

قرار رقم (٨٠٠٥) لسنة ٢٠١٣

بتاريخ ١٤/ ١٢/ ٢٠١٣

رئيس الهيئة العامة للرقابة المالية

بعد الاطلاع على القانون رقم ٩٥ لسنة ١٩٩٢ بإصدار قانون سوق رأس المال ولائحته التنفيذية ؛
وعلى القانون رقم ٩٣ لسنة ٢٠٠٠ بإصدار قانون الإيداع والقيود المركزي للأوراق المالية ولائحته التنفيذية،
وعلى القانون رقم ١٥ لسنة ٢٠٠٤ بإصدار قانون التوقيع الإلكتروني ،
وعلى القانون رقم ١٠ لسنة ٢٠٠٩ بتنظيم الرقابة على الأسواق والأدوات المالية غير المصرفية،
وعلى قرار رئيس الجمهورية رقم ١٩٢ لسنة ٢٠٠٩ بإصدار النظام الأساسي للهيئة العامة للرقابة المالية،
وعلى قرارات مجلس إدارة الهيئة أرقام ٤٩، ٥٠ لسنة ٢٠٠٦ و ٦٨ لسنة ٢٠١٢،

وعلى ما أقره مجلس إدارة الهيئة بجلسته الملغاة بتاريخ ٢٥/١١/٢٠١٣، بتفويض رئيس الهيئة في إصدار قرار موحد يحدد تنظيم متطلبات البنية التكنولوجية ونظم تأمين المعلومات اللازم توافرها لدى شركات السمسرة في الأوراق المالية.

تسرد

مادة (١)

تلغى البنود أرقام ١، ٢، ٣ من المادة الثالثة من قرار مجلس إدارة الهيئة رقم ٤٩ لسنة ٢٠٠٦ والملحقين رقمي ٣، ٤ من ذات القرار، وتلغى قرار مجلس إدارة الهيئة رقم ٥٠ لسنة ٢٠٠٦، وتلغى البنود التي تخص البنية التكنولوجية في الملحق رقم (١) من قرار مجلس إدارة الهيئة رقم ٦٨ لسنة ٢٠١٢، ويلغى الملحق رقم (٢) من ذات القرار.

مادة (٢)

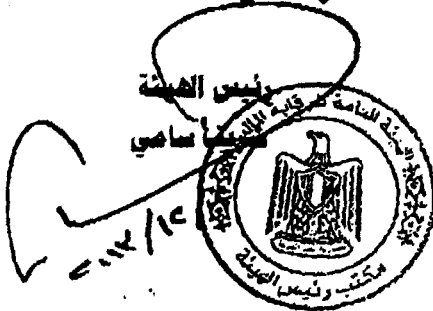
تلتزم شركات السمسرة بمتطلبات البنية التكنولوجية ونظم تأمين المعلومات الملحق بهذا القرار كحد أدنى للبنية التكنولوجية لشركات السمسرة.

مادة (٣)

تلتزم شركات السمسرة التي تعمل بنظام التداول الإلكتروني بتوفير أوضاعها طبقاً لأحكام هذه القرار وملحقه في موعد غايته ٢٠١٣/١٢/٣١.

مادة (٤)

يُعلن هذا القرار ومرفقاته على الموقع الإلكتروني للهيئة والبورصة، وينشر في الوقائع المصرية ويعمل به من اليوم التالي لنشره، ويلغى كل حكم يخالف أحكامه وملحقه.



ملحق القرار رقم ١١٦ لسنة ٢٠١٣ بشأن البنية التكنولوجية
لشركات السمسرة ونظم تأمين المعلومات

المصطلحات والتعريفات المستخدمة

يقصد - في تطبيق أحكام الملحق المرفق - بالكلمات والعبارات التالية المعاني المبينة قرين كل منهم وإنما وردت بهذا الملحق .

الهيئة العامة للمراقبة المالية	الهيئة
البورصة المصرية	البورصة
شركة مصر للمقاصة والإيداع والقيود المركزي	شركة المقاصة
شركة السمسرة في الأوراق المالية	الشركة
النظام المستخدم في تبادل الرسائل المالية على مستوى سوق المال بين الجهات المختلفة.	بروتوكول تبادل المعلومات المالية Financial Information exchange (FIEX)
المقر الاحتياطي لشركة السمسرة والذي تستخدمه في تنفيذ أنشطتها في حالة تعرض المقر الرئيسي لها لكارثة.	مقر احتياطي للطوارئ Disaster Recovery Site (DR)
الحاسبات الخادمة التي تثبت عليها أنظمة التشغيل والتطبيقات والبرمجيات المستخدمة لدى شركات السمسرة.	خوادم مركزية (Main Servers)
نمط من أنماط تشبيك أجهزة البنية التحتية للمعلومات ويضم ذلك نظامين متطابقين على الأقل بحيث يعمل احدهما كنظام أساسي Active والأخر يعمل كنظام احتياطي Passive ليحل محل النظام الأساسي في حالة عدم توفره لأي سبب.	Active-Passive
نمط من أنماط تشبيك أجهزة البنية التحتية للمعلومات ويضم ذلك نظامين متطابقين على الأقل بحيث يعمل النظامين كنظام واحد لتوزيع عبء التشغيل على أكثر من نظام.	Active -Active
قياس سرعة نقل البيانات خلال شبكات و خطوط الاتصال.	كيلو بت في الثانية (Kb/s)
قياس سرعة نقل البيانات خلال شبكات و خطوط الاتصال وتساوي ١٠٠٠ kb/s.	ميغا بت في الثانية (Mb/s)



نظام يعمل على العزل بين شبكتين من نوع واحد أو عدة أنواع والسماح بتدفق المعلومات بين الشبكات عبر مجموعة من قوائم التحكم في الدخول على الأقل على مستوى الشبكة.	الجدار الناري (Firewall)
تحتوي على سجلات محفوظة تشتمل على كل ما يتعلق بنشاط معين يتم من خلال أي مكون في البنية الأساسية للتكنولوجيا المعلومات، ويكون مسجلا بالوقت والتاريخ (System Logs, Security Logs, and Application Logs).	سجلات الأنشطة (Logging Activities)
قدرة النظام على التعافي من الأخطاء المحتملة الوقوع والتي تمنعه من العمل بصورة طبيعية.	Fault-Tolerant
مدى جاهزية النظام للتشغيل في حالة تعرضه لظروف تمنعه من العمل بصورة طبيعية.	Hot-Standby
تعني أن يتكون النظام الواحد من عدة أجزاء متطابقة (مثال: خوادم متطابقة) تعمل كلها على أنها كيان واحد يؤدي الوظيفة المطلوبة.	Cluster
البرنامج المسئول عن حماية أجهزة الحاسبات من الفيروسات والعناصر الضارة المحتمل التعرض لها.	Antivirus/Antimalware
مدى جاهزية النظام للتشغيل بدون توقف في حال تعرضه لظروف تمنعه من العمل بصورة طبيعية.	High Availability (HA)
هي الشبكات التي لا تتطلب وجود خطوط اتصال ثابتة بين جميع النقاط	الشبكات السحابية (Cloud Network)



الفرع الأول

متطلبات البنية التكنولوجية ونظم تأمين المعلومات

لدى شركات السمسرة في الأوراق المالية

تسري أحكام هذا الفرع على كافة شركات السمسرة في الأوراق المالية، وذلك على النحو التالي:

بند (١): وسائل الاتصال

على الشركة توفير البنية الأساسية اللازمة للربط الآلي مع البورصة وشركة المقاصة طبقاً للمواصفات الفنية التي تضعها البورصة وشركة المقاصة ، ويكون ذلك من خلال خط اتصال أساسي وخط اتصال احتياطي لكل منهما ، ويمكن أن يعمل الخيطان بأسلوب Active-Active أو Active-Passive بحيث لا تقل السعة الفعالة للاتصال عن 1Mb/s (واحد ميجابت في الثانية) ، كما يجب أن يتوفر خط اتصال بين كل شركة سمسرة والمقر الاحتياطي لها بحيث لا تقل سعته عن ١٢ kb/s . كما يمكن استخدام أية تقنية اتصالات أخرى تؤدي ذات الغرض مثل الاتصال السحابي (cloud network) عن طريق أي مقدم خدمة.

بند (٢): الخوادم المركزية وأنظمة التشغيل

تلتزم الشركة بتوفير أجهزة الخوادم اللازمة لتشغيل الخدمات المختلفة والحاسبات الخادمة التالية :-

- حاسبات تعمل كخوادم للتطبيقات Application Servers.
- حاسبات تعمل كخوادم لقواعد البيانات Database Servers.
- حاسبات تعمل كخادم مستقل لخدمة تبادل المعلومات المالية FIX Server.

وتكون مواصفات الأجهزة مناسبة لتشغيل تلك الخدمات، ويجب مراعاة التالي:

- توفير نظم تشغيل حديثة ومرخصة تعمل على الخوادم.
- توفير الأنظمة و التطبيقات و البرمجيات - المرخصة - اللازمة لتشغيل الخدمات المختلفة.
- يجب تجهيز أجهزة الخوادم بحيث تحقق المستوى المطلوب من العمل الدائم بدون توقف (High Availability).

بند (٣): حماية وتأمين المعلومات

تلتزم الشركة بما يلي:

- تركيب نظام جدار ناري Firewall لتأمين جميع شبكات الاتصال داخل الشركة وبين الشركة والجهات الأخرى ويجوز أن يكون ذلك من خلال مخرج متعددة للنس الـ Firewall.
- توفير نظم حماية للشبكة وفقاً للخدمات المطلوب حمايتها، على سبيل المثال: نظام منع الاختراق

Intrusion Prevention System



٤٦٠٧٦

- إجراء الصيانة الدورية لأجهزة تأمين الشبكات مع مراعاة قواعد الضبط المناسبة لها Configuration Rules، و تحديثها بصفة مستمرة.
- تزويد جميع أجهزة الحاسب المتصلة بشبكة الشركة (حاسبات مكتبية ، محمولة ، خوادم) ببرامج محدثة لمكافحة الفيروسات والبرمجيات الضارة (Antivirus/Antimalware).
- عمل التحديث الدوري لأنظمة التشغيل والتطبيقات والبرمجيات المختلفة.
- وضع نظام للمراقبة و التحكم في الدخول و الخروج لغرفة الخوادم Server /Data Room Center من الداخل والخارج بالوسائل المتاحة و المناسبة.
- الفصل المادي بين أنظمة الخدمات المختلفة وفقاً للمستوى الأمني لها (في حالة استخدام البيئة الافتراضية Virtualization).
- إبلاغ الهيئة عند حدوث اختراقات أمنية Security Incident تحدث على مستوى البنية الأساسية للمعلومات والأنظمة العاملة عليها.

بند (٤): ضبط التوقيت

- تلتزم الشركة بضبط التوقيت Time Synchronization لجميع أنظمة المعلومات والأجهزة المثبت عليها هذه الأنظمة وجميع أنظمة الشبكات والتأمين على توقيت واحد يكون مماثلاً لتوقيت أنظمة البورصة.

بند (٥): التسجيل والاحتفاظ بالسجلات

- تلتزم الشركة بإتاحة تسجيل جميع الأنشطة Logging Activities التي تحدث على جميع الأجهزة والأنظمة (System Logs, Security Logs, and Application Logs) وما تعتمد عليه من أجهزة مساعدة (حاسبات، أجهزة شبكات، أجهزة تأمين معلومات) لمدة لا تقل عن خمس سنوات من تاريخ حدوث النشاط.

بند (٦): المقر الاحتياطي للطوارئ

- تلتزم الشركة بتوفير مقر احتياطي للطوارئ Disaster Recovery Site يتوافر به أجهزة الخوادم اللازمة لتشغيل التطبيقات التي تعمل بالمقر الرئيسي مع الاحتفاظ بوجود نسخة من البيانات محدثة في نهاية اليوم - بحد أقصى - من خلال خط اتصال آمن، مع ضمان حماية هذه البيانات والحفاظ على سريتها.
- يخضع المقر الاحتياطي للطوارئ لنقص ضوابط التشغيل والتأمين بمقر الشركة الرئيسي بحيث يمكن تشغيل الخدمات في المقر الاحتياطي فور توقف العمل في المقر الرئيسي وذلك بعد إخطار الهيئة بذلك.
- في حالة استضافة المقر الاحتياطي للطوارئ، يجب مراعاة جميع الضوابط الخاصة باستضافة خدمات شركات السمسرة (وفقاً لما تصدره الهيئة في هذا الشأن).
- يجب ألا يتم تنفيذ إجراءات نقل المقر الرئيسي أو الاحتياطي إلا بعد الحصول على موافقة الهيئة.



الفرع الثاني

المتطلبات الخاصة بالشركات العاملة بنظام التداول عبر الإنترنت

مع عدم الإخلال بمتطلبات البنية التكنولوجية ونظم تأمين المعلومات السابقة لكافة شركات السمسرة، تسري أحكام هذا الفرع على شركات السمسرة العاملة بنظام التداول عبر الإنترنت (Online trading) على النحو التالي:

بند (٧): خطوط الاتصال بالإنترنت

يجب أن يتوافر خطي اتصال بشبكة الإنترنت أحدهما أساسي والآخر احتياطي ويكون ذلك من خلال خط اتصال أساسي وخط اتصال احتياطي، ويمكن أن يعمل الخطين بأسلوب Active-Active أو Active-Passive بحيث لا تقل السعة الفعلية للاتصال عن IMb/s (واحد ميجابايت في الثانية).

بند (٨): الخوادم المركزية و أنظمة التشغيل

يجب توافر خوادم لتشغيل موقع وتطبيق الشركة الرسمي الخاص بالتداول من خلال الإنترنت .

بند (٩): نظم التحقق من شخصية العميل

يجب إثبات شخصية العميل إلكترونياً باستخدام تقنية التحقق متعدد العوامل (Multi-Factor Authentication) وتكون على الأقل ذات عاملين (Two-Factor Authentication) على أن يكون العامل الأول باستخدام اسم المستخدم وكلمة المرور، ويمكن أن يكون العامل الثاني أحد الوسائل التالية على سبيل المثال:-

- كلمة المرور ذات الاستخدام الواحد (One Time Password).

- شهادة توقيع إلكتروني (Digital Signature Certificate).

- ما يستجد من وسائل التأمين الإلكتروني التي تعتمدها الهيئة.

وكذلك تلتزم الشركة بما يلي:

- تجهيز البنية التكنولوجية الداعمة لتقنيات التحقق (Multi-Factor Authentication).

- تجهيز البنية التكنولوجية الداعمة لتقنية التوقيع الإلكتروني (Digital Signature Certificate)، على أن تكون معتمدة بشهادة من إحدى الجهات المصرح لها من قبل هيئة تنمية صناعة تكنولوجيا المعلومات ITIDA.

- توفر الشركة لعملائها الاشتراك في خاصية التوقيع الإلكتروني خلال ٣ أيام عمل من اليوم التالي لطلبهم الاشتراك في الخاصية وبكلفتها الفعلية.



- يجب أن تسجل جميع عمليات التحقق من العميل - الناجحة و الفاشلة منها - وأن يشمل التسجيل الرقم المميز Unique Session ID، وأن يتم الاحتفاظ بالسجلات لمدة لا تقل عن خمس سنوات، وفي حالة وجود نزاع مع أحد العملاء تلتزم الشركة بالاحتفاظ بكافة الأوامر والسجلات لحين تسوية النزاع أو صدور حكم قضائي نهائي فيه.

بند (١٠): ضوابط خاصة بالتوقيع الإلكتروني

تلتزم الشركة بتوعية عملاء التداول عبر الإنترنت ب إتاحة خاصية التوقيع الإلكتروني وأهميتها على النحو التالي:

- إظهار تنويه على الشاشة الرئيسية لنظام التداول عبر الإنترنت يفيد توافر إمكانية الاشتراك في خاصية التوقيع الإلكتروني لأي عميل يرغب في العمل بها مع التأكيد على كونها من أعلى درجات تأمين العميل وتعاملاته
- تضمين ملحق عقد فتح حساب العميل ذات التنويه المشار إليه أعلاه..

بند (١١): ضوابط نظام التداول عبر الإنترنت

- يجب أن يؤمن الموقع الإلكتروني بشهادة إلكترونية مخصصة للتعريف وتشغيل البيانات Digital Certificate سارية، بحيث تظهر للعملاء عند تصفحهم الموقع الإلكتروني.
- يجب إصدار رقم لا يكرر Unique Session ID، مضافاً إليه ختم التوقيت Time Stamp لكل اتصال Session حال فتح الاتصال عند التحقق من الدخول.
- يجب عدم سماح نظام التداول عبر الإنترنت بدخول العميل إلى حسابه على أكثر من متصفح أو فتح أكثر من اتصال Session في نفس الوقت.
- يجب أن تكون التطبيقات مبنية على أساس التحقق من عمليات الإدخال Field Validation في الحقول الضرورية و مصممة بحيث يتم تشغيل البيانات بشكل كامل.
- يجب أن تحتفظ الشركة لمدة ٥ سنوات على الأقل بالسجلات الكاملة Transactions Logs و التي تشمل جميع عمليات الدخول و الخروج و الأوامر الصادرة من العملاء و غيرها.
- يجب على نظام التداول إلزام العميل بتغيير كلمة المرور الخاصة بحسابه عند الدخول لأول مرة على الحساب بعد إنشاء كلمة المرور الأولى من مشرف النظام أو بعد تغييرها لأي سبب من الأسباب.
- يجب أن يقوم نظام التداول بإخطار العميل آلياً عند تغيير كلمة المرور بنجاح من خلال وسيلة الاتصال المتفق عليها والمذكورة في العقد.
- يجب ألا يسمح نظام التداول باستمرار الاتصال غير الفعال مع عميل الإنترنت (Inactive Session) لمدة تزيد عن ٣٠ دقيقة فيما يخص التعامل على حسابه بإضافة أو تعديل أو حذف أوامر تؤثر في رصيده، ويطلب بعدها النظام من العميل إعادة إدخال كلمة المرور - كحد أدنى- لإعادة الدخول مرة أخرى.
- يجب أن يكون نظام التداول قادراً على إرسال رسالة نصية لصوره أو رسالة بريد الكتروني للعميل لإخطاره على سبيل التأكيد بأي عملية تؤثر في رصيده حسابه، من خلال وسيلة الاتصال المتفق عليها والمذكورة في العقد.

