



## قرار رقم (1) لسنة 2022

بشأن الضوابط التكنولوجية وقواعد تأمين وحماية المعلومات المرتبطة بتقديم الخدمات المالية غير المصرفية عبر المنصات الالكترونية

مدير عام الإدارة العامة لخدمات التمويل الرقمي والابتكار،  
استناداً لتعليمات رقم (2) لسنة 2022 بشأن ترخيص منصات الكترونية لبيع أو تقديم خدمة تجميع ومقارنة خدمات مالية غير مصرفية ولا سيما المادة (1/5/و)،  
وبناءً على الصلاحيات المخولة لنا قانوناً،  
وتحقيقاً للمصلحة العامة،  
قررنا الآتي:

### مادة (1)

يكون للكلمات والعبارات الواردة في هذا القرار المعاني المخصصة لها في تعليمات رقم (2) لسنة 2022 بشأن ترخيص منصات الكترونية لبيع أو تقديم خدمة تجميع ومقارنة خدمات مالية غير مصرفية، ما لم تدل القرينة على خلاف ذلك.

### مادة (2)

تلتزم الجهة المشغلة للمنصة الإلكترونية بالآتي:

1. استخدام واجهات تقنية معيارية من خلال (Web Service) لضمان تبادل البيانات الالكترونية ورسائل البيانات الكترونياً مع الأنظمة التقنية والوسائل الالكترونية للجهات المالية غير المصرفية، وذلك لغرض تبادل معلومات طالب الخدمة مع الجهات المالية غير المصرفية المتعاقد معها.
2. تمكين الجهات المالية غير المصرفية المتعاقد معها من تقييم المخاطر المرتبطة بطالب الخدمة المالية غير المصرفية.
3. ارسال طلب الخدمة او المنتج المالي غير المصرفي واستقبال عروض المنتجات والخدمات واصدارها لحظياً من خلال واجهات التخاطب التقنية (Web Service API) ما بين مشغل المنصة الالكترونية والجهات المالية غير المصرفية.
4. التأكد من تهيئة الجهة المالية غير المصرفية لبنيتها التقنية قبل الربط معها لتمكين تبادل المعلومات والبيانات الالكترونية عبر الوسيلة الالكترونية.





### مادة (3)

1. يجب على مشغل المنصة الالكترونية توفير مركز بيانات داخل فلسطين وفقاً للتشريعات السارية في فلسطين، ومجهز بإعدادات البنية التحتية المناسبة من حيث (الأمن، التكييف، خطوط الاتصال، الطاقة الكهربائية والاحتياطية، وأنظمة إطفاء الحريق ومستشعرات الرطوبة، وغيرها) ويجوز التعاقد على خدمات الاستضافة (Hosting) للبنية التكنولوجية لمشغل المنصة الالكترونية لدى جهة أخرى متخصصة ولها سابقة أعمال في المجال، وللهيئة التحقق من متطلبات البنية التحتية ومواصفات مركز البيانات وعلى نفقة مشغل المنصة.
2. يجب أن تكون كافة الوسائل الالكترونية ووسائل الاتصال الأخرى المستخدمة مصرح لها من الجهات المختصة في فلسطين
3. تلتزم الجهات المالية غير المصرفية التي ترغب باستخدام منصات الكترونية لإصدار خدمات ومنتجات مالية غير مصرفية، أن تضمن توافر الحد الأدنى من المتطلبات الالكترونية الموجودة لدى مشغل المنصة الالكترونية باستخدام أجهزة الخوادم المركزية التي يتوافر فيها ما يلي كحد أدنى:
  - أ. جهاز خادم مستقل او وسيط يعمل كخادم لقواعد البيانات Database Server (سواء خادم مادي Physical أو باستخدام بيئة افتراضية Virtual).
  - ب. الحد الأدنى من متطلبات التشغيل (Hardware and Software Requirement) اللازمة لتشغيل خدمات الاصدار للمنتجات والخدمات المالية غير المصرفية وتخزين بياناتها.
  - ج. كافة نظم التشغيل والبرامج الالكترونية المستخدمة في هذه الخوادم مرخصة ومحدثه.
  - د. الحد الأدنى من المستوى المطلوب من العمل الدائم دون توقف High Availability بمعدل لا يقل عن 95%.

### مادة (4)

1. يلتزم مشغل المنصة الالكترونية بتوفير البنية التكنولوجية اللازمة لأمن المعلومات لديه وفقاً للضوابط ادناه:
  - أ. تركيب نظام جدار ناري Firewall و / أو نظام إدارة التهديدات الموحدة (Unified Threat Management (UTM)) لتأمين شبكات الاتصال داخل الجهة المالية غير المصرفية وبينها وبين المنصات الأخرى المتعاقد معها ويجوز أن يكون ذلك من خلال مخارج متعددة لنفس الجدار الناري.
  - ب. توفير نظم حماية للشبكة وفقاً للخدمات المطلوب حمايتها (على سبيل المثال نظام للحماية من الاختراق Intrusion Prevention System IPS).
  - ت. اجراء الصيانة الدورية لأجهزة تأمين الشبكات والمعلومات مع مراعاة قواعد الضبط المناسبة لها ( Configuration Rules) وتحديثها بصفة مستمرة.





- ث. تزويد جميع أجهزة الحاسب المتصلة بشبكة الشركة (شخصية أو محمولة أو خوادم) ببرامج مكافحة الفيروسات والبرمجيات الضارة (Antivirus and Antimalware) على أن يتم تحديثها بصفة مستمرة.
- ج. وضع نظام للمراقبة والتحكم في الدخول والخروج لغرفة الخوادم المركزية (Data Center) من الداخل والخارج.
- ح. ابلاغ الهيئة فوراً حال حدوث أي اختراقات أمنية (Security Incident) تحدث على مستوى البنية الأساسية للمعلومات والأنظمة العاملة عليها، والاجراءات المتخذة بشأنها.
- خ. في حالة استخدام موقع الكتروني على شبكة المعلومات الدولية لتقديم خدمات ومنتجات مالية غير مصرفية، يجب أن يتم تأمين هذا الموقع باستخدام شهادة تأمين الكترونية (Website Digital Certificate SSL).
- د. في حال استخدام التوقيع الإلكتروني (E. Signature)، يجب أن يكون متوافقاً مع شروط ومتطلبات الجهات ذات الاختصاص في فلسطين.
- ذ. في حال رغبت مشغل المنصة الالكترونية استخدام بيئة افتراضية Virtual، يجب أن يتوفر بها نظام أمن معلومات يسمح بالفصل بين الخوادم باستخدام سياسات وقواعد أمن المعلومات (Security Polices and Rules).
- ر. القيام بالفحوصات الدورية اللازمة للتأكد من حماية النظام قبل وبعد الاطلاق كالتدقيق على أنظمة المعلومات (IT Audit) وفحوصات اختبار الاختراق (Penetration Testing).
- ز. يحق للهيئة تنفيذ او طلب تنفيذ فحوصات اختبار الاختراق او اية فحوصات تراها مناسبة وعلى نفقة مشغل المنصة.
2. تكون الجهة المالية غير المصرفية المتعاقد معها من قبل مشغل المنصة الالكترونية مسؤولة عن التأكد من توافر متطلبات حماية وأمن المعلومات لدى مشغل المنصة الالكترونية، وذلك في حال الاستضافة من طرف ثالث.

#### مادة (5)

يلتزم مشغل المنصة الالكترونية والجهات المالية غير المصرفية بما يلي:

1. أن تكون بيانات الخدمات والمنتجات المالية غير المصرفية التي تظهر على الشاشة سواءً من خلال منصة الشركة أو مشغل المنصة الإلكترونية متفقة مع البيانات والمتطلبات التي تحددها الهيئة.
2. استخدام نهج "خطوة خطوة" للإفصاح عن عناصر المعلومات الفردية (بدلاً من تقديم المعلومات بالكامل).
3. يجب أن يحتوي نظام تقديم الخدمات والمنتجات المالية غير المصرفية على علامة مميزة أو رمز للخانات الاجبارية مرتبطة برسائل تنبيهية تظهر للمستخدم حالة ادخال بيانات غير متوافقة مع طبيعة بيانات الخانة.
4. عدم اصدار المنتج او الخدمة المالية غير المصرفية الا بعد التأكد من ادخال جميع البيانات واظهار صفحة قابلة للطباعة وللمرجعة من قبل المستخدم تتضمن كافة البيانات المدخلة وجميع شروط الخدمة او المنتج، ويكون للمستخدم بعد ذلك خيار تأكيد قبوله لإصدار الخدمة او المنتج او رفضه من خلال الصلاحيات الممنوحة للمستخدم.





5. منع إجراء أي تعديل أو مسح لأية بيانات أو معلومات على الخدمة أو المنتج المالي غير المصرفي بعد إصداره عبر المنصة الإلكترونية.
6. أن تتيح المنصة لطالب الخدمة أو المنتج المالي غير المصرفي إمكانية الاطلاع وطباعة شروط الخدمة أو المنتج في أي مرحلة من مراحل التسجيل أو المراجعة أو بعد صدور المنتج أو الخدمة.

### مادة (6)

1. يجب أن يُراعى في النظام المستخدم لتشغيل المنصة الإلكترونية ما يلي:
- أ. عدم السماح باستمرار الاتصال غير الفعال مع المستخدم مباشرة (Inactive Session) لأكثر من 20 دقيقة ويطلب بعدها النظام إعادة ادخال بيانات التحقق مرة أخرى.
- ب. السماح للمستخدم أو المنصة المصدرة للخدمة أو المنتج المالي غير المصرفي بتغيير كلمة السر بنفسه في أي وقت، كما يجب أن يجبر النظام المستخدم (المنصة المصدرة أو المستفيد) على تغيير كلمة السر عند أول استخدام في حالة صدور أو تغيير كلمة السر من قبل الجهة المالية غير المصرفية نفسها على أن تتبع القواعد المعمول بها في انشاء كلمة السر، بحيث يصعب استنتاجها أو التعرف عليها (لا تقل عن 8 حروف وأرقام، يجب أن تحتوي على رموز ولا تكون سهلة الاستنتاج والتخمين).
- ج. إجبار جميع المستخدمين على تغيير كلمة السر بحد أدنى مرتين في العام.
- د. تسجيل العنوان الإلكتروني للمستخدم وقت الدخول IP address.
- هـ. حفظ سجلات مستقلة للعمليات التالية:
1. الدخول والخروج من النظام (Logoff, Login).
2. النموذج الإلكتروني لطلب الخدمة أو المنتج المالي غير المصرفي (Form Submission).
- و. تسجيل بيانات المستخدم من حيث تحديد اسم الجهة واسم المستخدم القائم بالإدخال، وعلى أن تكون تلك البيانات غير قابله للتعديل (Tamper Proof).
2. يلتزم مشغل المنصة الإلكترونية والجهات المالية غير المصرفية المتعاقد معها بضبط توقيتات (Time Synchronization) لجميع أنظمة المعلومات والأجهزة المثبت عليها هذه الأنظمة وجميع أنظمة الشبكات وأمن المعلومات على توقيت واحد يكون مماثل لتوقيت دولة فلسطين.



مادة (7)

يلتزم مشغل المنصة الالكترونية بتوثيق الأنشطة وحفظ السجلات على النحو الآتي:

1. تسجيل جميع الأنشطة Login Activities التي تحدث على جميع الأجهزة والأنظمة ( System Logs, Security Logs and Application Loges ) وما تعتمد عليه من أجهزة مساعدة (حاسبات، أجهزة شبكات، أجهزة تأمين معلومات).
2. تسجيل جميع محاولات الدخول والخروج من النظام لكل من المستخدم (مشغل المنصة)، وموظفي الجهات المالية غير المصرفية المتعاقد معها (المحاولات الناجحة أو الفاشلة منها) وأن يشمل التسجيل الرقم المميز Unique Session ID.
3. الاحتفاظ بجميع السجلات (Logs) المشار إليها في هذه التعليمات لمدة لا تقل عن خمس سنوات، وفي حال وجود نزاع مع أحد العملاء، تلتزم الجهة المالية غير المصرفية ومشغل المنصة بالاحتفاظ بكافة السجلات لحين تسوية النزاع أو صدور حكم قضائي نهائي فيه.
4. حفظ نسخ احتياطية لكافة البيانات المشار إليها في هذه التعليمات، بحيث تضمن استعادة تلك البيانات حالة الرجوع إليها عند الحاجة.
5. حفظ نسخ اضافية من النسخ المشار إليها اعلاه في موقع بديل، مع مراعاة أن يتم تبني وتطبيق سياسة مكتوبة وواضحة لتسلسل النسخ ومدة الاحتفاظ بها.

صدر هذا القرار في مدينة البيرة بتاريخ 28 تشرين ثاني 2022.

د. بشار أبو زعرور

مدير عام الإدارة العامة لخدمات التمويل الرقمي والابتكار

