17

سياسة إدارة الحوادث الأمنية
وخطة الاستجابة للطوارئ

م/ سيف السياغي

بنود السياسة

- يجب أن تضمن خطة أمن المعلومات إجراءات واضحة لإدارة الحوادث المرتبطة بأمن المعلومات ومعالجتها بطريقة فعالة وفي الوقت المناسب.
- يجب توقع الحوادث الأمنية المحتملة والتخطيط للاستجابة لها وبما يتلاءم مع دراسة تقييم المخاطر المحتملة وخطط استمرارية الأعمال لدى الجهة.
- يجب على الجهة الحكومية إعداد خطة للاستجابة للطوارئ تتضمن تحديد فريق طوارئ ومهام وإجراءات واضحة ومناسبة.
- يتعين على المعنيين الإبلاغ عن حوادث أمن المعلومات الهامة المتعلقة بالهجمات الإلكترونية ومحاولات الاختراق التي تتعرض لها الجهة، حتى يتسنى للمختصين في وزارة الاتصالات وتقنية المعلومات تقديم الدعم الفني المناسب.

عناصر السياسة

- المقدمة
- الاهداف
- النطاق
- بنود سياسة ادارة الحوادث الامنية وخطة الاستجابة للطوارئ
- الأدوار والمسئوليات

المقدمة

سياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ في الجهة الحكومية تشكل مجموعة من التوجيهات والإجراءات المستندة إلى المعرفة والخبرة في مجال الأمان السيبراني. يتعامل هذا الإطار مع كيفية التعامل مع الحوادث الأمنية والتهديدات السيبرانية في سياق الجهة الحكومية.

الهدف

- الحد من الضرر الناجم عن الحوادث الأمنية
- استعادة الخدمات والأنظمة المتأثرة
- اتخاذ الإجراءات الوقائية للحد من تكرار الحوادث الأمنية

النطاق

نطاق هذه السياسة يشمل الأصول المعلوماتية والموارد البشرية والتقنية التي تمتلكها وتديرها الجهة الحكومية.

وعلى الجهة الحومية تحديد النطاق بدقة واضحة لضمان التنفيذ الفعّال لهذه السياسة.

و ان يتضمن النطاق الاتي :

- **الأصول المعلوماتية:** الأنظمة والبيانات والتطبيقات وأي عناصر أخرى تتعلق بالأمان المعلوماتي.
- **الأشخاص المعنيين:** يشمل هذا النطاق جميع الموظفين بالجهة الحكومية ،ومدير امن المعلومات ومدير النظام .
- **الإجراءات والأمور المتعلقة بالأمان:** أي إجراءات أو سياسات أخرى تؤثر على الأمان العام للجهة الحكومية.
- **مو اقع:** يشمل النطاق المواقع الجغرافية أو المواقع التي يمكن أن تتأثر بالحوادث الأمنية والطوارئ.

طرق تطوير القدرات والإجراءات الأمنية

الإدارة الشاملة: تعتمد على إدارة شاملة للحوادث الأمنية، بما في ذلك الاستجابة والوقاية والتعامل مع التهديدات.

التحليل والتقييم: تهدف إلى تحليل وتقييم التهديدات والحوادث بشكل دقيق لتصنيفها وفهم أثرها.

الاستعداد والاستجابة: تقديم خطة تحتوي على إجراءات محددة وخطوات سريعة للاستجابة للحوادث والطوارئ.

المراقبة والمتابعة: توفير إطار لمراقبة الأنشطة والتعامل مع أي تغيرات أمنية بشكل فعال.

التوثيق والإبلاغ: توثيق جميع الأحداث والإجراءات وتقديم تقارير منتظمة لأغراض المراجعة والإبلاغ.

التحسين المستمر: تشجيع على التحسين المستمر للأمان السيبراني من خلال التقييم الدوري والتعلم من الحوادث.

تغطي سياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ على التالي:

- تحديد أنواع الحوادث الأمنية التي يمكن أن تؤثر على الجهة.

يمكن أن تشمل هذه الحوادث ما يلي:

- الاختراقات الأمنية
- البرمجيات الضارة
- فقدان البيانات
- الهجوم على البنية التحتية
- التهديدات البشرية

تغطي سياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ على التالي:

- تحديد أنواع الحوادث الأمنية التي يمكن أن تؤثر على الجهة.
- تحديد الإجراءات التي يجب اتخاذها عند وقوع حادث أمني.

يجب أن تغطي هذه الإجراءات ما يلي:

- اكتشاف الحادث الأمني
- تحديد نطاق الحادث الأمني
- التحقيق في الحادث الأمني
- تخفيف الأثر الضار للحادث الأمني
- استعادة الخدمة أو النظام المتأثر
- اتخاذ الإجراءات الوقائية للحد من تكرار الحادث الأمني

تغطي سياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ على التالي:

- تحديد أنواع الحوادث الأمنية التي يمكن أن تؤثر على الجهة.
- تحديد الإجراءات التي يجب اتخاذها عند وقوع حادث أمني.
- تحديد الأدوار والمسؤوليات للأفراد والفرق المشاركة في إدارة الحوادث الأمنية.

كمثال أن تتضمن الأدوار والمسؤوليات ما يلي:

- قائد فريق إدارة الحوادث الأمنية والفريق التابع له
- فرق الاستجابة للطوارئ
- فرق تقنية
- فرق قانونية
- فرق علاقات عامة

تغطي سياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ على التالي:

- تحديد أنواع الحوادث الأمنية التي يمكن أن تؤثر على الجهة.
- تحديد الإجراءات التي يجب اتخاذها عند وقوع حادث أمني.
- تحديد الأدوار والمسؤوليات للأفراد والفرق المشاركة في إدارة الحوادث الأمنية.
- تحديد الأدوات والتقنيات التي سيتم استخدامها في إدارة الحوادث الأمنية.

يمكن أن تشمل هذه الأدوات والتقنيات ما يلي:

- نظام إدارة الحوادث الأمنية
- أدوات التحقيق في الحوادث الأمنية
- أدوات استعادة الخدمة
- أدوات الاستجابة للطوارئ

تغطي سياسة إدارة الحوادث الأمنية وخطة الاستجابة للطوارئ على التالي:

- تحديد أنواع الحوادث الأمنية التي يمكن أن تؤثر على الجهة.
- تحديد الإجراءات التي يجب اتخاذها عند وقوع حادث أمني.
- تحديد الأدوار والمسؤوليات للأفراد والفرق المشاركة في إدارة الحوادث الأمنية.
- تحديد الأدوات والتقنيات التي سيتم استخدامها في إدارة الحوادث الأمنية.
- تحديد الاتصالات والتقارير التي سيتم إجراؤها عند وقوع حادث أمني.

يجب أن تغطي هذه الاتصالات والتقارير ما يلي:

- الاتصال مع الإدارة العليا
- الاتصال مع الفرق المشاركة في إدارة الحوادث الأمنية
- الاتصال مع الجهات الخارجية، مثل الجهات الحكومية ذات العلاقة
- التقارير اللاحقة للحادث الأمني

إجراءات الاستجابة للحوادث الأمنية:

- **الكشف عن الحوادث: يجب على جميع الموظفين الإبلاغ عن أي حادث أمني أو انتهاك يتعلق بأمان المعلومات فور حدوثه**
- **تصنيف الحوادث: يتم تصنيف الحوادث وفقًا لخطورتها وتأثيرها على الجهة ومواردها.**
- **تقييم الحوادث: يتم تقييم الحادث لفهم طبيعته وتأثيره واتخاذ الخطوات اللازمة للتصدي له.**
- **تقرير الحوادث: يجب على مسؤولي الأمن توثيق الحادث وإعداد تقرير يحتوي على التفاصيل والإجراءات المتخذة.**
- **التحقيق والمعالجة: يجب على الجهة تشكيل فريق تحقيق يتولى التحقيق في الحادث واتخاذ الإجراءات اللازمة للمعالجة وتقييم التأثير.**
- **استجابة للطوارئ: يجب تطوير وتنفيذ خطة استجابة للطوارئ تشمل إعادة تأهيل الخدمات المتأثرة وتقديم الدعم للمستخدمين وضمان استمرارية الأعمال.**
- **مراجعة وتحسين: يتعين مراجعة الحوادث والاستجابة المتبعة بانتظام لتحسين إجراءات الاستجابة وزيادة الوعي الأمني.**

وزارة الاتصالات وتقنية المعلومات

الأدوار والمسئوليات

كمثال لمسئولية الجهة

يجب على الجهة إنشاء آلية لتحديد الحوادث ومراقبتها.

يجب أن تكفل الجهة أن كل سجلات ومعلومات موارد المعلومات محفوظة لغرض إثبات وتتبع الحوادث الأمنية للعمل على حلها واسترجاعها وقت الحاجة.

يجب على الجهة أن تنشئ وتوثق وتحفظ خطوات معالجة الحوادث الأمنية لأنظمة المعلومات التابعة لها.

الأدوار والمسئوليات

كمثال لمسئولية المستخدمين

- يجب معرفة وإتباع خطوات معالجة الحوادث الأمنية الموثقة من قبل الإدارة العليا.
- يجب الإبلاغ عن جميع أعطال الشبكة أو أنظمة البرمجيات ومناطق الضعف لأمن المعلومات إلى الجهة المختصة وفقًا لإجراءات التعامل مع الأحداث الأمنية.
- يجب اتخاذ الخطوات الانية في حالة وجود اختراق النظام وفقا لخطوات معالجة الحوادث الأمنية الموثقة.