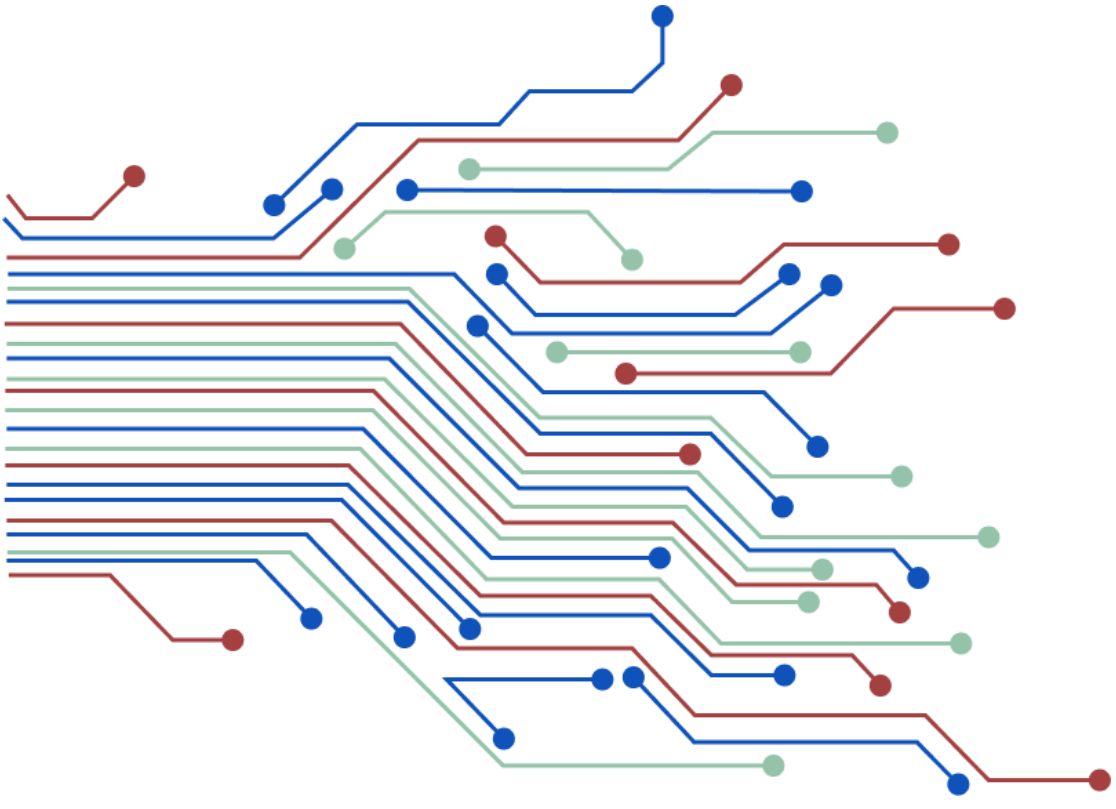
فريق الاستجابة للحوادث
السيبرانية للقطاع المالي
والمصرفي
Jo-FinCERT

RFC 2350

وحدة الاستجابة للحوادث السيبرانية للقطاع المالي

النسخة الاولى



١. معلومات الوثيقة

تعرِّف هذه الوثيقة بفريق وحدة الاستجابة للحوادث السيبرانية وفقًا لـ**RFC 2350** ، وتقدم معلومات أساسية عنه، تشمل قنوات الاتّصال الخاصة بالفريق، وأدواره، والمسؤوليات الخاصة به.

١,١ تاريخ آخر تحديث

تم إصدار النسخة الأولى في يناير ٢٠٢٤.

١,٢ قائمة توزيع التنبيهات

لا توجد قائمة لتوزيع التنبيهات.

١,٣ أماكن تواجد الوثيقة

تتوفر النسخة الحالية والأحدث من هذه الوثيقة على موقع البنك المركزي الأردني ضمن تبويب**Jo- FinCERT** ، العنوان الإلكتروني:

Https://www.cbj.gov.jo/Pages/viewpage.aspx?Pageid=1480

١,٤ مصادقة الوثيقة

تم توقيع هذه الوثيقة بمفتاح PGP الخاص بوحدة الإستجابة للحوادث السيبرانية، يمكن الوصول إلى التوقيع ضمن تبويب **Jo-FinCERT** الموجود على الموقع الخاص بالبنك المركزي الأردني.

العنوان الإلكتروني الخاص بالتوقيع هو:

Https://www.cbj.gov.jo/Pages/viewpage.aspx?Pageid=1480

١,٥ عنوان تعريف الوثيقة

عنوان الوثيقة: "Jo-FinCERT-RFC2350-EN_v1-0"

النسخة: وثيقة ١,٠

التاريخ: يناير - ٢٠٢٤

تاريخ الانتهاء: تبقى هذه الوثيقة قائمة إلى حين إصدار نسخة جديدة منها.

٢. معلومات الاتصال

٢,١ اسم الفريق

الاسم الكامل: فريق الإستجابة لحوادث الأمن السيبراني للقطاع المالي والمصرفي.

الاسم المختصر: Jo-FinCERT

٢,٢. العنوان

الأردن - عمّان - شارع الملك الحسين ٣٧ - ١١١١٨

٢,٣. المنطقة الزمنية

المنطقة الزمنية للملكة الأردنية الهاشمية (GMT +3)

٢,٤. رقم الهاتف

٠٠٩٦٢٦٤٦٣٠٣٠١ / الرقم الفرعي ٤٩٧٨

٢,٥. رقم الفاكس

٠٠٩٦٢٦٤٦١٣٣٠٧

٢,٦. وسائل الاتصال الأخرى

لا يوجد.

٢,٧. عنوان البريد الالكتروني

في حال وجود أي معلومات أو بلاغات عن حوادث أمنية أو تهديدات سيبرانية تستهدف المؤسسات المالية، يرجى الإبلاغ عنها عبر البريد الإلكتروني التالي:
Fincert@cbj.gov.jo

المفاتيح العامة ومعلومات التشفير، المفتاح متاح على:

Https://www.cbj.gov.jo/Pages/viewpage.aspx?Pageid=1480

٢,٨. أعضاء الفريق

يتكون فريق الإستجابة من خبراء في الأمن السيبراني ومحللي التهديدات السيبرانية، المدير التنفيذي للوحدة هو المهندس إبراهيم الشافعي.

٢,٩. نقاط تواصل العملاء

الوسيلة الموصى بها للإبلاغ عن أي حدث هي عبر البريد الإلكتروني التالي:

Fincert@cbj.gov.jo.

فريق الإستجابة للحوادث السيبرانية متاح للإجابة على الاستفسارات والمساعدة ضمن ساعات العمل من خلال البريد الالكتروني التالي : Fincert@cbj.gov.jo.

ساعات العمل (من الأحد إلى الخميس من السّاعة ٨ صباحاً الى ٤ مساءً بتوقيت الأردن (GMT +3))، باستثناء العطل الرسميّة والأعياد الوطنية.

للحالات المستعجلة أو الطارئة، يجب الإبلاغ عن الحادث باستخدام صيغة **[حالة طارئة]** في عنوان البريد الإلكتروني.

في حالة الاتصالات الواردة خارج نطاق ساعات العمل، يقوم ضابط الارتباط بتقييم الاتصال وطلب تدخل فريق الاستجابة إن استدعى الأمر ذلك.

٣. الميثاق

٣,١ المهمة

فريق وحدة الاستجابة هو فريق استجابة لحوادث الأمن السيبراني للقطاع المالي والمصرفي.

تتولى هذه الوحدة مسؤولية جميع الأنشطة السيبرانية والاستجابة للحوادث السيبرانية. تتمثل مهمة الفريق في دعم وحماية المؤسسات المالية والمصرفية، وأعمالها، ومصالحها، وسمعتها من أي نوع من الهجمات السيبرانية التي من شأنها إعاقتها أو إلحاق الضرر بها.

تتكون أعمال وأنشطة وحدة الاستجابة للحوادث السيبرانية من المراقبة الأمنية السيبرانية، والأنشطة الاستباقية من خلال مشاركة معلومات التهديدات السيبرانية، والوقاية، والكشف، والاستجابة للحوادث والتهديدات.

تُقدم وحدة الاستجابة الدعم للمؤسسات المالية والمصرفية من خلال:

- تعزيز قدرة القطاع المالي والمصرفي الأردني على مواجهة المخاطر الإلكترونية.
- تعزيز قدرة القطاع المالي والمصرفي على اكتشاف الحوادث السيبرانية والتصدي لها.
- زيادة قدرة القطاع المالي والمصرفي على الحصول على معلومات استخباراتية جنائية رقمية حول المخاطر السيبرانية التي قد يتعرض لها القطاع.
- رفع كفاءة العاملين في القطاع المالي والمصرفي ومستوى الوعي والثقافة بالمخاطر السيبرانية.

٣,٢ نطاق العمل

فريق وحدة الاستجابة للحوادث السيبرانية هو فريق استجابة لحوادث الأمن السيبراني الخاصة بالقطاع، ويشمل نطاق عمله مؤسسات القطاع المالي والمصرفي في الأردن، بما في ذلك البنوك، وشركات الصرافة، وشركات الدفع

وشـركات التأمين، وشـركات التمويل التي تخضـع لرقابة وإشـراف البنك المركزي الأردني.

٣,٣. الشراكات

تتبع وحدة الاسـتجابة للحوادث السـيبرانية للبنك المركزي الأردني، وتعد الوحدة عضـواً في مختلف فرق الاسـتجابة لحوادث الأمن السـيبراني الإقليمية والعالمية، وفقًا للاحتياجات والمعلومات المتبادلة ومبادئ التعاون التي تتماشـى مع مهمتها وقيمتها.

٣,٤. السلطة

تعمل الوحدة تحت سلطة محافظ البنك المركزي الأردني.

٤. السياسات

٤,١ أنواع الحوادث ومستوى الدعم

تمتلك الوحدة سـلطة التنسـيق والإدارة والتعامل والاسـتجابة لجميع أنواع التهديدات السـيبرانية، والهجمات الإلكترونية، وحوادث الأمن السـيبراني التي تحدث أو تهدد بحدوثها، والتي من شـأنها الإضـرار بالأعمال، والمصـالح، والسـمعة لأيّ مؤسسة مالية خاضعة لإشراف ورقابة البنك المركزي الأردني.

يتم تقديم خدمات الوحدة على مراحل، وفقًا لنوع، وخطورة، والتأثير المحتمل للحوادث الأمنية، كما يتم تقديم مستوى الدعم من الوحدة بناءً على شدة الحدث أو الحادث الأمني، وتأثيره المحتمل أو الفعلي والموارد المتاحة في ذلك الوقت.

٤,٢. التعاون والتفاعل والكشف عن المعلومات

تُصـنف الوحدة البيانات والمعلومات حسـب نوعها ودرجة حسـاسـيتها، لتحديد مسـتوى التدابير الأمنية المطابقة، والحد من مخاطر الكشـف عن المعلومات غير المصرح بها.

-يتم التعامل مع جميع المعلومات الواردة الى وحدة الاسـتجابة للحوادث السيبرانية بسرية، بغض النظر عن أولويتها ومستوى تصنيفها.

-يتم التعامل مع المعلومات التي تتصف بالسرية وتخزينها في بيئة آمنة، باستخدام تقنيات التشفير عند الضرورة.

-تتبادل الوحدة المعلومات مع مجتمع CSIRT العالمي لزيادة الأمان وتسهيل مشاركة المعلومات باستخدام بروتوكول إشارة المرور(TLP) .

٤,٣. التواصل والمصادقة

الطريقة الأفضل للتواصل هي عبر البريد الإلكتروني، إذا كان المحتوى حساسًا أو يتطلب المصادقة، يتم استخدام مفتاح PGP الخاص بوحدة الاستجابة للحوادث السيبرانية للتوقيع. يجب تشفير جميع الاتصالات الحسّاسة الموجهة إلى الوحدة باستخدام مفتاح PGP الخاص بالفريق.

٥. الخدمات

٥,١. التنبيهات والتحذيرات

٥,٢. الاستجابة للحوادث

٥,٣. اختبار الاختراق وتقييم الثغرات الأمنية

٥,٤. تقارير استخبارات التهديد

٥,٥. عمليات تدقيق وتقييم أمن المعلومات

٥,٦. برامج توعوية

٥,٧. التعليم والتدريب

٦. نماذج الإبلاغ عن الحوادث

للإبلاغ عن حادثة أو ثغرة أمنية لوحدة الاستجابة للحوادث السيبرانية، يرجى استخدام البريد الإلكتروني المدرج أدناه:

(Fincert@cbj.gov.jo.)

٧. إخلاء مسؤولية

لا تتحمل وحدة الاستجابة للحوادث السيبرانية أي مسؤولية عن أي أضرار قد تنجم عن استخدام المعلومات التي تقدمها.