**مثال توضيحي عن سياسة أمن المعلومات**

**(تم حذف جزء كبير من المعلومات التي تتعلق بالشركة X)**

**الفصل الأول**

**سياسة أمن المعلومات في شركة X**

# أولاً - مقدمة

"تعريف بالشركة ... والأنظمة المعلوماتية المستخدمة لديها وعلاقتها بتحقيق أهداف أعمالها...." ونظراً لأهمية هذه المنظومة المعلوماتية في إنجاز ...، فإن الشركة تسعى جاهدةً للتصدي­ للتهديدات التي تستهدفها والتقليل من المخاطر ... ، وذلك من خلال اتخاذ كافة تدابير الحماية المناسبة وتبني أفضل ممارسات أنشطة إدارة أمن المعلومات المعتمدة وفق الأنظمة النافذة والمعايير الدولية ذات الصلة.

وتتضمن سياسة أمن المعلومات ... . وتتكون من هذا الفصل، الذي يعبر عن توجيهات إدارة الشركة وإرشاداتها اتجاه حماية أصولها المعلوماتية، ومن مجموعة من السياسات الخاصة المتعلقة بتدابير الحماية المعتمدة في الشركة.

# ثانياً - الهدف

إن الهدف من سياسة أمن المعلومات هو إنشاء إطار عمل ناظم لإدارة أمن المعلومات في الشركة لضمان سرية وسلامة وإتاحة المعلومات (يمكن إضافة متطلبات أخرى حسب الحاجة) بشكليها الرقمي والورقي بما يتوافق مع القوانين والأنظمة الحاكمة، وضمان اعتماد أفضل ممارسات أمن المعلومات المناسبة والفعّالة، ... .

# ثالثاً - نطاق سياسة أمن المعلومات

تغطي سياسة أمن المعلومات في الشركة X المعلومات والبيانات بشكليها الورقي والإلكتروني والأنظمة الحاسوبية والبرمجية والبنية التحتية الشبكية وجميع الأنظمة المرتبطة بها. وتطبق هذه السياسة على المقر الرئيسي للشركة ..... ، وعلى جميع العاملين في الشركة ... وكل من يستخدم الأصول المعلوماتية... .

# رابعاً – الأنظمة والقوانين

إن الغاية من سياسة أمن المعلومات هو تحقيق أهداف الأمن آنفة الذكر تلبيةً لمتطلبات التشريعات والأنظمة المرعية، لذلك يجب تطبيق تدابير الحماية (الضوابط) وفق هذه السياسة تماشياً مع الأنظمة والقوانين والمعايير الدولية التالية (على سبيل المثال):

* قانون الجريمة الإلكترونية (الصادر بالقانون رقم ؟؟ تاريخ ؟؟)
* قانون الاتصالات (رقم ؟؟ تاريخ ؟؟)
* قانون حقوق الملكية الفكرية (رقم ؟؟ تاريخ ؟؟)
* المعيار ISO/IEC 27001
* ...

# خامساً - تعاريف

تستخدم المصطلحات والتعاريف التالية ضمن سياق هذه السياسة:

1. **الأصول المعلوماتية (information assets)**: كل ما هو قيّم للشركة، وتشمل المعطيات والمعلومات الهامة والحساسة بشكليها الرقمي والورقي، والمكونات الداعمة المستخدمة في توليد ومعالجة وتخزين ونقل المعلومات والتعامل معها سواء كانت أنظمة حاسوبية أو شبكية أو برمجية أو أفراد. ويجب حمايتها من جميع التهديدات التي تلحق الأذى أو الضرر بالشركة.
2. **الأنظمة المعلوماتية (information systems):** الأجهزة الحاسوبية والشبكية والأنظمة البرمجية وأي أنظمة أخرى تستخدم لمعالجة المعطيات، أو نقلها، أو تخزينها.
3. **أمن المعلومات (information security)**: تعنى بتأمين السرية والسلامة والإتاحة للمعلومات في الشركة.
   1. السرية (confidentiality): عدم إتاحة المعلومات أو كشفها لأفراد أو كيانات أو إجراءات غير مخولة.
   2. السلامة (integrity): وتعنى بصحة وكمال المعلومات، وتغطي منع حذف أو تعديل المعلومات من قبل أفراد أو كيانات غير مخولة.
   3. الإتاحة (availability): هي ميزة توفر المعلومات للكيانات المخولة عند الطلب.
4. **الضوابط الأمنية (security controls)**: الإجراءات والسياسات والتقنيات والممارسات التي تعتمد أو تستخدم لتخفيض أو الحفاظ على مستوى مخاطر أمن المعلومات.
5. **تقويم المخاطر (risk assessment):** تقييم للتهديدات التي تستهدف الأصول المعلوماتية وأثر هذه التهديدات على الأصول، وتقييم نقاط الضعف في الأصول المعلوماتية واحتمال حدوث الاختراقات، واقتراح الحلول المناسبة.
6. **إدارة المخاطر (risk management):** هي عملية تحديد المخاطر التي يمكن أن تؤثر على الأصول المعلوماتية وضبط هذه المخاطر والتقليل منها أو إلغاؤها بتكلفة مقبولة.
7. **التهديدات** (threats): أي شيء يمكن أن يسبب الضرر أو الخسارة للأصول المعلوماتية، مثل الأفعال التخريبية والكوارث الطبيعية وأخطاء التشغيل.
8. **الثغرات الأمنية** (vulnerabilities): مجموعة العوامل التي تساعد على حدوث اختراق. مثل غياب قواعد بناء كلمات المرور و وجود ثغرة أمنية في نظم التشغيل.
9. **نظام إدارة أمن المعلومات** (information security management system, ISMS): هو جزء من نظام الإدارة العام في الشركة ويغطي تطوير وتنفيذ وتشغيل ومراقبة ومراجعة وصيانة وتحسين أمن المعلومات في المنظمة لتحقيق أهداف الأعمال فيها. ويتكون من السياسات والإجرائيات والإرشادات والموارد ذات الصلة والأنشطة المدارة من قبل الشركة في سعيها لحماية أصولها المعلوماتية.

# سادساً - بيان السياسة

1. فريق أمن المعلومات: تشكل الشركة فريق أمن المعلومات ليشرف ويدير ويحرص على تأمين الدعم المالي لأنشطة إدارة أمن المعلومات في الشركة. ....
2. مسؤوليات فريق أمن المعلومات:
   1. متابعة تطوير سياسة أمن المعلومات وتوثيقها ومتابعة تبنيها من قبل...
   2. مراجعة سياسة أمن المعلومات وتقييم مدى الامتثال للسياسة....
   3. التخطيط لإدارة أمن المعلومات: يجب على فريق أمن المعلومات أن يخطط ويشرف على تنفيذ خطط إدارة أمن المعلومات. يجب أن تعالج هذه الخطط إدارة المخاطر وتقويمها، وأن ترفع سوية وعي العاملين في الشركة لأهمية أمن المعلومات ومساعدتهم على فهم سياسة أمن المعلومات، وتأهيلهم لتطبيق ممارسات الأمن المعتمدة في الشركة.
   4. إدارة أمن المعلومات في الشركة ومتابعة أنشطتها والإشراف عليها، ونذكر منها على سبيل المثال لا الحصر ما يأتي:
      1. تطوير وتوثيق ونشر ومراجعة سياسة أمن المعلومات؛
      2. تقويم المخاطر؛
      3. تنفيذ الحلول والضوابط الأمنية المتوافقة مع السياسة الأمنية التي تحد من آثار المخاطر الأمنية؛
      4. المسح الأمني وإدارة الثغرات الأمنية؛
      5. اختبارات الاختراق؛
      6. إعداد خطط التعامل مع الحوادث الأمنية، وخطط استمرارية الأعمال ، و وضع إجراءات processes التشغيل والإجرائيات procedures والإرشادات ذات الصلة بإدارة أمن المعلومات و وفق الحاجة؛
      7. التدقيق والتقييم ومراقبة الأنشطة الشبكية وأنشطة الأنظمة المعلوماتية؛
   5. مراجعة الوثيقة:...
   6. توثيق وتحديث وتقييم ضوابط وتدابير الحماية...
   7. تدريب وتوعية الموظفين: ....
   8. رفع التقارير: ...
   9. استكمال تطوير سياسة أمن المعلومات وفق متطلبات نظام إدارة أمن المعلومات ISO/IEC 27001:2022، بحيث تغطي على الأقل المواضيع التالية: تصنيف المعلومات، وأمن الموارد البشرية، وإدارة الأصول المعلوماتية، والتحكم بالنفاذ إلى الأصول المعلوماتية، وتشفير المعلومات والتعمية، والأمن المادي والبيئي، وعمليات التشغيل (إجرائيات التشغيل، حماية من الكودات الخبيثة، الحفظ الاحتياطي، مراقبة سجلات الأحداث والتدقيق، إدارة الثغرات الأمنية، تقويم المخاطر، ...)، أمن الاتصالات والشبكات، توريد وتطوير وصيانة الأنظمة، إدارة العلاقة مع الموردين، إدارة الحوادث الأمنية، إدارة استمرارية الأعمال، التقيد والامتثال للأنظمة والقوانين.
3. يتحمل مدير تقانة المعلومات مسؤولية...
4. يتحمل مدير أمن المعلومات مسؤولية...
5. يجب أن يظهر جميع الموظفين وكل من يُمنَح صلاحيات نفاذ إلى الأنظمة المعلوماتية في الشركة إلتزامهم بتطبيق أحكام سياسات أمن المعلومات في الشركة التي تطبق عليهم أو المرتبطة بالأصول المعلوماتية التي يستخدمونها.
6. عقوبات انتهاك سياسة أمن المعلومات: ... .
7. يجري تنظيم جميع الوثائق المتعلقة بالسياسة الأمنية والإجرائيات والأدلة الإرشادية وتحدث دورياً، وتحفظ نسخ وإصدارات الوثائق لمدة خمس سنوات على الأقل.

# سابعاً - العقوبات

تتخذ الشركة الإجراءات المناسبة ضد من ينتهك سياسة أمن المعلومات...

# ثامناً – بنية سياسة أمن المعلومات

تنظم مكونات سياسة أمن المعلومات من ....

# تاسعاً - تاريخ بدء تطبيق هذه السياسة

تحدد إدارة الشركة X تاريخ اعتماد وتطبيق سياسة أمن المعلومات وتحديثاتها اللاحقة.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**الفصل ؟؟**

**سياسة إدارة المخاطر**

# أولاً - لمحة

....

إن الهدف من هذه السياسة هو وضع الأسس لتحديد مكامن المخاطر ذات الصلة بالأصول المعلوماتية بالوقت المناسب وإدارة هذه المخاطر بهدف استمرارية انجاز الأعمال في الشركة وتأمين متطلبات أمن المعلومات فيها.

تطبق هذه السياسة على جميع الأصول المعلوماتية في الشركة.

وتتكون سياسة إدارة المخاطر من هذه الوثيقة و....

# ثانياً - بيان السياسة

1. تعد هذه السياسة وثيقة معلومات سرية.
2. يقع على عاتق فريق أمن المعلومات مسؤولية التطبيق السليم لهذه السياسة.
3. يتم وضع إجراءات وخطط إدارة مخاطر أمن المعلومات تلحظ سياق عمل الشركة والمنهجية المتبعة ومعايير قبول المخاطر والمسؤولين عن تنفيذها وتحديثها وتوثيقها.
4. يتم تحديد مكامن مخاطر أمن المعلومات بناءً على تقويم الثغرات الإدارية، والتشغيلية، والفيزيائية والبيئية، والتقنية التي تؤثر على انجاز الأعمال في الشركة.
5. يتم تقويم المخاطر واقتراح الحلول وتقديم التوصيات لتخفيض مستواها بما يتوافق وإمكانيات الشركة وحاجات استمرارية الأعمال فيها.
6. توضع خطط معالجة مخاطر أمن المعلومات بإشراف ....
7. تجرى عمليات تقويم المخاطر مرة على الأقل سنوياً، وقبل أي تعديل أو تحديث يتعلق بأحد الأصول المعلوماتية وبعد التعديل وقبل إدخال أنظمة جديدة.
8. ينفذ تقويم المخاطر بعد تعديل سياق عمل الشركة (صدور قوانين جديدة، متطلبات مالكين، ...).
9. ينفذ تقويم المخاطر على الأنظمة المعدلة أو المحدثة قبل وضعها في الخدمة و وصلها إلى الشبكة وبعد وضعها في الخدمة.
10. ...

# ثالثاً - العقوبات

يتعرض الموظف الذي يخالف أيٍ من الأحكام الواردة في هذه السياسة ...

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**الفصل ؟؟**

**سياسة إدارة الحوادث الأمنية**

# أولاً - لمحة

...

إن الهدف من هذه السياسة هو ضمان وجود طريقة فعالة ومناسبة لإدارة الحوادث الأمنية والتبليغ عنها وعن نقاط الضعف المكتشفة.

وتطبق هذه السياسة على جميع موظفي الشركة والمتعاقدين معها وأي طرف آخر لديه نفاذ إلى الأصول المعلوماتية في الشركة. وتغطي هذه السياسة جميع الأصول في الشركة.

وتتكون سياسة إدارة الحوادث من هذه الوثيقة والإجرائيات ذات الصلة.

# ثانياً - بيان السياسة

1. تعد هذه السياسة وثيقة معلومات سرية.
2. يقع على عاتق فريق أمن المعلومات مسؤولية التطبيق السليم لهذه السياسة.
3. يوضع إجراءً لإدارة الحوادث الأمنية والإجرائيات ذات الصلة، والإشراف على تنفيذها وتوثيقها مع تحديثاتها.
4. تصنف الحوادث الأمنية بهدف تسهيل التعامل معها.
5. يتم الإبلاغ عن أي حدث أمني وفق الإجرائيات المعتمدة، بسرية ومن دون كشف أي معلومات عنها إلا للمدير العام ولفريق أمن المعلومات، ويتم الاستجابة سريعاً للحوادث الأمنية بهدف الحد من أضرارها والرجوع بالسرعة الممكنة لحالة التشغيل الطبيعية.
6. يتم الإبلاغ عن أي ثغرة أمنية وفق الإجرائية المتبعة، بسرية ومن دون كشف أي معلومات عنها لغير الجهة المخولة داخل الشركة، ويمنع محاولة استغلالها.
7. يتولى فريق أمن المعلومات تنفيذ إجراء إدارة الحوادث بما فيه عمليات التحري وجمع الأدلة والمعالجة، واتخاذ كافة الإجراءات لمنع تكرار الحادث، وتوثيق الحادث وإجراءات المعالجة المتخذة، ويتم حفظ الوثائق مع الأدلة.
8. يحق لفريق أمن المعلومات مراقبة أنشطة الشبكة واستخدام الأصول المعلوماتية للكشف عن محاولات الاختراق وإساءة الاستخدام وجميع الأدلة مسبقاً.
9. يتم مناقشة حوادث أمن المعلومات ودراسة إمكانية الاستفادة من الدروس المكتسبة وتعديل السياسات الأمنية، ومراجعة تدابير الحماية المطبقة، وتعديل برنامج التدريب والتوعية وفق الحاجة.

# ثالثاً - ...

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**الفصل ؟؟**

**سياسة استمرارية الأعمال**

# أولاً - لمحة

....

إن الهدف من هذه السياسة هو ضمان استمرار إتاحة معلومات الشركة والأصول ذات الصلة للنفاذ لدى وقوع الحوادث الأمنية والكوارث التي تؤثر على أداء الأنظمة المعلوماتية.

تطبق هذه السياسة على الأصول المعلوماتية ... التي تستخدم في تنفيذ خطط استمرارية الأعمال في الشركة.

وتتكون سياسة استمرارية العمل من هذه الوثيقة و ...

# ثانياً - بيان السياسة

1. تعد هذه السياسة وثيقة معلومات ... (اذكر تصنيفها).
2. يقع على عاتق فريق أمن المعلومات مسؤولية متابعة التطبيق السليم لهذه السياسة.
3. يقوم فريق أمن المعلومات بتحليل تأثر الأعمال بالكوارث والأعطال المحتملة بهدف تقييم درجة ارتباط العمليات A و B بالأصول المعلوماتية ووضع وتوثيق الخطط والإجرائيات لاستمرارية تقديم الخدمات وإنجاز الأعمال وتحديد المتطلبات الأمنية للأصول المعلوماتية في حال الكوارث والحوادث الخطيرة.
4. يتم متابعة تأمين متطلبات تنفيذ إجرائيات استمرارية الأعمال المتعلقة بالأصول المعلوماتية واختبارها دورياً وتأهيل وتدريب الموظفين على تنفيذها.
5. يتم مراجعة خطط استمرارية الأعمال وتنفيذ تحليل تأثر الأعمال دورياً ...
6. ...

**الفصل ؟؟**

**سياسة المراقبة والتدقيق**

# أولاً - لمحة

...

إن الهدف من هذه السياسة هو وضع الأسس لمراقبة استخدام الأنظمة المعلوماتية وأنشطة المستخدمين، وتوليد الأدلة الرقمية ذات الصلة. كذلك تهدف هذه السياسة إلى اكتشاف حالات عدم الامتثال لسياسة أمن المعلومات، وإلى ...

# ثانياً - بيان السياسة

1. تعد هذه السياسة وثيقة معلومات داخلية.
2. يقع على عاتق فريق أمن المعلومات مسؤولية متابعة التطبيق السليم لهذه السياسة.
3. يحدد فريق أمن المعلومات الأنظمة المهمة (مخدمات، جدران نارية، تطبيقات، ...) التي تحتاج للمراقبة والأحداث التي تحتاج إلى التسجيل والمراقبة، ومدة الاحتفاظ بها بهدف المراجعة الدورية ولدى التحري عن الاختراقات الأمنية وإجراء عمليات التدقيق.
4. تعامل سجلات الأحداث كمعلومات سرية ويحتفظ بنسخ احتياطية منها وفق سياسة الحفظ الاحتياطي المعتمدة في الشركة وتنسخ أحداث الأنظمة الحساسة جداً إلى وسائط منفصلة عن الشبكة.
5. يتم مراجعة سجلات الأحداث كل ستة أشهر على الأقل، ولدى حصول حادث أمني وترفع التقارير إلى المدير العام.
6. يتم مزامنة ساعات جميع الأنظمة الحاسوبية المهمة موضوع عمليات تسجيل الأحداث والمراقبة والتدقيق.
7. يتم اتخاذ الإجراءات المناسبة لكشف ومنع محاولات تعديل أو حذف سجلات الأحداث.
8. يتم تسجيل محاولات الاختراقات الأمنية والأنشطة المشبوهة للتحري عنها.
9. يتم إنشاء قائمة بأسماء المستخدمين ومدراء الأنظمة وصلاحياتهم وتحدث كلما حصل تعديل.
10. يتم تنفيذ تدقيق داخلي على ضوابط أمن المعلومات وأنشطة الإدارة ذات الصلة وفق إجراء تدقيق وبرنامج تدقيق داخلي يراعي تكرار التدقيق، وطرائق تنفيذه، ومتطلبات التخطيط، وقوالب تقارير التدقيق.
11. تنفذ مراجعة مستقلة ودورية مرة على الأقل في السنة ولدى حدوث تغيير مهم في الأنظمة المعلوماتية لتقييم فعالية الضوابط الأمنية والتحقق من مؤامتها لتحقيق متطلبات أمن المعلومات ومدى التقيد بتطبيق سياسة أمن المعلومات، بحيث تغطي المراجعة الأطر المتخصصة، والإجراءات، والتقنيات المستخدمة. وترفع التقارير ذات الصلة إلى المدير العام الذي يوجه لإتخاذ الإجراءات التصحيحية ضمن الإمكانات المتاحة.

...