



سلطة النقد الفلسطينية
PALESTINE MONETARY AUTHORITY

تعميم رقم (55 / 2022)

إلى كافة شركات خدمات الدفع العاملة في فلسطين

التاريخ: الإثنين، 07 آذار، 2022

الموضوع: الأحداث التشغيلية المتعلقة بتكنولوجيا المعلومات/ أمن المعلومات

بهدف الحد من المخاطر السيبرانية التي قد تتعرض لها شركات خدمات الدفع، وبهدف عدم التأثير سلباً على سلامة واستمرارية عملها في ظل ارتفاع حجم الهجمات السيبرانية، وللحد من المخاطر المتوقع أن تتعرض لها، واستناداً لأفضل المعايير والممارسات الفضلى وتعليماتنا ذات العلاقة يُطلب من كافة شركات خدمات الدفع الالتزام بما يلي:

1- إنشاء فريق داخلي في الشركة يتولى مسؤولية مراجعة وتقييم منظومة أمن المعلومات وقدرتها على مواجهة المخاطر بهدف ضمان استمرارية الاعمال في الأوقات الحرجة، وتحديد الخطوات الإضافية المطلوب القيام بها لمواجهة ارتفاع مستوى التهديدات، وتحديد الفجوة الحالية وخطة المعالجة، ورصد الموازنات اللازمة للتنفيذ في اقرب وقت ممكن.

2- تزويد سلطة النقد بتقرير الفجوة وخطة المعالجة في موعد لا يتجاوز 2022/6/30.

3- إخطار سلطة النقد بشكل فوري، دون تأخير، بالأحداث والهجمات السيبرانية التي تعرّضت لها أو قد تتعرض لها الشركة أو أي طرف ثالث متعاقد معها تؤثر أو من المرجح أن تؤثر على أنظمة وخدمات الشركة، وبغض النظر عن فترة الانقطاع أو عدم انتظام الخدمة، بما يشمل:

أ. الهجمات السيبرانية وأي انتهاك لأمن المعلومات سواء كانت ناجحة أو محاولة فاشلة.

ب. أحداث الاحتيال.

ت. فشل الأنظمة/ تشويش على عمل الانظمة.

ث. الدخول غير المصرح به.

ج. تسرب البيانات.

4- يتم الإبلاغ من خلال البريد الإلكتروني أدناه أو الهاتف/الموبايل على أن تُعزز خطياً وبشكل تفصيلي بحد أقصى يومين من تاريخ الحدث حسب الملحق المرفق.

(To: ITSVD@pma.ps) (CC: bshubairi@pma.ps)

مجموعة الرقابة

سلطة النقد الفلسطينية



Incidents Form

Basic Information	
1. Particulars of Reporting:	
• Name of the Company	
• Date and Time of Reporting to PMA	
• Name of Person Reporting	
• Designation/Department	
• Contact details (e.g. official email-id, telephone no, mobile no) - IT Manager. - Information Security Officer	
2. Details of Incident:	
• Date and time of incident detection	



Incidents Form

- **Type of incidents and systems affected**

i. Outage of Critical IT system(s)

ii. Cyber Security Incident (e.g. DDOS, Ransom ware/crypto ware, data breach, data destruction, web defacement, etc.)?

iii. Theft or Loss of Information (e.g. sensitive customer or business information stolen or missing or destroyed or corrupted)?

iv. Outage of Infrastructure (e.g. which premises- DC, branch, etc., power/utilities supply, telecommunications supply,)?

v. Financial (e.g. liquidity)?



Incidents Form

What actions or responses have been taken by the Company?	
3. Impact Assessment(examples are given but not exhaustive): - Business impact including availability of services - Impact on stakeholders– affected retail/corporate customers, affected participants including operator(s), settlement institution(s), business partners, and service providers, etc. - Financial and market impact – Trading activities, transaction volumes and values, monetary losses, liquidity impact, company run, etc. - Regulatory and Legal impact	
4. Chronological order of events: Date of incident, start time and duration	



Incidents Form

Escalations done including approvals sought on interim measures to mitigate the event, and reasons for taking such measures	
Channels of communications used (e.g. email, internet, SMS, press release, website notice, etc.)	
Rationale on the decision/activation of BCP and/or DR.	
5. Root Cause Analysis(RCA):	
Factors that caused the problem/ Reasons for occurrence, Cause and effects of incident	



Incidents Form

Interim measures to mitigate/resolve the issue, and reasons for taking such measures.	
Steps identified or to be taken to address the problem in the longer term. List the remedial measures/corrections affected (one time measure) and/or corrective actions taken to prevent future occurrences of similar types of incident	
6. Date/target date of resolution _____ (DD/MM/YYYY).	

Note: All fields are REQUIRED to be filled unless otherwise stated.