الهيئة العامة
للرقابة المالية
Egyptian Financial Supervisory Authority

رئيس مجلس الإدارة

قرار رقم (٧٢٩) لسنه ٢٠١٦
بتاريخ: ٢٠١٦/٨/٢٨
بشأن الضوابط التكنولوجية وقواعد تأمين المعلومات المرتبطة
بإصدار وتوزيع شركات التأمين لبعض وثائق التأمين النمطية الكترونياً
من خلال شبكات نظم المعلومات

رئيس الهيئة العامة للرقابة المالية

بعد الاطلاع على القانون رقم ١٠ لسنة ١٩٨١ بإصدار قانون الإشراف والرقابة على التأمين فى مصر ولائحته التنفيذية وتعديلاتها،

وعلى القانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الالكتروني في مصر،

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

وعلى النظام الأساسي للهيئة العامة للرقابة المالية الصادر بقرار رئيس الجمهورية رقم ١٩٢ لسنة ٢٠٠٩،

وعلى مذكرة السيد المستشار نائب رئيس مجلس الدولة المستشار القانوني للهيئة بتاريخ ٢٠١٥/٩/١،

وعلى قرار مجلس إدارة الهيئة رقم (١٢٢) لسنة ٢٠١٥ بشأن تنظيم إصدار وتوزيع شركات التأمين لبعض وثائق التأمين النمطية الكترونياً من خلال شبكات نظم المعلومات.

قـــرر

(المادة الأولى)

على شركات التأمين الحاصلة على موافقة الهيئة على إصدار وثائق تأمين نمطية الكترونياً من خلال نظم معلومات الشركة وإتاحة طباعة الوثيقة وتوزيعها بواسطة المؤمن له مباشرة أو بواسطة إحدى الجهات التى وافقت عليها الهيئة وذلك كله وفقاً للقرار (١٢٢) لسنة ٢٠١٥، أن تلتزم بالضوابط التكنولوجية وقواعد تأمين المعلومات المرفقة بهذا القرار.

(المادة الثانية)

ينشر هذا القرار بالوقائع المصرية وعلى الموقع الالكتروني للهيئة ، ويعمل به من اليوم التالي لتاريخ نشره، ويبلغ إلى الإدارات المعنية لتنفيذه.

رئيس الهيئة
شريف سامي

الهيئة العامة للرقابة المالية
مكتب رئيس الهيئة

٤٦٠٧٦

القرية الذكية، مبنى ١٥- ٨٤ ب
الكيلو ٢٨ طريق مصر / اسكندرية الصحراوى
محافظة الجيزة، الرمز البريدى: ١٢٥٧٧

تليفون: ٠٠ (٠٢٠٢) ٣٥٣٧٠٠٤١ فاكس: ٣٥٣٤٥٣٢٢ (٠٢٠٢)
البريد الإلكتروني: info@efsa.gov.eg
الموقع على الإنترنت: www.efsa.gov.eg

رئيس مجلس الإدارة

الضوابط التكنولوجية وقواعد تأمين المعلومات المرتبطة

بإصدار وتوزيع شركات التأمين لبعض وثائق التأمين النمطية الكترونياً من خلال شبكات نظم المعلومات

أولاً: البنية التحتية التكنولوجية

يكون مركز معلومات شركة التأمين داخل حدود جمهورية مصر العربية وخاضع لقوانينها ويجوز اللجوء للتعاقد على خدمات الاستضافة (Hosting) للبنية التكنولوجية للشركة لدى جهة أخرى داخل مصر من ضمن الجهات المعتمدة من الهيئة لتقديم تلك الخدمات وفقا لقرار رئيس الهيئة رقم ٣١٦ لسنة ٢٠١٤، أو لدى المساهم الرئيسي للشركة خارج مصر فى حال كونه شركة تأمين أو إحدى شركاتها التابعة أو لدى شركات أخرى متخصصة ولها سابقة أعمال فى المجال وذلك بشرط أن توافق عليها الهيئة. يجب أن تكون شركة الاستضافة مقدمة الخدمة معتمدة من الهيئة .

١- وسائل الاتصال

يجب ان تكون كل وسائل الاتصال المستخدمة مصرح لها من الجهاز القومى لتنظيم الاتصالات

٢- الخوادم المركزية ونظم التشغيل

تلتزم شركة التأمين باستخدام أجهزة الخوادم المركزية يتوافر فيها ما يلى كحد أدنى:

أ. جهاز خادم مستقل يعمل كخادم لقواعد البيانات Database Sever (سواء خادم مادي Physical أو باستخدام بيئة افتراضية Virtual)

ب. جهاز خادم مستقل يعمل كخادم للتطبيقات Application Server (سواء خادم مادي Physical أو باستخدام بيئة افتراضية Virtual)

ج. يأن تحقق مواصفات تلك الخوادم الحد الأدنى من متطلبات التشغيل (Hardware and Software Requirements) اللازمة لتشغيل خدمات الإصدار والتوزيع الالكترونى لوثائق التأمين وتخزين بياناتها .

د. أن تكون جميع نظم التشغيل والبرامج الإلكترونية المستخدمة في هذه الخوادم مرخصة ومحدثة

ه. أن يتوافر بها الحد الادني من المستوى المطلوب من العمل الدائم دون توقف (High Availability) بمعدل لا يقل عن ٩٥ %.

في حال رغبة الشركة استخدام بيئة افتراضية Virtual يجب ان يتوفر بها نظام أمن معلومات يسمح بالفصل بين الخوادم باستخدام سياسات وقواعد أمن المعلومات (Security policies and rules)

القرية الذكية، مبنى ٥أ- ٨٤ ب
الكيلو ٢٨ طريق مصر / اسكندرية الصحراوى
محافظة الجيزة، الرمز البريدي: ١٢٥٧٧

تليفون ٣٥٣٧٠٠٤٠ (٠٢) فاكس ٣٥٣٤٥٣٣٣ (٠٢)
البريد الإلكتروني info@efsa.gov.eg
الموقع على الإنترنت: www.efsa.gov.eg

رئيس مجلس الإدارة

٣ حماية وأمن المعلومات

تلتزم الشركة بتوفير البنية التكنولوجية اللازمة لأمن المعلومات لديها (أو لدى جهة الاستضافة) وفقا للضوابط التالية:

أ. تركيب نظام جدار ناري Firewall لتأمين شبكات الاتصال داخل الشركة وبين الشركة والجهات الأخرى القائمة بتوزيع الوثائق ويجوز ان يكون ذلك من خلال مخارج متعددة لنفس الـ Firewall

ب. توفير نظم حماية للشبكة وفقا للخدمات المطلوب حمايتها (على سبيل المثال نظام للحماية من الاختراق Intrusion Prevention System IPS)

ج. اجراء الصيانة الدورية لأجهزة تأمين الشبكات والمعلومات مع مراعاة قواعد الضبط المناسبة لها (Configuration Roles) وتحديثها بصفة مستمرة

د. تزويد جميع أجهزة الحاسب المتصلة بشبكة الشركة (شخصية أو محمولة أو خوادم) ببرامج لمكافحة الفيروسات والبرمجيات الضارة (Antivirus and Antimalware) على أن يتم تحديثها بصفة مستمرة

ه. وضع نظام للمراقبة والتحكم في الدخول والخروج لغرفة الخوادم المركزية (Data Center) من الداخل والخارج.

و. إبلاغ الهيئة عند حدوث أي اختراقات أمنية (Security Incident) تحدث على مستوى البنية الأساسية للمعلومات والأنظمة العاملة عليها، والإجراءات المتخذة بشأنها.

ز. في حالة استخدام موقع الكتروني علي شبكة المعلومات الدولية لاستصدار و طباعة وثائق التأمين يجب أن يتم تأمين هذا الموقع باستخدام شهادة تأمين الكترونية SSL (Website Digital Certificate)

ح. فى حال رغبة شركة التامين فى تطبيق نظام التوقيع الإلكتروني (Digital Signature) يجب أن يكون متوافقاً مع شروط ومتطلبات هيئة تنمية صناعة تكنولوجيا المعلومات. وليكون للتراسل بالبريد الالكترونى مع العملاء حجية قانونية، فإنه يجب فإنه يجب على الشركة توثيق البريد الإلكتروني ومرفقاته باستخدام شهادة توقيع إلكتروني.

ثانياً: المواصفات الفنية لنظام المعلومات (التطبيقات)

١ نظام المعلومات

تلتزم شركة التأمين بتوفير نظام معلومات كامل ومؤمن لتسجيل ومعالجة بيانات العملاء سواء بالتعامل المباشر مع العميل او من خلال الجهة الموزعة للوثيقة. ويتكون النظام من التطبيقات وقواعد البيانات الخاصة بجميع التعاملات على منتجات التامين النمطية المنصوص عليها في القرار رقم ١٢٨ لسنة ٢٠١٥.

رئيس مجلس الإدارة

وفي جميع الأحوال يجب ان تلتزم شركة التأمين بما يلي:

أ. عدم الاحتفاظ ببيانات العميل لدى الجهة الموزعة للوثيقة (تسجيل البيانات والاحتفاظ بها على قاعدة البيانات تكون لدى شركة التأمين فقط).

ب. الحفظ الإلكتروني لدى الشركة لكامل بيانات الوثيقة وشروطها (لتجنب حالات الاقتصار على بيانات العميل وباقى بيانات جدول الوثيقة والإشارة إلى شروط نمطية Template يمكن تعديلها لاحقاً).

ج. أن تكون بيانات الوثيقة التي تظهر على الشاشة والنسخ المطبوعة متفقة مع البيانات التى حددتها الهيئة.

د. يجب ان يحتوي النظام علي علامة مميزة أو رمز للخانات الإجبارية مرتبطة برسائل تنبيهية تظهر للمستخدم حالة ادخال بينات غير متوافقة مع طبيعة بيانات الخانة.

ه. يجب أن يصدر النظام رقم موحد (Unique number) لكل وثيقة علي ان يكون مسلسل وغير متكرر. وذلك بخلاف رقم الوثيقة (Policy Number)

و. الوثيقة لا تصدر ولا يتم إصدار رقم لها إلا بعد التأكد من ادخال جميع البيانات و اظهار للعميل صفحة قابلة للطباعة للمراجعة ويكون بها جميع البيانات المدخلة و جميع شروط الوثيقة، ويكون للمستخدم بعد ذلك خيار تأكيد قبوله لإصدار الوثيقة أو رفضه من خلال الصلاحيات الممنوحة للمستخدم.

ز. على النظام أن يمنع تعديل أو مسح أي بيانات أو معلومات بعد إصدار الوثيقة، ويمكن إلغاء الوثيقة دون حذفها من النظام وتبقى بما يشير إلى أنها ملغاه على قاعدة بيانات الشركة بنفس رقم الوثيقة.

ح. أن يتيح النظام للعميل إمكانية الاطلاع و طباعة شروط الوثيقة في أي مرحلة من مراحل التسجيل أو المراجعة أو بعد صدور الوثيقة.

٢ تأمين دخول المستخدم

أ- يجب ان يمنع النظام دخول نفس اسم المستخدم أكثر من مرة واحدة في نفس الوقت او فتح أكثر من اتصال Sessionبواسطة نفس اسم المستخدم في نفس الوقت.

ب- يجب ألا يسمح النظام باستمرار الاتصال الغير الفعال مع العميل مباشرة أو الجهة الموزعة للوثيقة (Inactive Session) لأكثر من ٢٠ دقيقة ويطلب بعدها النظام إعادة ادخال بيانات التحقق مرة أخرى.

ج - يجب أن يسمح النظام للعميل أو الجهة الموزعة للوثيقة بتغير كلمة السر بنفسه في أي وقت، كما يجب أن يجبر النظام المستخدم (الجهة الموزعة للوثيقة او المستفيد) على تغير كلمة السر عند أول استخدام في حالة صدور أو تغير كلمة السر من قبل شركة التامين نفسها على أن تتبع القواعد المعمول بها في إنشاء كلمة السر بحيث يصعب استنتاجها أو التعرف عليها (لا تقل عن ٨ حروف وأرقام، يجب أن تحتوي على رموز ولا تكون سهلة الاستنتاج والتخمين

القرية الذكية: مبنى ٥أ- ٨٤ ب
الكيلو ٢٨ طريق مصر/ اسكندرية الصحراوى
محافظة الجيزة، الرمز البريدى: ١٢٥٧٧
تليفون: ٣٥٣٢ (٠٢٠٢) فاكس: ٣٥٢١٤٣٣٣ (٠٢٠٢)
البريد الإلكتروني: info@efsa.gov.eg
الموقع على الإنترنت: www.efsa.gov.eg

رئيس مجلس الإدارة

د - فى حالة تعامل العميل مع الشركة مباشرة يمكن للعميل تسجيل حساب جديد على الموقع الاكترونى للشركة على ان يتم التحقق من العميل عن طريق ارسال بريد الكترونى للتحقق من هويته او ارسال رسالة نصية الى رقم هاتف محمول يحدده العميل

هـ فى غير حالات التعامل المباشر بين العميل والشركة، أى وجود جهة قائمة بتوزيع الوثائق – فى الحالات التى سمح بها القرار ١٢٢ لسنة ٢٠١٥ - لا يمكن للعاملين بالجهة تسجيل أنفسهم على نظام شركة التأمين أو موقعها الالكترونى مباشرة ولكن يتم فتح حساب الكترونى لهم من خلال الشركة . وتكون الشركة مسئولة عن تامين كلمة السر التى تمنحها لأي منهم.

و- فى حالة وجود أكثر من مستخدم لدى الجهة القائمة بالتوزيع يجب على شركة التأمين إنشاء حساب لكل مستخدم على حدي كما يجب على الوسيط إخطار شركة التأمين عند أي تغيير يطرأ على المستخدمين لنظام الشركة.

ح - يجب أن يجبر النظام كافة المستخدمين على تغيير كلمة السر كل ٩٠ يوم على الأكثر

ط- يجب على نظام الشركة تسجيل العنوان الاكترونى للمستخدم وقت الدخول IP Address

ثالثاً: ضوابط عامة

١ ضبط التوقيت

تلتزم شركة التأمين بضبط توقيتات (Time Synchronization) لجميع انظمة المعلومات والاجهزة المثبت عليها هذه الانظمة وجميع انظمة الشبكات وأمن المعلومات على توقيت وأحد يكون مماثل لتوقيت جمهورية مصر العربية

٢ - التسجيل والحفاظ بالسجلات

تلتزم شركة التامين بما يالي :

أ. تسجيل جميع الأنشطة Logging Activities التي تحدث على جميع الأجهزة و الأنظمة (System Logs ,Security Logs and Application Logs) و ما تعتمد عليه من أجهزة مساعدة (حاسبات، أجهزة شبكات ، أجهزة تأمين معلومات)

ب. تسجيل جميع محاولات الدخول والخروج من النظام لكل من العميل/ الجهة الموزعة للوثيقة / موظفي الشركة – (الناجحة أو الفاشلة منها) وأن يشمل التسجيل الرقم المميز Unique Session ID،

ج. تسجيل بيانات المستخدم القائم بإدخال البيانات

١. في حالة التعامل المباشر مع العميل يقوم النظام بتسجيل اسم المستخدم القائم بإدخال البيانات

رئيس مجلس الإدارة

٢. في حالة التعامل مع جهة موزعة للوثيقة يجب أن يقوم النظام بتسجيل اسم الجهة واسم المستخدم القائم بالإدخال، وعلى أن تكون تلك البيانات غير قابلة للتعديل (Tamper Proof).

د. يجب ان يقوم النظام بحفظ سجلات مستقلة للعمليات التالية:

١. الدخول والخروج من النظام (Login، Logoff)

٢. النموذج الالكترونى لطلب إصدار الوثيقة (Form Submission)

ويجب أن يتم الاحتفاظ بجميع السجلات(Logs) المشار إليها في هذا القرار لمده لا تقل عن خمس سنوات. وفي حالة وجود نزاع مع أحد العملاء تلتزم الشركة بالاحتفاظ بكافة السجلات لحين تسوية النزاع أو صدور حكم قضائي نهائي فيه.

٣. النسخ الاحتياطية (Backup)

تلتزم شركة التأمين بحفظ نسخ احتياطية لكافة البيانات المشار اليها في هذا القرار بحيث تضمن استعادة تلك البيانات حالة الرجوع إليها عند الحاجة .

ويتم حفظ نسخ إضافية من النسخ المشار إليها أعلاه فى موقع بديل مع مراعاة أن يتم تبنى وتطبيق سياسة مكتوبة وواضحة لتسلسل النسخ ومدة الإحتفاظ.

٤- الخصوصية

يقتصر استخدام بيانات العميل للغرض الذي أدخلت من أجله، وحماية خصوصية العميل وعدم إتاحة بياناته الشخصية لأي أغراض تسويقية بالاتصال الهاتفي أو الإلكتروني من قبل الجهة الموزعة للوثيقة أو المصدرة لها، وعدم اتاحة تلك البيانات لأي طرف آخر.

٤٦٠٧٦

القرية الذكية، مبنى ١٥أ- ٨٤ ب
الكيلو ٢٨ طريق مصر/ اسكندرية الصحراوى
محافظة الجيزة، الرمز البريدى: ١٢٥٧٧

تليفون ٣٥٣٧٠٠٤٠ (٠٢٠٢) فاكس ٣٥٣٤٥٢٣٣ (٠٢٠٢)
البريد الإلكتروني info@efsa.gov.eg
الموقع على الإنترنت www.efsa.gov.eg