



سلطة النقد الفلسطينية
PALESTINE MONETARY AUTHORITY

تعليمات رقم (6) لسنة 2021 بشأن تنظيم الأعمال الخاصة بشركات خدمات الدفع

استناداً لأحكام القرار بقانون رقم (17) لسنة 2012 بشأن قانون تسوية المدفوعات الوطني ولاسيما المادتين (5) و(9) منه،
واستناداً لما أقره مجلس إدارة سلطة النقد في جلسته رقم (236) بتاريخ 2021/06/23،
وتحقيقاً للمصلحة العامة،
فقد أصدرنا التعليمات الآتية:

الفصل الأول التعريفات ونطاق التطبيق

مادة (1)

تعريفات

يكون للكلمات والعبارات الواردة في هذه التعليمات المعاني المخصصة لها أدناه ما لم تدل القرينة على خلاف ذلك:

سلطة النقد:	سلطة النقد الفلسطينية.
خدمات الدفع:	كافة الخدمات التي ترتبط بإرسال واستقبال وتنفيذ أوامر الدفع في أي من العملات.
مقدم الخدمة:	الشركة المرخص لها من سلطة النقد لتقديم خدمات الدفع.
الشخص:	الشخص الطبيعي أو الاعتباري.
المستخدم:	الشخص الذي يستخدم خدمات الدفع بصفته دافع أو مستفيد.

مادة (2)

الهدف ونطاق التطبيق

1. تهدف هذه التعليمات إلى تنظيم أعمال مقدمي خدمات الدفع في فلسطين بشكل آمن وشفاف.
2. تطبق أحكام هذه التعليمات على كافة الشركات المرخص لها من سلطة النقد لتقديم خدمات الدفع.



سلطة النقد الفلسطينية
PALESTINE MONETARY AUTHORITY

مادة (3)

الخدمات والأعمال المحظورة

يحظر على مقدم الخدمة القيام بأي من الآتي:

1. استخدام أو التعامل بالعملات الافتراضية و/أو الأصول الافتراضية.
2. تقديم التسهيلات الائتمانية/ التمويلات المباشرة وغير المباشرة.
3. ممارسة أعمال شراء وبيع العملات.
4. تقديم أي خدمة دون الحصول على الموافقة الخطية المسبقة من سلطة النقد.
5. المتاجرة على الهامش في الأسواق العالمية (الفوركس) والمتاجرة بالأوراق المالية.
6. تملك العقارات أو المتاجرة بها، باستثناء تملك عقار بموافقة خطية مسبقة من سلطة النقد لغايات استخدامه كمقر لمقدم الخدمة.

مادة (4)

الحصول على التسهيلات الائتمانية

يحظر على مقدم الخدمة الاقتراض أو الاستدانة بشكل مباشر أو غير مباشر دون الحصول على الموافقة الخطية المسبقة من سلطة النقد.

مادة (5)

التأمينات النقدية

يجب على مقدم الخدمة إيداع تأمينات نقدية لدى سلطة النقد بنسبة 5% من متطلبات الحد الأدنى لرأس المال المدفوع.

مادة (6)

الترابط مع أنظمة تشغيل المدفوعات المدارة من قبل سلطة النقد

يجب أن تكون خدمة الدفع قابلة للتشغيل المتبادل والمواءمة مع أنظمة تشغيل المدفوعات المدارة من قبل سلطة النقد أو من ترخصه لذلك.





سلطة النقد الفلسطينية
PALESTINE MONETARY AUTHORITY

مادة (7)

منع الاحتكار

يحظر على مقدم الخدمة الإخلال بالمنافسة أو الحد منها أو منعها من خلال عقد اتفاقيات خاصة وممارسات تؤدي في نهايتها إلى احتكار تقديم أي من خدمات الدفع.

مادة (8)

طلب إيقاف خدمة الدفع

يجوز إيقاف تقديم خدمة الدفع بناءً على طلب مقدم الخدمة وفق الإجراءات الآتية:

1. تقديم طلب خطي.
2. تزويد سلطة النقد بكافة الوثائق ومبررات الطلب.
3. تقديم المستندات والوثائق التي تثبت التزام مقدم الخدمة بالوفاء بتعهداته تجاه مستخدميه.
4. تتخذ سلطة النقد قراراً في الطلب خلال 30 يوماً من تاريخ استكمال الطلب وتقوم بإبلاغ مقدم الخدمة بردها خطياً.

مادة (9)

المتطلبات الأساسية لأمن أنظمة خدمات الدفع

يجب على مقدم الخدمة الالتزام بالمتطلبات الأساسية وأمن أنظمة خدمات الدفع بما يتوافق مع المتطلبات الواردة في الملحق رقم (1) المرفق بهذه التعليمات (ملحق المتطلبات الأساسية لأمن أنظمة خدمات الدفع).

مادة (10)

الإلغاء

1. تلغى التعليمات رقم (6) لسنة 2020 بشأن تنظيم الأعمال الخاصة بشركات خدمات الدفع.
2. يلغى كل ما يتعارض مع أحكام هذه التعليمات.



سلطة النقد الفلسطينية
PALESTINE MONETARY AUTHORITY

مادة (11)

التنفيذ والنفذ

يجب على كافة الجهات المختصة، كل فيما يخصه، تنفيذ أحكام هذه التعليمات، وتطبق من تاريخ صدورها.

صدرت في مدينة رام الله بتاريخ 30/06/2021 م

د. فراس ملحم

المحافظ

ز.م

ملحق رقم (1)

المتطلبات الأساسية لأمن أنظمة خدمات الدفع

أولاً: الحوكمة وإدارة المخاطر

1. وضع ضوابط رقابية فعالة على المخاطر المرتبطة بالأنشطة المتعلقة بخدمات الدفع، بما في ذلك المساءلة وإعداد السياسات والضوابط لإدارة هذه المخاطر.
2. المراجعة الشاملة والمستمرة لبذل العناية الواجبة والرقابة لإدارة عمليات الاسناد الخارجي والاعتماد على الأطراف الثالثة التي تدعم خدمات الدفع الإلكتروني، حال إقرارهما من سلطة النقد.

ثانياً: أمن المعلومات:

1. يقع على عاتق الشركة مسؤولية الحفاظ على سلامة أنظمة وتطبيقات خدمات الدفع والحفاظ على سرية المعلومات باستخدام التكنولوجيا المناسبة ووسائل التدقيق لتوفير الحماية -لكافة الخدمات التي تقدمها الشركة- من المخاطر والمحافظة على سرية المعلومات واتخاذ التدابير اللازمة لذلك وبما يتناسب مع حساسية المعلومات المخزنة، وبما يشمل ما يلي:
 - أ. استخدام التكنولوجيا المناسبة لتشفير المعلومات ومنع الاختراق وتنفيذ الرقابة المستمرة على الأنظمة المستخدمة في الشركة.
 - ب. استخدام أحدث الأجهزة والأنظمة اللازمة لمراقبة وحماية الشبكة وبيئة تكنولوجيا المعلومات مثل (Firewalls, WAF, IDS, IPS, SEIM).
 - ت. اعتماد الإجراءات والضوابط التي تكفل الوصول الآمن لشبكة وأنظمة الشركة عن بعد (Remote Access).
 - ث. إجراء تقييم لنقاط الضعف Vulnerability Assessment بشكل دوري وعند حدوث تغيير جوهري في البيئة التشغيلية للأنظمة.
 - ج. إجراء اختبار لفحص الاختراق الخارجي Penetration Testing مرة واحدة سنوياً على الأقل من قبل فريق مؤهل وقبل البدء في تقديم أي خدمات جديدة، ولسطة النقد طلب إجراء الاختبار في أي وقت.
 - ح. الامتثال للمعايير الدولية الخاصة بأمن بيانات بطاقات الدفع والمعرفة باسم PCI-DSS عند تفعيل أي من خدمات الدفع بواسطة البطاقات.
 - خ. تعزيز الخصائص الأمنية لتطبيقات الدفع بشكل مستمر ومتى تطلب، وإخضاعها إلى اختبارات متعددة قبل التشغيل وإتاحتها للمستخدمين حصراً من خلال عناوين مقدم الخدمة وموقعها الإلكتروني الرسمي.
2. اتخاذ الإجراءات المناسبة لحماية وسائل الدفع الخاصة بالمستخدمين، بما يشمل ما يلي:
 - أ. درجة تعقيد كلمة السر وطولها.
 - ب. تشفير كلمة السر.
 - ت. مدة صلاحية كلمة السر والحد من تكرارها.
 - ث. استخدام التقنيات الآلية المناسبة الآمنة لإنشاء كلمة السر

- ج. الحد الأقصى للمحاولات غير الناجحة في ادخال كلمة السر.
- ح. محددات انشاء وتفعيل كلمة السر وضوابط تسليمها للمستخدمين.
3. على مقدم الخدمة حماية بياناته بمختلف انواعها عند تخزينها او نقلها، من خلال التشفير وحفظ مفاتيح التشفير والمصادقة بمكان آمن ضمن ضوابط رقابة ثنائية ومراجعتها بشكل مستمر.
4. تشفير اية بيانات شخصية او بيانات الحركات المالية او بيانات المستخدمين والتي يتم حفظها لدى طرف ثالث.
5. على مقدم الخدمة ضبط اعدادات البنية التحتية من أنظمة تشغيل وقواعد بيانات وخوادم وأنظمة حماية بما يتوافق مع أحد المعايير العالمية لأمن المعلومات مثل ISO27001.
6. يجب على مقدم الخدمة اتخاذ الإجراءات المناسبة للمصادقة على هوية المستخدمين الذين تدير أعمالهم في خدمة الدفع والاذن بذلك.
7. يجب على مقدم الخدمة استخدام أساليب مصادقة المعاملات التي تعزز عدم التتصل وتثبت المساءلة والمحاسبة فيما يخص معاملات خدمات الدفع الإلكترونية.
8. تغيير كلمات السر المصاحبة لكافة مكونات بيئة تكنولوجيا المعلومات والاتصالات (Default Passwords) بشكل فوري عند بدء استخدامها وقبل الانتقال إلى بيئة العمل الفعلية.
9. على مقدم الخدمة تحديث أنظمة التشغيل والبرمجيات المثبتة على اجهزة وخوادم بيئة تكنولوجيا المعلومات والاتصالات بأخر التحديثات الموصى بها من الجهة الموردة مع ضرورة اجراء الفحوصات اللازمة قبل تنفيذ هذه التحديثات.
10. استخدام نسخ مرخصة من البرامج والأنظمة وقواعد البيانات.
11. استخدام خطوط اتصال ذات سرعة مناسبة لاستيعاب حجم البيانات المرسله لضمان عدم بطؤ او انقطاع الاتصال أو فقدان البيانات.

ثالثاً: التوعية وأمن وحماية المستخدمين:

1. ينبغي ان تغطي التوعية الأمنية بالحد الأدنى ما يلي:
 - أ. التوعية وتقنيات تجنب محاولات الاحتيال المحتملة عبر الإنترنت، بما في ذلك:
 - هجمات التصيد واستخدام هوية مقدم خدمة الدفع من خلال المواقع المزيفة.
 - تقديم النصيحة للمستخدمين بعدم الوثوق بأي موقع الكتروني عبر الإنترنت لمجرد انه يحمل هوية مقدم خدمة الدفع.
 - ب. الاستخدام السري لاسم المستخدم وكلمة المرور
 - يجب على المستخدمين عدم مشاركته كلمات المرور الخاصة بهم.
 - لا يحتاج العميل تحت أي ظرف من الظروف الإفصاح عن رقم التعريف الشخصي (PIN) أو كلمة المرور لأي من موظفي مقدم خدمة الدفع.
 - ضرورة تغيير كلمه المرور بشكل دوري.
 - ت. اختيار كلمة المرور بعناية لتجنب تخمينها.

- ث. تقديم المشورة والنصح للعملاء حول كيفية تحديد أو إنشاء كلمات مرور قوية أو أرقام تعريف شخصية لا يمكن تخمينها أو توقعها بسهولة.
- ج. الحفظ المناسب لكلمة المرور.
2. الاعتماد واستخدام ضوابط نفاذ قوية من خلال فئتين من فئات التوثيق Two Factor Authentication .
3. عدم الكشف عن المعلومات الشخصية للأشخاص غير المصرح لهم أو للمواقع المشكوك فيها أو لرسائل البريد الإلكتروني.
4. توعية المستخدمين بعدم استخدام ادوات الدفع الإلكتروني من خلال أجهزة الكمبيوتر العامة أو المشتركة والشبكات اللاسلكية المجانية.
5. تقديم المشورة والنصح للعملاء حول كيفية التعرف على موظفي مقدم خدمة الدفع في حال تم تلقي اتصال من شخص مدعى بأنه من مقدم خدمة الدفع.
6. استخدام أحدث الإصدارات لجدار الحماية الشخصي Firewall وأنظمة مكافحه الفيروسات Anti-Virus.

رابعاً: ضوابط الوصول

1. تطبيق سياسة فصل المهام والصلاحيات في الوظائف التشغيلية والفنية والتقنية المرتبطة بالخدمة.
2. يجب على مقدم خدمة الدفع التأكد من وجود ضوابط فعالة وامتيازات تفويض الوصول المناسبة، لمنع دخول الأشخاص غير المخول لهم لأنظمة مقدم خدمة الدفع الإلكتروني وقواعد البيانات والتطبيقات الخاصة بخدمة الدفع الإلكتروني.
3. منح الصلاحيات على قدر الحاجة، ومراجعتها بشكل دوري.
4. اعداد واعتماد مصفوفة الصلاحيات Authority Matrix بحيث تشمل على كافة الصلاحيات الوظيفية والمالية لكافة مستخدمي الأنظمة لدى الشركة.
5. تقييم برنامج ادارة الوصول وهوية المستخدم المطبق في الخدمات المقدمة.
6. وضع ضوابط مناسبة للتحكم بالوصول عن بعد لبيئة العمل من قبل شركات الدعم الفني من خلال برامج آمنة.

خامساً: المراقبة الفعالة

1. على مقدم خدمة الدفع التأكد من تفعيل خاصية تسجيل الأحداث (Audit trail) للاحتفاظ بجميع الحركات والتغييرات التي تحدث على بيانات أنظمة الدفع وضمان الرجوع إليها.
2. مراجعة سجلات الدخول والتدقيق عليها والاحتفاظ بها للتأكد من دخول المستخدمين المخولين فقط على البيانات ومن قيام الأشخاص المخولين بالتعديل على أي إعدادات أو بيانات خاصة بمنظومة الدفع الإلكتروني.
3. التأكد من وجود سجلات الأحداث الأمنية لكافة الأنظمة.
4. اخطار سلطة النقد بشكل فوري، دون تأخير اضطراري عن أحداث الاحتيال أو فشل أنظمة أو الدخول لغير المصرح لهم، أو أي انتهاك لأمن المعلومات، أو تسرب للبيانات هم على دراية بها، يؤثر أو من المرجح أن

يؤثر على بيانات مقدم خدمة الدفع او خدماته الإلكترونية التي قد يتعرض لها مقدم الخدمة أو أي طرف ثالث متعاقد معه فوراً.

5. توفير الية وأنظمة خاصة بتحليل ومراقبة السجلات المختلفة وبشكل مستمر .

6. المراقبة الفعالة للخوادم وأجهزة الشبكة والحماية ووحدات التخزين من حيث Logs، Critical and Warning.

سادساً: استمرارية العمل

1. الاحتفاظ بنسخ احتياطية بشكل دائم ضمن إجراءات معتمدة، لضمان استعادة كافة البيانات والمعلومات المتعلقة بالأنظمة المرتبطة بتقديم الخدمات.

2. توفير مستوى مناسب من الحماية المادية وغير المادية للنسخ الاحتياطية.

3. توفير التقنيات والضوابط اللازمة لتخزين واسترجاع البيانات بسرعة وكفاءة وضمان توافرية وتكاملية وموثوقية تلك البيانات.

4. فحص استرجاع النسخ الاحتياطية وفق إجراءات النسخ الاحتياطي المعتمدة وتوثيق إجراءات ونتائج الاسترجاع.

5. وضع وتنفيذ خطط دورية لاختبار الأنظمة والبيئة الأمنية المرتبطة بها.

6. إضافة الخدمة إلى موقع التعافي من الكوارث الخاص بمقدم خدمة الدفع بما يضمن إدارة وتشغيل الخدمة المقدمة بشكل فوري في حال حدوث أي عطل أو طارئ يمنع استمرار خدماته من خلال المقر الأصلي.

7. تحديث خطة استمرارية عمل مقدم خدمة الدفع بما يشمل هذه الخدمة.

8. اعداد واعتماد خطة لإدارة استمرارية العمل تحدد فيها الإجراءات والعمليات والأنظمة المطلوبة لاستمرار العمليات التشغيلية في الشركة في حالات التعطل عن العمل، على ان يتم مراجعة الخطة وتحديثها بشكل دوري.

9. يكون مقدم خدمة الدفع مسؤولاً مسؤولاً كاملة تجاه كافة مستخدمي الخدمات التي يقدمها في حال فشل الأنظمة التي يديرها أو اختراقها أو تسرب المعلومات منها أو سوء إدارة الحسابات، وبما يشمل تحمل كافة الخسائر المادية التي قد تنتج عن ذلك.

10. على مقدم خدمة الدفع التأكد من وجود الضوابط الكافية لضمان التوافرية العالية (High Availability) لمكونات بيئة تكنولوجيا المعلومات والاتصالات والخوادم والأنظمة المرتبطة بالخدمة، لتقليل نقاط الفشل التي يمكن ان تؤدي الى تعطل العمل.

11. اعداد واعتماد إجراءات تفصيلية والتي يمكن من خلالها تشغيل بيئة تكنولوجيا المعلومات والانتقال الى الموقع البديل.

سابعاً: سياسة التغيير والتحديث

1. على مقدم خدمة الدفع تطوير اجراءات شاملة لإدارة التغيير والتحديث على الأنظمة المستخدمة بما يشمل توثيق الموافقات الإدارية اللازمة وآلية وصلاحيات التطبيق والمراجعة بعد التطبيق، والتأكد من خضوع التغييرات الجديدة للاختبار الكافي قبل التطبيق، بحيث تشمل ادارة التصحيح (Patch Management) والتحكم في التغييرات (Control Management).
2. توفير بيئة خاصة للتطوير والفحص منفصلة عن البيئة الحية للنظام.
3. اجراء فحص ومراجعة أمنية للبرامج المطورة Source Code Review لضمان سلامة أنظمة الدفع المستخدمة.
4. على مقدم خدمة الدفع اعداد واعتماد الإجراءات اللازمة لضمان عدم تنفيذ أي تعديل غير مصرح به على نسخة النظام الأصلية (Source Code) وحفظها في مكان آمن وفق مستويات حماية مناسبة.

