QNB Cyber Security Statement

TABLE OF CONTENTS

Summary Profile

Scope/Coverage	QNB Group
Publication Date	November 2025
Version	1.0

1. Our Commitment to Cyber Security

QNB Group is committed to protecting the personal and financial information of our clients. We maintain a secure and resilient operating environment, supported by robust systems designed to safeguard against cyber threats. Our comprehensive security framework ensures that customer data remains private and secure, while our IT infrastructure is secure and resilient.

2. Our Security Policies and Governance

- Our Group Cybersecurity Committee (GCSC) defines and monitors the implementation of our IT security and cybersecurity governance framework, including strategy, policies, controls, capabilities, budget, skills, and roles and responsibilities across the Group. The GCSC is headed by the GCEO, with the Group Chief Operating Officer as the Vice-Chairman. The Committee also includes the Group Chief Business Officer, Group Chief Risk Officer, SEVP - Information Technology and EVP - Information Security Officer. The Group Chief Information Security Officer (CISO) provides regular formal cybersecurity reports to the GCSC, highlighting threat intelligence trends and recommending mitigation measures. The GCSC, in turn, reports to the supervising Group Management Risk Committee (board level committee) on a quarterly basis.
- QNB's cybersecurity policies and procedures are regularly reviewed and updated to ensure alignment with applicable regulatory requirements, industry best practices, and recognized frameworks such as NIST standards.
- Reviews are performed by the Cybersecurity, Compliance, Operational Risk and Internal Audit teams.
- The bank is committed to promptly identifying, assessing, and responding to any potential security threats or vulnerabilities.

3. How We Prepare for Cyber Threats

- QNB has established a comprehensive Security Operating Model that defines clear governance structures to effectively manage all cybersecurity related risks.
- The bank continuously invests in advanced technologies to detect, prevent, and defend against evolving cyber threats.
- A dedicated Security Operations Center (SOC) operates 24/7, continuously monitoring the environment for anomalous activity and ensuring rapid incident response.
- The Chief Information Security Officer (CISO) provides regular briefings to the bank's executive leadership, offering timely insights on emerging cyber threats and strategic mitigation measures.
- Periodic penetration tests and red team exercises are conducted to evaluate control effectiveness and identify potential vulnerabilities.
- All QNB employees undergo mandatory annual cybersecurity awareness training to maintain a strong security culture across the organization.
- QNB maintains comprehensive disaster recovery and business continuity plans to ensure service availability and operational resilience, even in the event of significant disruptions.

4. Independent Audits and Certifications

- QNB holds internationally recognized certifications and attestations such as ISO/IEC 27001 (Information Security Management), SOC 2 Type 2 and PCI DSS (Payment Card Industry Data Security Standard) to fulfil our customer and regulatory obligations.
- These audits are performed on a regular basis to maintain the certifications.
- These certifications affirm QNB's commitment to maintaining compliance with global standards and demonstrate the bank's dedication to protecting client data through rigorous independent assessments.

5. In Summary:

QNB Group is deeply committed to cybersecurity. We leverage advanced technologies, enforce robust security policies, provide mandatory staff training, and conduct independent assessments to ensure continuous protection of QNB systems and customer information.

Qatar National Bank (Q.P.S.C.)
P.O Box 1000, Doha, Qatar
Tel: +974 4440 7777
Fax: +974 4441 3753

qnb.com