بنك سورية والمهجر
سياسة أمن المعلومات والأمن السيبراني

2024

4/29/2024
دائرة أمن المعلومات والأمن السيبراني
عامر العطوان

سياسة مختصرة عن سياسة أمن المعلومات والأمن السيبراني الشاملة والمتبعة في المصرف

بنك سورية والمهجر ش.م.س.ع

جدول المحتويات

مقدمة..... 2

1 . سياسة أمن المعلومات 3

2 . إدارة تصنيف وضبط الأصول المعلوماتية 3

3 . أمن الموارد البشرية 4

4 . الأمن المادي والبيئة المحيطة..... 5

5 . إدارة العمليات والشبكات والاتصالات 5

6 . سياسات المستخدم..... 6

7 . إدارة التحكم بالنفاذ وصلاحيات الدخول 6

8 . اقتناء النظم وتطويرها وصيانتها..... 7

9 . إدارة استمرارية العمل 7

10 . سياسة الوصول عن بعد..... 8

11 . أمن وصول الطرف الثالث 8

12 . الاستعانة بمصادر خارجية لتطوير تقنية المعلومات..... 9

13 . سياسة مركز البيانات..... 9

14 . سياسة الوصول إلى شبكة الانترنت 10

15 . سياسة إدارة الاستثناءات..... 10

16 . سياسة الأمن السيبراني..... 11

17. سياسة حماية أنظمة الدفع الإلكتروني 11

18 . سياسة الخصوصية وحماية البيانات..... 11

19 . سياسة الوصول إلى ملفات السجلات والاحتفاظ بها..... 12

20 . الامتثال وإدارة الحوادث الأمنية 12

21. سياسة تقوية النظام..... 13

مقدمة

تعتبر المعلومات من الأصول الهامة كأي أصل من أصول الأعمال والتي تكون بحاجة إلى حماية بشكل دائم ومستمر. حيث يتم استخدام المعلومات في كافة جوانب الأعمال التجارية، من معالجة المدفوعات إلى اتخاذ قرارات هامة في الاستثمارات. وتأتي المعلومات بصور مختلفة فإما أن تكون مكتوبة أو مطبوعة على أوراق أو مخزنة إلكترونياً أو منقولة عبر الشبكة أو حتى ما يتم قوله خلال المحادثات.

وتعتبر المعلومات إحدى أهم الأصول ذات القيمة في بنك سورية والمهجر، لذا يقوم المصرف بحمايتها بشكل مناسب من مجموعة واسعة من التهديدات لضمان السرية والسلامة والتوافر والتقليل من الخسائر التجارية. مع اتخاذ مجموعة مناسبة من الضوابط والإجراءات لتحقيق أمن المعلومات.

أمن المعلومات هو حماية المعلومات من مجموعة كبيرة من التهديدات لضمان استمرارية العمل وتقليل المخاطر. والتي يتم تحقيقها من خلال تطبيق مجموعة مناسبة من الضوابط والسياسات والاجراءات والعمليات والوظائف البرمجية والعتادية. وهذه الضوابط بحاجة إلى تأسيس وتطبيق ومراقبة ومتابعة ومراجعة وتحسين عند الضرورة لضمان أن هذه الضوابط الأمنية تلتقي مع أهداف العمل الخاصة بالمصرف.

وتزداد أهمية أمن المعلومات عندما يصبح العمل متصل على الشبكة مع مزودي خدمة خارجيين ومع فروع وخدمات على شبكة الانترنت. لذا يولي بنك سورية والمهجر أهمية قصوى للسعي لإدارة أمن المعلومات وضوابطه للحفاظ على مستوى عالي من الأمن الذي نسعى لتحقيقه.

1 . سياسة أمن المعلومات

تهدف سياسة أمن المعلومات إلى تحقيق الأمن الكلي للأصول المعلوماتية الخاصة بالمصرف. وتسعى إلى ضمان الحماية الكافية لجميع أصول تقنية المعلومات التي يعتمد عليها المصرف في تحقيق أعماله المصرفية والتجارية ونشاطاته.

الأهداف

توفير التوجيه والدعم الإداري لأمن المعلومات وفق متطلبات العمل وأهداف المؤسسة والقوانين واللوائح ذات الصلة.

يجب أن تضع الإدارة توجيهات سياسة واضحة متماشية مع أهداف العمل وتظهر الدعم والالتزام لأمن المعلومات من خلال إصدار السياسة والحفاظ عليها ضمن المؤسسة.

تعتبر سياسة أمن المعلومات المرجع الرئيسي لأمن المعلومات في بنك سورية والمهجر، وتساعد على التأكد من أن بيانات ومعلومات المصرف (بالإضافة إلى بيانات العملاء) والتجهيزات التقنية والشبكية المستخدمة لحفظ ونقل البيانات بالإضافة إلى أشكال المعلومات الأخرى محمية من التصريح أو التعديل أو التدمير المقصود وغير المقصود أو غير المصرح به

2 . إدارة تصنيف وضبط الأصول المعلوماتية

الهدف

تحديد جميع الأصول المعلوماتية وتحديد صاحب كل أصل وتزويد التوجيهات اللازمة لتحقيق الحماية المناسبة لأصول المصرف المعلوماتية والحفاظ عليها.

تحديد التوجيهات لتعريف التفاصيل الهامة لأصل ما، وفهم أهمية الأصول المعلوماتية لتوفير مستوى مناسب من الحماية لوقايتها بحسب الحساسية والخطورة.

الضوابط

يجب أن يقوم المصرف بتصنيف جميع الأصول المعلوماتية بما يتوافق مع طبيعتها ودرجة مخاطر أمن المعلومات المتعلقة بها وذلك لتحقيق الحد الأدنى من الضوابط الأمنية الأساسية المتوافقة مع سياسة أمن المعلومات.

3 . أمن الموارد البشرية

الهدف

الحد من المخاطر إلى مستويات مقبولة، والناتجة عن الأخطاء البشرية أو السرقة أو الاحتيال أو سوء الاستخدام لتجهيزات تقنية المعلومات. وضمان أن يكون الموظفون والمتعاقدون وموظفي الشركات الخارجية والأطراف الأخرى والموردين على وعي بمسؤولياتهم تجاه سرية وسلامة وتوافر والأصول المعلوماتية المصرفية، والتي تمكنهم ضرورة عملهم أو التوصيف الوظيفي الخاص بهم من الوصول إليها.

السياسة

يجب أن يقوم المصرف بفحص واختبار والتأكد من حالة ونزاهة الموظفين المحتملين المتقدمين إلى العمل بالإضافة إلى المتدربين ومزودي الخدمات من الأطراف الأخرى كالمتعهدين والمقاولين والبائعين. وتحديد المسؤوليات الأمنية كجزء من عقد العمل بالإضافة إلى اتفاقية السرية المصرفية.

4 . الأمن المادي والبيئة المحيطة

الهدف

منع الدخول الغير مصرح فيه إلى مراكز البيانات ومرافق معالجة المعلومات والأصول المعلوماتية في مبنى الإدارة العامة أو فروع المصرف، لتقليل الخسائر الناجمة عن السرقة أو التخريب أو المخاطر البيئية أو التلف للأصول المعلوماتية.

ووضع حماية مناسبة لمراكز البيانات والأصول المعلوماتية لمنع الوصول غير المصرح به، ويجب أن تكون الحماية متناسبة مع المخاطر المحددة.

السياسة

يجب أن يقوم المصرف بشكل دائم العمل على توفير آليات عمل وبيئة مادية آمنة بالشكل الكافي لتناسب مستوى الأمان المطلوب للأصول المعلوماتية.

كما يجب أن يوفر المصرف الحماية اللازمة ضد المخاطر البيئية للأصول المعلوماتية بحسب الأهمية.

5 . إدارة العمليات والشبكات والاتصالات

الهدف

الاستخدام الأمثل والآمن لتجهيزات وشبكات ومرافق المصرف. الفصل بين المهام لتقليل مخاطر إساءة الاستخدام الخاطئ أو المتعمد للنظم.

السياسة

يجب أن يقوم المصرف بتوفير آليات ضبط وأمن ذات كفاءة وفعالية لكافة التجهيزات الحاسوبية والشبكات والعمليات عليها.

ويجب أن تكون جميع مكونات الشبكة في المصرف محمية بشكل جيد من أخطار البرامج الضارة التي من الممكن أن تشكل أي تهديد يؤثر على أمن الشبكة.

6 . سياسات المستخدم

الهدف

ضبط وتحسين الاستخدام الآمن للأصول المعلوماتية والتجهيزات الخاصة بالمصرف من قبل الموظف (المستخدم النهائي).

السياسة

يجب أن يقوم المصرف بالطلب من جميع الموظفين (المستخدمين النهائيين) أن يقوموا بالاستخدام الأمثل للأصول المعلوماتية المقدمة لهم بما يتوافق مع أعمال المصرف فقط.

يجب أن يقوم المصرف بتوفير آليات أمن للأصول المعلوماتية المقدمة للمستخدم النهائي بما يتناسب مع فئة هذه الأصول لضمان أن النظام المصرفي محمي من الاختراق.

7 . إدارة التحكم بالنفاذ وصلاحيات الدخول

الهدف

التحكم في الوصول إلى أصول المعلومات للأشخاص المصرح لهم، لضمان توفر المعلومات الصحيحة للشخص المناسب في الوقت المناسب، على أساس متطلبات العمل وضمان أمن المعلومات.

سياسة التحكم بالنفاذ

يجب وضع وتوثيق ومراجعة سياسة التحكم بالنفاذ وفقاً لمتطلبات العمل ومتطلبات أمن المعلومات للوصول إلى الأصول المعلوماتية الخاصة بالمصرف.

يجب أن يقوم المصرف بضبط الوصول إلى المعلومات الالكترونية في الأنظمة والتطبيقات وقواعد البيانات، بالإضافة إلى الدخول إلى المرافق الحاسوبية وخدمات الشبكة والبنية التحتية بحسب متطلبات العمل.

8 . اقتناء النظم وتطويرها وصيانتها

الهدف

التأكد من أنه قد تم تصميم وتطبيق الأمان على كافة نظم المعلومات من أنظمة تشغيل وبنية تحتية ونظام بنكي وتطبيقات خدمية، ويجب تحديد متطلبات الأمن والاتفاق عليها مع بدء تطوير وتنفيذ أي مشروع برمجي وتوثيقها كجزء من العمل البرمجي ككل.

السياسة

يجب على المصرف إدراك وملاحظة أهمية دور أمن المعلومات ضمن دورة حياة تطوير النظام من البداية لكي لا يكون هنالك حاجة لإعادة تأهيل الأمن في النظام.

ويضمن المصرف أن يتم الالتزام بجميع متطلبات الضوابط المتعلقة بالأمن أثناء تصميم ووضع الأنظمة الحاسوبية في الخدمة على شبكة المصرف.

9 . إدارة استمرارية العمل

الهدف

مواجهة الانقطاع في نشاطات العمل وحماية العمليات الحرجة من تأثيرات الفشل الشديد في نظم المعلومات أو الكوارث والتأكد من الاستئناف بوقت مناسب.

السياسة

يجب التأكد من أن المصرف لديه خطة موثّقة لاستمرارية العمل لمواجهة انقطاع أنشطة العمل المصرفية وحماية العمليات الحرجة من آثار الانقطاعات أو الكوارث.

يجب أن يتم اختبار الإجراءات الموثّقة بشكل جيد وبأوقات محددة ومنتظمة وأن تكون محدثة.

10 . سياسة الوصول عن بعد

الهدف العام

تقدم هذه السياسة القواعد المنظمة لعملية الاتصال عن بعد، مع التأكد من أن الاتصالات عن بعد آمنة وتقدم للأشخاص المخولين فقط.

مجال التطبيق

تطبق هذه السياسة على جميع الموظفين المخولين من قبل الإدارة العليا بالوصول إلى الشبكة المصرف عن بعد.

11 . أمن وصول الطرف الثالث

الهدف

حماية الأصول المعلوماتية التي يمكن الوصول إليها من مزودي الخدمات أو جهات الطرف الثالث.

السياسة

يجب أن تكون إمكانية وصول الطرف الثالث إلى أي من الأصول المعلوماتية محدودة وتحت رقابة صارمة ومضبوطة.

ويتم تضمين العقود الموقعة مع الطرف الثالث المسؤوليات والعواقب للوصول غير المصرح به للأصول المعلوماتية الخاصة بالمصرف.

12 . الاستعانة بمصادر خارجية لتطوير تقنية المعلومات

الهدف

ضمان اتخاذ التدابير الأمنية المناسبة من قبل المصرف عند الاستعانة بمصادر خارجية لتقديم الدعم الفني أو تطوير التطبيقات والأنظمة من حيث متابعة نشاطات الأطراف الخارجية بشكل مستمر من أجل جودة المنتج وفعاليته.

السياسة

يجب أن يتم تقييم المخاطر المرتبطة بالاستعانة بمصادر خارجية لخدمات تقنية المعلومات لتطوير التطبيقات وإجراءات الأعمال، وإدارة هذه المخاطر للوصول إلى مستوى مقبول، ويجب وضع الضوابط المناسبة لضمان تلبية متطلبات العمل المصرفي من قبل مزود الخدمة الخارجي.

13 . سياسة مركز البيانات

الهدف

ضمان إدارة مركز البيانات بكفاءة عالية، وحمايته بالشكل الكافي من الدخول غير المصرح، وتهديدات البيئة المحيطة.

السياسة

يجب أن يتمتع مركز البيانات بحماية فيزيائية ومنطقية وبيئية للمعلومات والتجهيزات والبرمجيات والمرافق الموجودة ضمنه، ويجب اتباع عمليات آمنة في إدارة ومراقبة توزيع المخدمات وتجهيزات الشبكة ضمن مركز البيانات.

14 . سياسة الوصول إلى شبكة الانترنت

الهدف

ضمان وصول آمن وملائم للتطبيقات والخدمات الالكترونية إلى شبكة الانترنت، وتوفير بيئة وتجهيزات آمنة ومراقبة لوصول المستخدمين من داخل المصرف أو خارجه إلى شبكة الانترنت.

السياسة

يجب أن يتم فصل شبكة المصرف الداخلية المتصلة مع النظام المصرفي عن شبكة الانترنت باستخدام تجهيزات وتقنيات وضوابط وتدابير مناسبة.

كما يجب أن تتم مراقبة الوصول إلى المواقع عن طريق سجل الوصول في حال استدعت طبيعة العمل الوصول إلى جميع مواقع الانترنت.

15 . سياسة إدارة الاستثناءات

الهدف

توفر هذه السياسة ضماناً للعمليات المصرفية، وذلك من خلال تضمين ضوابط أمنية مكملة في حال حدوث طوارئ خلال مرحلة العمل.

السياسة

الاستثناءات هي حالات خاصة تحيد عن السلوك الطبيعي في المصرف. وتحتاج إلى معالجة وعناية خاصة. حيث يجب توثيق هذه الاستثناءات، واعتمادها من قبل الإدارة، ويجب وضع هذه الضوابط قيد التنفيذ لإدارة المخاطر الناشئة عن عدم إدراجها سابقاً في سياسة أمن المعلومات.

16 . سياسة الأمن السيبراني

الهدف

توفر هذه السياسة التوجيهات اللازمة لأصحاب العمل والمعنيين بمعالجة القضايا المتعلقة بالجرائم المعلوماتية والهجمات الرقمية وأعمال قراصنة الحاسوب التخريبية.

السياسة

تواجه مرافق المصرف مستوى معين من المخاطر المرتبطة بأنواع مختلفة من التهديدات. قد تكون هذه التهديدات ناتجة عن أحداث طبيعية و/أو حوادث وأفعال جرمية متعمدة للتسبب بالضرر. بغض النظر عن طبيعة التهديد يتحمل أصحاب العمل مسؤولية الحد من المخاطر الناتجة عن هذه التهديدات و معالجتها إلى أقصى حد ممكن.

17. سياسة حماية أنظمة الدفع الإلكتروني

الهدف العام

الغرض من هذه السياسة هو حماية سرية، سلامة، وتوافر البيانات من خلال حماية المعلومات الحساسة من الوصول غير المصرح به إليها وحذفها أو التعديل عليها وضمان توافر المعلومات عند الحاجة لها وضمان استمرارية الخدمة.

مجال التطبيق

تطبق هذه السياسة على عملاء المصرف والموردين والموظفين العاملين في المصرف.

18 . سياسة الخصوصية وحماية البيانات

الهدف

ضمان أن البيانات الشخصية التي يتم جمعها ومعالجتها من خلال النظام المصرفي تتم إدارتها وفقاً لقواعد الخصوصية وأمن وحماية البيانات.

السياسة

يجب أن يضمن المصرف أمان وخصوصية وسرية أي بيانات شخصية هامة، أو المعلومات التي يتم جمعها واستلامها وامتلاكها وتخزينها أو التعامل معها.

19 . سياسة الوصول إلى ملفات السجلات والاحتفاظ بها

هدف السياسة

نظرا لحاجة المصرف إلى الحفاظ على الأنظمة الرقمية بشكل جيد وحماية البيانات التي تحتفظ بها هذه الأنظمة، أصبحت إدارة وحوكمة الوصول إلى السجلات والاحتفاظ بها أمرا ضروريا للحفاظ عليها وعلى أمانها ولسهولة الوصول إليها عند الحاجة من أجل تحقيق أهداف العمل وتطبيق مبدأ المحاسبة.

السياسة

يجب الاحتفاظ بملفات السجلات التي يتم إنشاؤها بواسطة أنظمة البنك والخدمات الرقمية وتخزينها، يجب أن تكون جميع الأنظمة المصرفية والخدمات الرقمية قادرة على تسجيل مستوى مقبول من السجلات لتلبية متطلبات الأعمال والامتثال واستكشاف الأخطاء وإصلاحها وتلبية متطلبات أمن المعلومات.

20 . الامتثال وإدارة الحوادث الأمنية

الهدف

تجنب أي مخالفة أو انتهاك للقانون الجنائي أو المدني، أو القوانين والتشريعات والقرارات والتعاميم من الجهات الرقابية، أو الالتزامات التعاقدية والتنظيمية، بالإضافة إلى المتطلبات المنصوص عليها في سياسة أمن المعلومات.

السياسة

يجب أن يضمن المصرف التزامه بالقوانين والتشريعات والأنظمة النافذة في الجمهورية العربية السورية وقرارات المصرف المركزي وتعاميم مجلس النقد والتسليف وتوجيهات مفوضية الحكومة لدى المصارف، والمتطلبات التعاقدية فيما يخص الأصول المعلوماتية ومرافق معالجة وتخزين البيانات والمعلومات الناتجة عنها.

21. سياسة تقوية النظام

الهدف العام

تقوية النظام هو إجراء أمني فعال للغاية حيث يحمي منظومة التشغيل، بغض النظر عمّا إذا كان نظاماً مادياً أو افتراضياً، كما أنه يجعل البنية التحتية والأنظمة والتطبيقات مثل برامج المكتب والمتصفحات أكثر أماناً - على سبيل المثال: ضد سرقة البيانات.

مجال التطبيق

تطبق هذه السياسة على جميع التطبيقات والأنظمة والبنية التحتية والبرامج الثابتة ومجالات أخرى في منظومة المصرف.