QNB

مجموعة QNB
بيان الأمن السيبراني

جدول المحتويات

ملخص الوثيقة

النطاق/ التغطية	QNB مجموعة
تاريخ الإصدار	نوفمبر 2025
النسخة	1.0

1. التزامنا بالأمن السيبراني

تلتزم مجموعة QNB بحماية المعلومات الشخصية والمالية لعملائها. نحافظ على بيئة تشغيل آمنة ومرنة، مدعومة بأنظمة قوية مصممة للحماية من التهديدات السيبرانية. يضمن إطارنا الأمني الشامل خصوصية بيانات العملاء وأمانها، بينما تتمتع بنيتنا التحتية لتكنولوجيا المعلومات بالأمان والمرونة.

2. سياسات الأمن والحوكمة لدينا

- تُحدد لجنة الأمن السيبراني للمجموعة وتراقب تطبيق إطارنا لحوكمة أمن تكنولوجيا المعلومات والأمن السيبراني، بما في ذلك الاستراتيجية والسياسات والضوابط والقدرات والميزانية والمهارات والأدوار والمسؤوليات على مستوى المجموعة. يرأس اللجنة الرئيس التنفيذي للمجموعة، بينما يشغل رئيس قطاع العمليات للمجموعة منصب نائب رئيس اللجنة. تضم اللجنة أيضاً رئيس قطاع الأعمال للمجموعة، ورئيس قطاع المخاطر للمجموعة، ونائب رئيس تنفيذي أول- تكنولوجيا المعلومات، ونائب رئيس تنفيذي- أمن المعلومات. يقدم رئيس قطاع أمن المعلومات للمجموعة تقارير رسمية منتظمة عن الأمن السيبراني إلى لجنة الأمن السيبراني للمجموعة، حيث يتم تسليط الضوء على التهديدات والتطورات، مع التوصية بإجراءات التخفيف المناسبة. بدورها، ترفع لجنة المخاطر السيبرانية للمجموعة تقاريرها إلى لجنة إدارة المخاطر التابعة للإدارة التنفيذية للمجموعة (لجنة على مستوى مجلس الإدارة) على أساس ربع سنوي.
- تتم مراجعة وتحديث سياسات وإجراءات الأمن السيبراني في QNB بانتظام لضمان توافقها مع المتطلبات التنظيمية المعمول بها، وأفضل ممارسات القطاع، والأطر المعترف بها مثل مقاييس المعهد الوطني للمعايير والتكنولوجيا (NIST).
- يتم إجراء المراجعات من قِبل فرق الأمن السيبراني، والانضباط، والمخاطر التشغيلية، والتدقيق الداخلي.
- يلتزم البنك بتحديد أي تهديدات أو ثغرات أمنية محتملة وتقييمها والاستجابة لها على الفور.

3. كيف نستعد للتهديدات السيبرانية؟

- أنشأ QNB نموذجاً تشغيلياً أمنياً شاملاً يُحدد هياكل حوكمة واضحة لإدارة جميع المخاطر المتعلقة بالأمن السيبراني بفعالية.
- يستثمر البنك باستمرار في التقنيات المتقدمة للكشف عن التهديدات السيبرانية المتطورة ومنعها والحماية منها.
- يعمل مركز مخصص للعمليات الأمنية على مدار الساعة طوال أيام الأسبوع، ويراقب الوضع باستمرار بحثاً عن أي نشاط غير طبيعي، ويضمن الاستجابة السريعة للحوادث.
- يقدم رئيس قطاع أمن المعلومات إحاطة دورية للقيادة التنفيذية للبنك، حيث يوفر رؤىً آنية حول التهديدات السيبرانية الناشئة وتدابير التخفيف الاستراتيجية.
- تُجرى اختبارات اختراق دورية وتمارين الفريق الأحمر لتقييم فعالية الرقابة وتحديد نقاط الضعف المحتملة.
- يخضع جميع موظفي QNB لتدريب سنوي إلزامي للتوعية بالأمن السيبراني للحفاظ على ثقافة أمنية قوية في جميع أنحاء المؤسسة.
- يحافظ QNB على خطط شاملة للتعافي من الكوارث واستمرارية الأعمال لضمان توافر الخدمة والمرونة التشغيلية، حتى في حالة حدوث اضطرابات كبيرة.

4. عمليات التدقيق والشهادات المستقلة

- حصل QNB على شهادات واعتمادات معترف بها دولياً، مثل ISO/IEC 27001 (إدارة أمن المعلومات)، ومعيارSOC 2 Type 2، و PCI DSS (معيار أمن بيانات قطاع بطاقات الدفع) للوفاء بالتزاماتنا تجاه العملاء والجهات التنظيمية.
- تُجرى عمليات التدقيق هذه بانتظام للحفاظ على الشهادات.
- تؤكد هذه الشهادات التزام QNB بالحفاظ على الامتثال للمعايير العالمية، وتُظهر حرص البنك على حماية بيانات عملائه من خلال تقييمات مستقلة دقيقة.

5. ملخص:

تلتزم مجموعة QNB التزاماً راسخاً بالأمن السيبراني. نستخدم أحدث التقنيات، ونطبق سياسات أمنية فعّالة، ونقدم تدريباً إلزامياً للموظفين، ونُجري تقييمات مستقلة لضمان الحماية المستمرة لأنظمة QNB ومعلومات عملائه.

بنك قطر الوطني (ش.م.ع.ق)
صندوق بريد 1000، الدوحة، قطر
هاتف: 2444 4425 974+
فاكس: 3753 4441 974+

qnb.com