السلبية- مثال

النوع	أمثلة على الثغرات	أمثلة على التهديدات	التأثيرات السلبية
البيانات	عدم توفر سياسة للتحكم بالوصول، الخ	الوصول الغير مصرح به للبيانات	سرية أو تكامل أو توافر البيانات
	عدم استخدام التواقيع الرقمية أو النسخ الاحتياطية أو عدم تشفير البيانات	تدمير أو تعديل أو تزوير أو فقدان البيانات	تكامل أو توافر البيانات
	عدم وجود بدائل للأجهزة أو نسخ احتياطية للبيانات أو حماية الأجهزة التي توجد عليها البيانات من القراصنة	انقطاع الخدمة DOS	توافر البيانات
	لا يوجد في النظام آليات للتأكد من بيانات المصادقة السرية	انتحال شخصية المستخدمين	سرية أو تكامل أو توافر البيانات
	عدم تشفير البيانات	التجسس	سرية البيانات
	عدم استخدام التواقيع الرقمية، الخ	الإنكار	المحاسبة والمسائلة
Hardware المعدات	تركيب خاطئ للأجهزة أو سائط التخزين أو صيانة غير كافية لها	خرق لسهولة صيانة نظم المعلومات	عدم تكامل أو توافر البيانات
	نقص في خطط استبدال الأجهزة قبل انتهاء عمرها الافتراضي، خصوصاً وسائط (أجهزة) التخزين	تلف للأجهزة أو وسائط التخزين	عدم توافر البيانات أو تكاملها
	تعرض الأجهزة للرطوبة أو الغبار أو الأتربة	التآكل/ الصدأ والغبار والتجمد.	عدم توافر البيانات
	الحساسية للإشعاعات الإلكترونية	خطأ في الاستخدام	عدم توافر البيانات أو تكاملها

طرق التعامل مع مخاطر أمن المعلومات (معالجتها)

١. **تخفيف درجة الخطر.**

وذلك (بإعداد) وتنفيذ ضوابط تقنية أو إدارية معينة.

٢. **الإبقاء على الخطر (تقبله).**

وذلك إذا كانت تكاليف تخفيف درجة الخطر لا تعطي أي منفعة للجهة. مثلاً تكلفة شراء وتشغيل وترخيص جدار ناري أكثر من الخسائر (التأثيرات السلبية) التي قد تحدث للجهة عند استغلال هذه ثغرة عدم وجود جدار ناري.

٣. **تجنب الخطر.**

وذلك بتوقيف النشاط الذي يؤدي إلى ذلك الخطر، مثل عزل الإنترنت عن الشبكة الداخلية.

٤. **مشاركة الخطر.**

وذلك بنقل مسئولية أمن الأصل أو جزء من المسئولية على أطراف أخرى مثل شركات التأمين أو المزودين.

تحديد معايير لمستويات المخاطر- مثال

مستوى الخطر كمّاً	ما يقابله نوعاً/ الأولوية في المعالجة	معيار مستوى الخطر
1-0	منخفض جداً	لا يوجد خطر- تجاهله
4-2	منخفض	تجاهل الخطر مع الانتباه لتغير مستوى الخطر مستقبلاً
6-5	متوسط	معالجة الخطر بإحدى الطرق الأربع المناسبة
8-7	عالي	معالجة الخطر في أقرب وقت بإحدى الطرق الأربع المناسبة
12-9	عالي جداً	معالجة الخطر فوراً بإحدى الطرق الأربع المناسبة

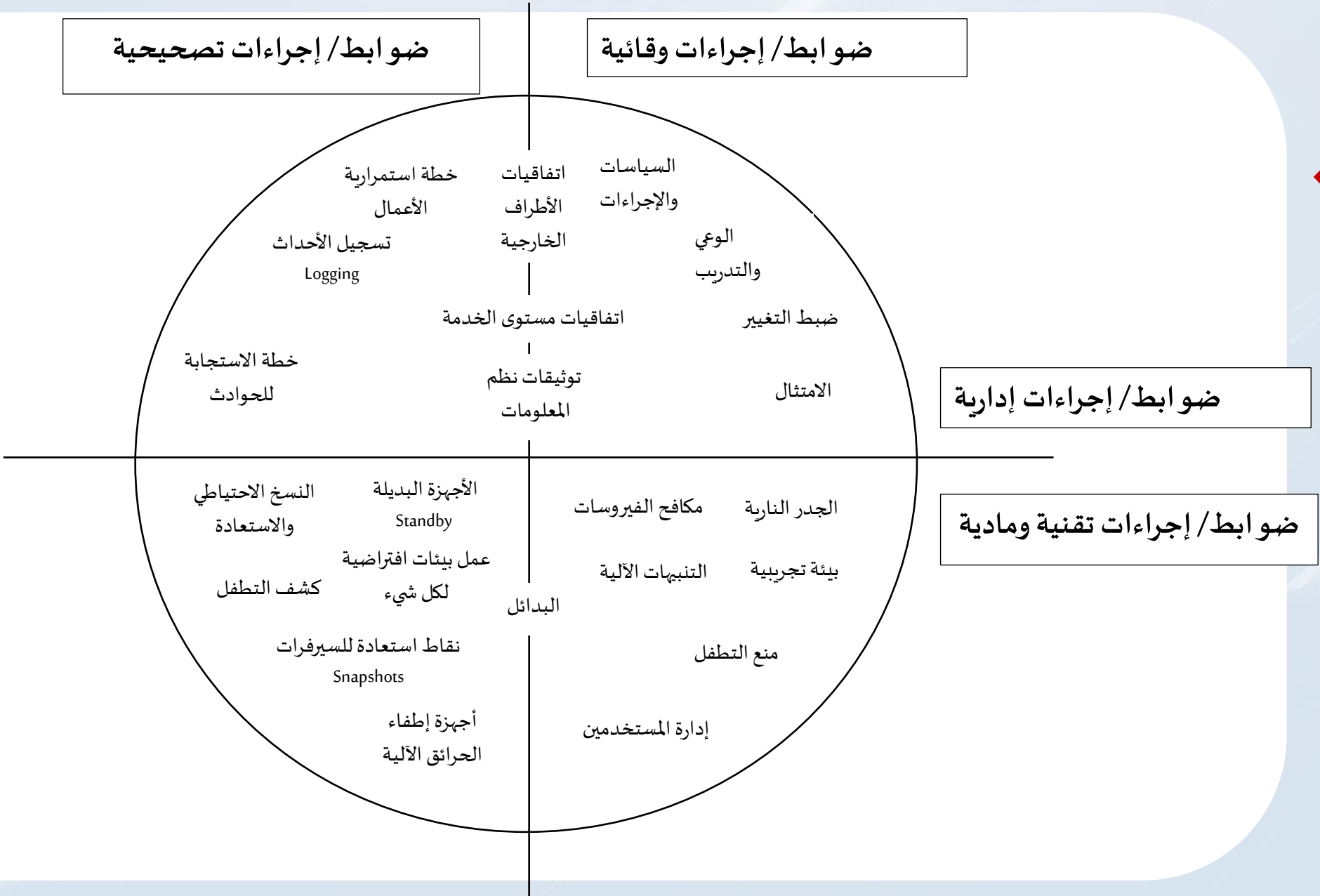
تحليل وتقييم مخاطر أمن المعلومات

Risk – Assessment

تقدير التهديد[1]	منخفض جداً (م.ج=0)					منخفض (م=1)					متوسط (ت=2)					عالي (ع=3)					عالي جداً (ع.ج=4)				
تقدير الثغرة[2]	م.ج	م	ت	ع	ع.ج	م.ج	م	ت	ع	ع.ج	م.ج	م	ت	ع	ع.ج	م.ج	م	ت	ع	ع.ج	م.ج	م	ت	ع	ع.ج
تقدير الأصل 0	0	1	2	3	4	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8
1	1	2	3	4	5	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9
2	2	3	4	5	6	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10
3	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
4	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12

نموذج على خطة إدارة المخاطر والتعامل معها

نوع الأصل	اسم الأصل	تقدير الأصل	التهديد	تقدير التهديد	الثغرة	تقدير الثغرة	مستوى الخطر	طرق التعامل مع الخطر
المعدات	السيرفر الرئيسي	4 تم تقدير السيرفر عالي جداً وفقاً لقيمته المالية	ارتفاع درجة حرارة السيرفر وتوقفه عن العمل	1 التقدير هنا ضعيف كون المكيف قديم لكن يوجد مكيف احتياطي	تعطل أو توقف المكيف	2 التقدير هنا متوسط كون المكيف قديم ويمكن أن يتعطل	6	تبديل المكيف القديم عند توفر الميزانية
		4	فقدان بيانات السيرفر	4 تم التقدير عالي جداً لأنه قد حدثت هذه الحادثة من قبل مرتين في كل عام	عدم عمل نسخ احتياطي لبيانات السيرفر	4 التقدير عالي كون الجهة لا تقوم بعمليات النسخ الاحتياطي	12	توفير المعدات والبرمجيات اللازمة فوراً لمزامنة النسخ الآلي لبيانات السيرفر وإعداد وتنفيذ سياسة للنسخ الاحتياطي والاستعادة


ضو ابط/ إجراءات وقائية
ضو ابط/ إجراءات تصحيحية
ضو ابط/ إجراءات إدارية
ضو ابط/ إجراءات تقنية ومادية
السياسات والإجراءات
اتفاقيات الأطراف الخارجية
خطة استمرارية الأعمال
الوعي والتدريب
تسجيل الأحداث Logging
ضبط التغيير
اتفاقيات مستوى الخدمة
الامتثال
توثيقات نظم المعلومات
خطة الاستجابة للحوادث
الجدر النارية
مكافح الفيروسات
الأجهزة البديلة Standby
النسخ الاحتياطي والاستعادة
بيئة تجريبية
التنبيهات الآلية
عمل بيئات افتراضية لكل شيء
كشف التطفل
البدائل
منع التطفل
نقاط استعادة للسيرفرات Snapshots
إدارة المستخدمين
أجهزة إطفاء الحرائق الآلية

إعداد الخطة التشغيلية - نموذج

الهدف	الأنشطة والإجراءات	مقياس الأداء	تاريخ البدء / تاريخ الانتهاء	المدة باليوم	المسئولين عن التنفيذ	المشرفين/ الوحدة الإدارية المشرفة	المتطلبات التشغيلية	الميزانية
إعداد سياسات وإجراءات أمن المعلومات الخاصة بالجهة	إعداد السياسات والإجراءات وفقاً للسياسات العامة	وثيقة سياسات وإجراءات أمن المعلومات الخاصة بالجهة	1/1/2022م / 31/2/2022م	60	الفريق التنفيذي	الفريق الإشرافي		
تحقيق الأمن المادي والبيئي لمركز بيانات الجهة.	تنفيذ بنود سياسة الأمن المادي والبيئي							
	تنفيذ بنود سياسة إدارة التحكم بالنفاذ والوصول...							
التدريب والتوعية	تدريب وتوعية المهندسين							
	تدريب وتوعية المطورين							
	تدريب وتوعية المستخدمين							

السياسات العامة المفترض تضمينها في خطة أمن المعلومات

1. سياسة الأمن المادي والبيئي
2. سياسة أمن التوظيف والموظفين (الموارد البشرية)
3. سياسة التعاقد والتعامل مع الأطراف الخارجية
4. سياسة الامتثال
5. سياسة تصنيف المعلومات
6. سياسة إدارة الأصول المعلوماتية
7. سياسة ضبط التغيير
8. سياسة إدارة التحكم بالنفاذ والوصول
9. سياسة خصوصية البيانات
10. سياسة تطوير أو اقتناء البرمجيات وصيانتها
11. سياسة أمن الشبكات والاتصالات
12. سياسة أمن الإنترنت
13. سياسة أمن البريد الإلكتروني
14. سياسة التشفير
15. سياسة الحماية من البرامج الخبيثة
16. سياسة النسخ الاحتياطي والاستعادة
17. سياسة إدارة حوادث أمن المعلومات
18. سياسة خطة الاستجابة للطوارئ واستمرارية الأعمال
19. سياسة مراقبة وتقييم وتدقيق المخاطر الأمنية

هيكل السياسات - بشكل مفصل

- اسم السياسة.
- الهدف.
- النطاق.
- البنود.
  - بنود عامة
  - مسئوليات الإداريين
  - مسئوليات الفنيين
  - مسئوليات المستخدمين/ الموظفين
  - مسئوليات الأطراف الخارجية
  - مسئوليات الحراس الأمنيين
- المسئول عن تنفيذ السياسة.
- المسئول الإداري عن السياسة.
- تاريخ نفاذ السياسة.
- إلزامية التنفيذ

البند	المطابقة	الملاحظات	الأدوار
المسئوليات/ البنود العامة			
هل أماكن الأصول المعلوماتية الحساسة مزودة بباب مدرع؟	☐نعم ☐لا ☐غ.م		☐ المراجع ☐ المدقق
هل أماكن الأصول المعلوماتية الحساسة مزودة بجهاز بصمة لفتحها؟	☐نعم ☐لا ☐غ.م		☐ المراجع ☐ المدقق
هل توجد منظومة كاميرات مراقبة فعالة داخل وخارج الجهة تغطي جميع الأصول المعلوماتية ومراكز البيانات؟	☐نعم ☐لا ☐غ.م		☐ المراجع ☐ المدقق
هل توجد منظومات وطفايات حريق CO_2 داخل وخارج مراكز البيانات؟	☐نعم ☐لا ☐غ.م		☐ المراجع ☐ المدقق
هل توجد أجهز إنذار ومكافحة حرائق آلية داخل مراكز البيانات؟	☐نعم ☐لا ☐غ.م		☐ المراجع ☐ المدقق

نموذج لـ
Checklist
لسياسة الأمان المادي والبيئي

أي أسئلة؟

شكراً لكم