نموذج (١/١٠/٧٠٠١/١)

بسم الله الرحمن الرحيم

البنك المركزي الأردني
CENTRAL BANK OF JORDAN

الرقم : ١٠/١ ٣٣٤٤

التاريخ : ١٨/٢/١٤٢٦هـ

الموافق : ٢٠٠٥/٣/٢٨م

تحية طيبة وبعد ،،،

الموضوع: مبادئ إدارة مخاطر العمل المصرفي الإلكتروني
(Risk management principles for electronic banking)

في ظل قيام العديد من البنوك المرخصة بالمملكة بتقديم الخدمات المصرفية عبر الوسائل الإلكترونية، وفي ضوء أن هذه الخدمات تؤدي إلى رفع مستوى المخاطر التي تواجه البنوك وبالأخص المخاطر الاستراتيجية والمخاطر التشغيلية ومخاطر السمعة والمخاطر القانونية، فإن ذلك يتطلب من البنوك ضرورة تطوير وتعزيز مستوى إدارتها للمخاطر بشكل عام ولمخاطر العمل المصرفي الإلكتروني ولمخاطر تكنولوجيا المعلومات بشكل خاص، وفي هذا السياق فقد قامت لجنة بازل للرقابة المصرفية بإصدار ورقة تتضمن إطارا عاما لإدارة هذه المخاطر تحت عنوان مبادئ إدارة مخاطر العمل المصرفي الإلكتروني، وفيما يلي المبادىء العامة التي تضمنتها ورقة بازل المشار إليها أعلاه والصادرة في تموز / ٢٠٠٣ ، منوهين إلى أنه إضافة لهذه المبادىء فإن على البنوك اتخاذ أي إجراءات إضافية تراها مناسبة بحيث تضمن السيطرة المحكمة على هذه المخاطر:-

أولاً : مسؤوليات مجلس الإدارة والإدارة العليا في البنك:-

١- يقع على عاتق مجلس الإدارة والإدارة العليا إنشاء نظام فعال لإدارة مخاطر العمل المصرفي الإلكتروني والاستمرار بتحديثه وتطويره بحيث يشمل تحديد عمليات المساءلة والضوابط الواجب استخدامها للسيطرة على هذه المخاطر.

ص.ب. ٣٧ • عمان ١١١١٨ الاردن • هاتف ٤٦٣٠٣٠١ • برقيا بنكمركزي / عمان • فاكس ٤٦٣٨٨٨٩، ٤٦٣٩٧٣٠، ٤٦١٣٣٠٨

٢- على مجلس الإدارة والإدارة العليا الاستمرار بمراجعة المواضيع الرئيسية المتعلقة بالإجراءات والضوابط المستخدمة في السيطرة على مخاطر العمل المصرفي الإلكتروني والمصادقة على أي تعديلات عليها.

٣- على مجلس الإدارة والإدارة العليا العمل على إنشاء نظام وآلية لإدارة خدمات الجهات الخارجية (**Outsourcing relationships**) المتعاقد معها بغرض دعم عملية تقديم خدمات العمل المصرفي الإلكتروني والاستمرار في تطوير ذلك.

ثانياً : <u>الضوابط الأمنية</u> :-

١- على البنك استخدام الوسائل والتقنيات المناسبة بغرض تحديد هوية العملاء والتأكد منها عند استخدامهم الخدمات المصرفية الإلكترونية وضمن الصلاحيات الممنوحة لكل منهم.

٢- على البنك استخدام وسائل وتقنيات التحقق من الخدمات المصرفية المنفذة بوسائل إلكترونية وبما يضمن تحقيق المساءلة وعدم الإنكار (**Accountability and non-repudiation**).

٣- على البنك التأكد من استخدام الضوابط المناسبة وبما يضمن تحقيق فصل المهام ضمن أنشطة العمل المصرفي الإلكتروني وقواعد البيانات والأنظمة التطبيقية العائدة لها.

٤- على البنك التأكد من وجود آلية فعالة لضبط عمليات النفاذ إلى أنظمة العمل المصرفي الإلكتروني وقواعد البيانات والبرامج التطبيقية العائدة لها وحسب الصلاحيات الموافق على منحها للمستخدمين بهذا الخصوص.

٥- على البنك التأكد من وجود آلية فعالة تعمل على ضمان تكاملية (**Integrity (complete and accurate)**) البيانات والمعلومات والسجلات العائدة للعمليات المصرفية الإلكترونية.

٦- على البنك التأكد من وجود سجلات تدقيق (Audit trails) للعمليات المصرفية الإلكترونية مع توفير الحماية اللازمة لهذه السجلات بما يضمن تكامليتها (Integrity (complete and accurate)).

٧- على البنك استخدام الضوابط اللازمة للحفاظ على سرية المعلومات المنقولة و/او المخزنة عبر الوسائل الإلكترونية والعمل على تفعيلها وبما يتناسب وطبيعة وحساسية هذه المعلومات.

ثالثاً : إدارة مخاطر السمعة والمخاطر القانونية:-

١- يتوجب على البنك عند تقديم خدمات مصرفية عبر الإنترنت توفير المعلومات اللازمة واستخدام الوسائل التقنية المحكمة وتوعية عملائه بشكل مستمر عن كيفية التأكد من هوية البنك على الإنترنت.

٢- على البنك استخدام الوسائل المناسبة للتأكد من التزامه بالمتطلبات القانونية للولاية القضائية في الدولة التابع لها حيثما وجد.

٣- على البنك امتلاك المقدرة الفعالة لوضع وتنفيذ خطط لاستمرارية العمل (Business continuity plans) بشكل يؤدي إلى توفير الخدمات المصرفية الإلكترونية وبما يتناسب واستراتيجيته وسياساته بهذا الخصوص.

٤- على البنك تطوير خطط و إجراءات فعالة للتعامل مع الحوادث (Incident response plans) بغرض احتواء تلك المشاكل والأحداث غير المتوقعة والتقليل من آثارها بما في ذلك محاولات الاختراق الداخلي والاختراق الخارجي لأنظمة العمل المصرفي الإلكتروني.

وتفضلوا بقبول فائق الاحترام ،،،

المحافظ

د.أمية طوقان