الدليل الاسترشادي للتعاون في مجال الأمن السيبراني

إطار تنظيمي لتعزيز العمل المشترك
وتبادل المعلومات بين الهيئات الأعضاء

الأمانة العامة لاتحاد هيئات الأوراق المالية العربية
يونيو 2026
دبي / الإمارات العربية المتحدة

إتحاد هيئات الأوراق المالية العربية
UNION OF ARAB SECURITIES AUTHORITIES

الدليل الاسترشادي

للتعاون في مجال الأمن السيبراني

الأمانة العامة لاتحاد هيئات الأوراق المالية العربية

دبي/ الإمارات العربية المتحدة

2026

أولاً: الهـــدف

يهدف هذا الدليل إلى تعزيز التعاون بين الأعضاء في مجال الأمن السيبراني لتحقيق ما يلي:

- حماية البنية التحتية لأنظمة الأعضاء من الهجمات الإلكترونية.
- تطوير وتنفيذ استراتيجيات وسياسات فعالة للأمن السيبراني بين الأعضاء.
- تبادل المعرفة والمعلومات بين الأعضاء حول التهديدات الإلكترونية الناشئة وأفضل الممارسات للتخفيف من حدتها.

ثانياً: مجالات التعـــاون

يشمل التعاون في إطار هذا الدليل، على سبيل المثال لا الحصر، المجالات التالية:

- تبادل المعلومات حول التهديدات الإلكترونية والحوادث الأمنية، وأنماط الهجمات، ومؤشرات الاختراق.
- التعاون في مجال بناء القدرات من خلال برامج التدريب وورش العمل المشتركة في مجال الأمن السيبراني.
- تبادل الخبرات حول تطوير وتنفيذ معايير الأمن السيبراني وأطر الحوكمة ذات الصلة.
- التنسيق في حالات الاستجابة للحوادث الإلكترونية التي قد تؤثر على أكثر من سوق.
- التعاون في رفع الوعي بالمخاطر الإلكترونية بين المؤسسات المالية والمستثمرين

ثالثاً: تبادل المعلومـات والمسـاعدة

- يلتزم الأعضاء، في حدود ما تسمح به قوانينهم وأنظمتهم الداخلية، بتقديم المساعدة الفنية والمعلوماتية في مجال الأمن السيبراني بناء على طلب خطي من أي عضو.
- تخضع جميع المعلومات المتبادلة بموجب هذا الدليل لأحكام السرية المنصوص عليها في المادة السابعة من مذكرة التفاهم.
- يلتزم الأعضاء، عند تبادل المعلومات المتعلقة بالحوادث أو التهديدات السيبرانية، بمراعاة التشريعات والأنظمة الوطنية النافذة الخاصة بحماية البيانات والمعطيات الشخصية، واتخاذ التدابير اللازمة لضمان عدم الكشف عن البيانات

الشخصية أو معالجتها أو مشاركتها إلا بالقدر الضروري لتحقيق أغراض التعاون المنصوص عليها في هذا الدليل ووفقاً للأطر القانونية المعمول بها لدى كل عضو.

- **يجب مراعاة الأمور الوارد ذكرها أدناه لدى تبادل المعلومات:**

1. توحيد نماذج طلب المعلومات.
   a. طبيعة الواقعة المسببة لطلب المعلومات.
   b. الغرض الرئيسي لطلب المعلومات.
   c. المعلومات والوثائق المطلوبة بشكل دقيق.
   d. الجهات المشتركة في الواقعة.
   e. الإطار الزمني المطلوب.
2. وضع إطار زمني للرد على طلبات المعلومات سواء بالتزويد بالمعلومات المطلوبة أو الاعتذار عن التزويد بها مع بيان الأسباب. (مثلاً مدة أقصاها عشرة أيام عمل، كما يمكن تمييز الحالات التي تحتاج للرد العاجل خلال 24 ساعة مثلاً).
3. توجيه الطلبات حصراً عبر القنوات الرسمية المحددة في الملحق /2/ من مذكرة التفاهم.
4. يمكن الطلب عبر الهاتف أو الفاكس في الحالات الطارئة وفي هذا الإطار يتوجب:
   - تسجيل المكالمات الهاتفية.
   - تأكيد الطلب بالوثائق الرسمية خلال 48 ساعة.
5. من الضروري أن يتم تزويد المعلومات بشكل مشفّر، ويجب تحديد الحد الأدنى من نوع التشفير الواجب اتباعه.
6. يجوز للأعضاء تبادل المؤشرات التقنية للتهديدات السيبرانية (Indicators of Compromise – IOC) وغيرها من المعلومات الفنية ذات الصلة، بما في ذلك عناوين بروتوكول الإنترنت الضارة (Malicious IP Addresses)، وأسماء النطاقات المشبوهة، وأنماط البرمجيات الخبيثة، وأساليب الهجوم المكتشفة، وذلك بهدف تعزيز قدرات الكشف المبكر والاستجابة الفعّالة للحوادث السيبرانية والحد من انتشارها.
7. أي استخدام إضافي للمعلومات خارج الغرض الرئيسي الموضح في الطلب الأولي يجب أن يتم بعد الحصول على موافقة خطية خاصّة.
8. إعداد تقارير دورية عن نتائج التعاون وتبادل المعلومات.

رابــعاً: قنــوات الاتصــال

1- يتم تعيين نقطة اتصال مختصة بالأمن السيبراني من كل عضو، يتم إدراج تفاصيلها في وثيقة منفصلة يوافق عليها جميع الأعضاء، يتم التواصل بشأن الطلبات العاجلة عبر القنوات المتفق عليها.

خامســاً: آلية الإشعار السريع

1- يلتزم العضو الذي يتعرض لحادثة أو تهديد إلكتروني ذي تأثير جوهري أو محتمل على استقرار السوق المالية أو سلامة البنية التحتية التقنية أو أمن المعلومات، بإشعار الأعضاء الآخرين في أقرب وقت ممكن عبر نقاط الاتصال المعتمدة.

2- يجب أن يتضمن الإشعار الأولي، قدر الإمكان، المعلومات الأساسية التالية:

a) وصفاً مختصراً للحادثة أو التهديد الإلكتروني.

b) تاريخ ووقت اكتشاف الحادثة.

c) الأنظمة أو الخدمات المتأثرة.

d) مستوى التأثير المتوقع أو الفعلي.

e) الإجراءات الأولية المتخذة لاحتواء الحادثة.

f) أي مؤشرات اختراق أو معلومات فنية يمكن أن تساعد الأعضاء الآخرين في اتخاذ التدابير الوقائية المناسبة.

3- يتم إرسال الإشعار الأولي خلال مدة لا تتجاوز (24) ساعة من اكتشاف الحادثة أو التهديد، متى سمحت الظروف بذلك، على أن يتم استكمال المعلومات التفصيلية لاحقاً عند توفرها.

4- يتعاون الأعضاء في تقييم المخاطر المحتملة للحوادث المبلَّغ عنها واتخاذ الإجراءات الوقائية اللازمة للحد من آثارها وانتشارها.

5- في حال كانت الحادثة ذات طبيعة عابرة للحدود أو يحتمل أن تؤثر على أكثر من سوق مالية، يتم تعزيز التنسيق بين الأعضاء وتبادل المستجدات بصورة دورية حتى انتهاء الحادثة واحتواء آثارها.

6- يجوز للأعضاء، عند انتهاء الحادثة، تبادل تقرير ختامي يتضمن الدروس المستفادة وأفضل الممارسات والإجراءات التصحيحية المتخذة، بما يسهم في تعزيز الجاهزية السيبرانية الجماعية للأعضاء.

سادساً: الاجتماعات والتشاور

- يعقد الأعضاء اجتماعات دورية (على الأقل مرة سنوياً) للتشاور حول مستجدات التهديدات الإلكترونية واستراتيجيات المواجهة ويمكن تنظيم هذه الاجتماعات عن بعد.
- يتم تنظيم برامج تدريبية مشتركة لموظفي الأمن السيبراني في الهيئات الأعضاء.
- يتم إعداد تقارير دورية حول مدى تبني الدول الأعضاء للمتطلبات الواردة في هذا الدليل.

سابعاً: التدريب وبناء القدرات

يقوم الأعضاء فيما بينهم بالتباحث لإعداد خارطة طريق بهدف رفع مستويات التنسيق لمواجهة مخاطر السيبرانية وتعزيز بناء القدرات الذاتية لدى الأعضاء وفي هذا المجال يتوجب العمل على:

a) إعداد خطة تدريبية سنوية تشمل ورش عمل ومؤتمرات متخصصة.

b) تبادل الخبراء بين الدول الأعضاء لتدريب الموظفين.

c) إنشاء مكتبة رقمية للبحوث والدراسات وأفضل الممارسات.

d) عقد جلسات تشاورية لمناقشة التحديات وتبادل الحلول.

e) إعداد مواد توعوية موحّدة باللغتين العربية والإنكليزية، يتم نشرها على جميع المواقع الالكترونية للأعضاء.

f) إنشاء منصة إلكترونية موحّدة لتثقيف وتوعية المستثمرين.

g) تنظيم تمارين محاكاة مشتركة للحوادث السيبرانية بشكل دوري، بهدف اختبار جاهزية الأعضاء ورفع مستوى التنسيق خلال الأزمات.

ملحق أعضاء فريق العمل

جاء إعداد هذا الدليل بجهود مخلصة من فريق العمل الذي ساهم بخبراته ومعرفته في بلورته وإخراجه بصورته الحالية.

هيئة الأوراق والأسواق المالية السورية - سوريا	**نيفين سعيد** – مدير الدراسات والأبحاث والتوعية **أحمد القصار** – مدير الرقابة والتفتيش
الهيئة العامة للرقابة المالية - مصر	**أميرة فوزي** – مهندس أمن الشبكات
هيئة سوق رأس المال الفلسطينية - فلسطين	**د. بشار أبو زعرور** – مدير عام الإدارة العامة لخدمات التمويل الرقمي والابتكار
هيئة السوق المالية - السعودية	**وليد الثبيتي** – مدير إدارة الأمن السيبراني