الهيئة العامة للرقابة المالية

قرار رقم ١٠٠٥ لسنة ٢٠١٣

بتاريخ ٢٠١٣/١٢/٢

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 والقيد المركزى للأوراق المالية ولائحته التنفيذية ؛

وعلى القانون رقم ١٥ لسنة ٢٠٠٤ بإصدار قانون التوقيع الالكترونى ؛

وعلى القانون رقم ١٠ لسنة ٢٠٠٩ بتنظيم الرقابة على الأسواق والأدوات المالية غير المصرفية ؛

وعلى قرار رئيس الجمهورية رقم ١٩٢ لسنة ٢٠٠٩ بإصدار النظام الأساسى للهيئة العامة للرقابة المالية ؛

وعلى قرارات مجلس إدارة الهيئة أرقام ٤٩ ، ٥٠ لسنة ٢٠٠٦ و٦٨ لسنة ٢٠١٢ ؛

وعلى ما أقره مجلس إدارة الهيئة بجلسته المنعقدة بتاريخ ٢٠١٣/١١/٢٥ بتفويض رئيس الهيئة فى إصدار قرار موحد يحدث تنظيم متطلبات البنية التكنولوجية ونظم تأمين المعلومات اللازم توافرها لدى شركات السمسرة فى الأوراق المالية ؛

قـــرر :

مـادة (١)

تُلغى البنود أرقام (١ ، ٢ ، ٣) من المادة الثالثة من قرار مجلس إدارة الهيئة رقم ٤٩ لسنة ٢٠٠٦ والملحقان رقما (٣ ، ٤) من ذات القرار ، ويُلغى قرار مجلس إدارة الهيئة رقم ٥٠ لسنة ٢٠٠٦ ، وتُلغى البنود التى تخص البنية التكنولوجية فى الملحق رقم (١) من قرار مجلس إدارة الهيئة رقم ٦٨ لسنة ٢٠١٢ ، ويُلغى الملحق رقم (٢) من ذات القرار .

مـــادة (٢)

تلتـزم شـركات السـمسـرة بمتطلبـات البنيـة التكنولوجيـة ونظـم تأمـين المعلومـات الملحقة بهذا القرار كحد أدنى للبنية التكنولوجية لشركات السمسرة .

مـــادة (٣)

تلتزم شركات السمسرة التى تعمل بنظام التداول الالكترونى بتوفيـق أوضاعهـا طبقًا لأحكام هذا القرار وملحقه فى موعد غايته ٢٠١٣/١٢/٣١

مـــادة (٤)

يُعلن هذا القـرار ومرفقـاتـه على الموقـع الالكترونـى للهيئـة والبورصـة ، ويُنشـر فى الوقائـع المصريـة ، ويُعمـل بـه من اليوم التالى لنشره ، ويُلغى كل حكم يخالف أحكامه وملحقه .

رئيس الهيئة

شـريف سـامى

ملحق القرار رقم ١٠٠٥ لسنة ٢٠١٣

بشأن البنية التكنولوجية لشركات السمسرة ونظم تأمين المعلومات

المصطلحات والتعريفات المستخدمة

يُقصد - فى تطبيق أحكام الملحق المرفق - بالكلمات والعبارات التالية المعانى المبينة قرين كل منها أينما وردت بهذا الملحق :

الهيئة : الهيئة العامة للرقابة المالية .

البورصة : البورصة المصرية .

شركة المقاصة : شركة مصر للمقاصة والإيداع والقيد المركزى .

الشركة : شركة السمسرة فى الأوراق المالية .

بروتوكول تبادل المعلومات المالية Financial Information exchange (FIX) :

النظام المستخدم فى تبادل الرسائل المالية على مستوى سوق المال بين الجهات المختلفة .

مقر احتياطى للطوارئ Disaster Recovery Site (DR) : المقر الاحتياطى لشركة السمسرة والذى تستخدمه فى تنفيذ أنشطتها فى حالة تعرض المقر الرئيسى لها لكارثة .

خوادم مركزية (Main Servers) : الحاسبات الخادمة التى تثبت عليها أنظمة التشغيل والتطبيقات والبرمجيات المستخدمة لدى شركات السمسرة .

Active - Passive : نمط من أنماط تشبيك أجهزة البنية التحتية للمعلومات ويضم ذلك نظامين متطابقين على الأقل بحيث يعمل أحدهما كنظام أساسى Active والآخر يعمل كنظام احتياطى Passive ليحل محل النظام الأساسى فى حالة عدم توفره لأى سبب .

Active - Active : نمط من أنماط تشبيك أجهزة البنية التحتية للمعلومات ويضم ذلك نظامين متطابقين على الأقل بحيث يعمل النظامان كنظام واحد لتوزيع عبء التشغيل على أكثر من نظام .

كيلو بت فى الثانية (Kb/s) : قياس سرعة نقل البيانات خلال شبكات وخطوط الاتصال .

ميجا بت فى الثانية (Mb/s) : قياس سرعة نقل البيانات خلال شبكات وخطوط الاتصال وتساوى ١٠٠٠ kb/s .

الجدار النارى (Firewall) : نظام يعمل على العزل بين شبكتين من نوع واحد أو عدة أنواع والسماح بتدفق المعلومات بين الشبكات عبر مجموعة من قوائم التحكم فى الدخول على الأقل على مستوى الشبكة .

سجلات الأنشطة (Logging Activities) : تحتوى على سجلات محفوظة تشتمل على كل ما يتعلق بنشاط معين يتم من خلال أى مكون فى البنية الأساسية لتكنولوجيا المعلومات ، ويكون مسجلاً بالوقت والتاريخ (System Loge, Security Logs, and Application Logs) .

Fault - Tolerant : قدرة النظام على التعافى من الأخطاء المحتملة الوقوع والتى تمنعه من العمل بصورة طبيعية .

Hot - Standby : مدى جاهزية النظام للتشغيل فى حالة تعرضه لظروف تمنعه من العمل بصورة طبيعية .

Cluster : تعنى أن يتكون النظام الواحد من عدة أجزاء متطابقة (مثال : خوادم متطابقة) تعامل كلها على أنها كيان واحد يؤدى الوظيفة المطلوبة .

Antivirus/Antimalware : البرنامج المسئول عن حماية أجهزة الحاسبات من الفيروسات والعناصر الضارة المحتمل التعرُض لها .

High Availability (HA) : مدى جاهزية النظام للتشغيل بدون توقف فى حال تعرضه لظروف تمنعه من العمل بصورة طبيعية .

الشبكات السحابية (Cloud Network) : هى الشبكات التى لا تتطلب وجود خطوط اتصال ثابتة بين جميع النقاط .

الفرع الأول

متطلبات البنية التكنولوجية ونظم تأمين المعلومات

لدى شركات السمسرة فى الأوراق المالية

تسرى أحكام هذا الفرع على كافة شركات السمسرة فى الأوراق المالية ، وذلك على النحو التالى :

بند ١ - وسائل الاتصال :

على الشركة توفير البنية الأساسية اللازمة للربط الآتى مع البورصة وشركة المقاصة طبقًا للمواصفات الفنية التى تضعها البورصة وشركة المقاصة ، ويكون ذلك من خلال خط اتصال أساسى وخط اتصال احتياطى لكل منهما ، ويمكن أن يعمل الخطان بأسلوب Active - Active أو Active - Passive بحيث لاتقل السعة الفعالة للاتصال عن IMb/s (واحد ميجابت فى الثانية) ، كما يجب أن يتوفر خط اتصال بين كل شركة سمسرة والمقر الاحتياطى لها بحيث لاتقل سعته عن ٥١٢ kb/s . كما يمكن استخدام أية تقنية اتصالات أخرى تؤدى ذات الغرض مثل الاتصال السحابى (cloud network) عن طريق أى 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 التالى :

توفير نظم تشغيل حديثة ومرخصة تعمل على الخوادم .

توفير الأنظمة والتطبيقات والبرمجيات - 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 يلى :

تركيب نظام جدار نارى Firewall لتأمين جميع شبكات الاتصال داخل الشركة وبين الشركة والجهات الأخرى ويجوز أن يكون ذلك من خلال مخارج متعددة لنفس الـ Firewall .

توفير نظم حماية للشبكة وفقًا للخدمات المطلوب حمايتها ، على سبيل المثال : نظام منع الاختراق Intrusion Prevention System .

إجراء الصيانة الدورية لأجهزة تأمين الشبكات مع مراعاة قواعد الضبط المناسبة لها Configuration Rules ، وتحديثها بصفة مستمرة .

تزويد جميع أجهزة الحاسب المتصلة بشبكة الشركة (حاسبات مكتبية ، محمولة ، خوادم) ببرامج محدثة لمكافحة الفيروسات والبرمجيات الضارة (Antivirus/Antimalware) .

عمل التحديث الدورى لأنظمة التشغيل والتطبيقات والبرمجيات المختلفة .

وضع نظام للمراقبة والتحكم فى الدخول والخروج لغرفة الخوادم Server/Data Room Center من الداخل والخارج بالوسائل المتاحة والمناسبة .

الفصل المادى بين أنظمة الخدمات المختلفة وفقًا للمستوى الأمنى لها (فى 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 التى 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 الاحتياطى للطوارئ :

تلتزم الشركة بتوفير مقر احتياطى للطوارئ Disaster Recovery Site يتوافر به أجهزة الخوادم اللازمة لتشغيل التطبيقات التى تعمل بالمقر الرئيسى مع الاحتفاظ بوجود نسخة من البيانات محدثة فى نهاية اليوم - بحد أقصى - من خلال خط اتصال آمن ، مع ضمان حماية هذه البيانات والحفاظ على سريتها .

يخضع المقر الاحتياطى للطوارئ لنفس ضوابط التشغيل والتأمين بمقر الشركة الرئيسى بحيث يمكن تشغيل الخدمات فى المقر الاحتياطى فور توقف العمل فى المقر الرئيسى وذلك بعد إخطار الهيئة بذلك .

فى حالة استضافة المقر الاحتياطى للطوارئ ، يجب مراعاة جميع الضوابط الخاصة باستضافة خدمات شركات السمسرة (وفقًا لما تصدره الهيئة فى هذا الشأن) .

يجب ألا يتم تنفيذ إجراءات نقل المقر الرئيسى أو الاحتياطى إلا بعد الحصول على موافقة الهيئة .

الفرع الثانى

المتطلبات الخاصة بالشركات العاملة بنظام التداول عبر الإنترنت

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

بند ٧ - خطوط الاتصال بالإنترنت :

يجب أن يتوافر خطا اتصال بشبكة الإنترنت أحدهما أساسى والآخر احتياطى ويكون ذلك من خلال خط اتصال أساسى وخط اتصال احتياطى ، ويمكن أن يعمل الخطان بأسلوب Active - Active أو Active - Passive بحيث لا تقل السعة الفعالة للاتصال عن 1Mb/s (واحد ميجابت فى الثانية) .

بند ٨ - الخوادم المركزية وأنظمة التشغيل :

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

بند ٩ - نظم التحقق من شخصية العميل :

يجب إثبات شخصية العميل الكترونيًا 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 الثانى أحد الوسائل التالية على سبيل المثال :

كلمة المرور ذات الاستخدام الواحد (One Time Password) .

شهادة توقيع إلكترونى (Digital Signature Certificate) .

ما يستجد من وسائل التأمين الإلكترونى التى تعتمدها الهيئة .

وكذلك تلتزم الشركة بما يلى :

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

تجهيز البنية التكنولوجية الداعمة لتقنية التوقيع الإلكترونى (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 فى خاصية التوقيع الإلكترونى خلال ٣ أيام عمل من اليوم التالى لطلبهم الاشتراك فى الخاصية وبتكلفتها الفعلية .

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

بند ١٠ - ضوابط خاصة بالتوقيع الإلكترونى :

تلتزم الشركة بتوعية عملاء التداول عبر الإنترنت بإتاحة خاصية التوقيع الإلكترونى وأهميتها على النحو التالى :

إظهار تنويه على الشاشة الرئيسية لنظام التداول عبر الإنترنت يفيد توافر إمكانية الاشتراك فى خاصية التوقيع الإلكترونى لأى عميل يرغب فى 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 الإلكترونى بشهادة إلكترونية مخصصة للتعريف وتشفير البيانات Digital Certificate سارية ، بحيث تظهر للعملاء عند تصفحهم الموقع الإلكترونى .

يجب إصدار رقم لا يكرر Unique Session ID ، مضافًا 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 فى نفس الوقت .

يجب أن تكون التطبيقات مبنية على أساس التحقق من عمليات الإدخال Field Validation فى الحقول الضرورية ومصممة بحيث يتم تشفير البيانات بشكل كامل .

يجب أن تحتفظ الشركة لمدة ٥ سنوات على الأقل بالسجلات الكاملة Transactions Logs والتى تشمل جميع عمليات الدخول والخروج والأوامر الصادرة من العملاء وغيرها .

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 لأى سبب من الأسباب .

يجب أن يقوم نظام التداول بإخطار العميل آليًا عند تغيير كلمة المرور بنجاح من خلال وسيلة الاتصال المتفق عليها والمذكورة فى 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 فى 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 قصيرة أو رسالة بريد إلكترونى للعميل لإخطاره على سبيل التأكيد بأى عملية تؤثر فى رصيد حسابه ، من خلال وسيلة الاتصال المتفق عليها والمذكورة فى العقد .