بنـــك الريـــــان
ALRAYAN BANK

DATA PRIVACY & PROTECTION POLICY STATEMENT

1. Purpose, Scope & Policy Governance

Protecting customer and stakeholder data remains a core component of AlRayan Bank 's governance and operational resilience framework. Underpinning these efforts, ARB has established a robust Information Security Policy, within which the Data Privacy and Protection Policy is embedded.
This policy applies to all business lines, subsidiaries, employees, contractors, third-party service providers, and all information assets of the Bank, whether processed in physical or digital form. The policy establishes requirements for the protection and processing of personal information, including stakeholder rights, identification and registration of personal information assets, control of data processors and third parties through contractual requirements, and procedures related to breach reporting, access, update, objection, withdrawal of consent, and right to be forgotten.

2. Regulatory Alignment & Standards Reference

AlRayan Bank's data privacy and protection framework is designed in alignment with:

- Qatar's Personal Data Privacy Protection Law (Law No. 13 of 2016).
- Qatar Central Bank Technology Risk Circular.
- National Information Assurance (NIA) Standard.
- ISO/IEC 27001:2022.
- PCI DSS v4.0.1.

The Bank and its subsidiaries monitor regulatory developments across all jurisdictions in which it operates and adjusts its privacy framework accordingly.

3. Information Security Governance

This policy is owned by the Group Chief Risk Officer (GCRO), supported by the Head of Legal, and is subject to oversight and approvals from the Board Risk & Compliance Committee, ensuring strong top-level governance. A dedicated Security Steering Committee is actively involved in governance matters, alongside the Head of Information, Cyber and Physical Threat Management, who oversees the implementation of security controls and threat mitigation strategies. These comprehensive structures and high-level responsibilities demonstrate AlRayan Bank 's commitment to maintaining the highest standards of data protection and information security, reinforcing trust and confidence amongst its customers and stakeholders.
AlRayan Bank 's information security governance framework provides for:

- **Board-level oversight** through the Board Risk & Compliance Committee, which reviews cybersecurity risks, incidents, and strategy at least quarterly.
- **Executive accountability** through the Group Chief Risk Officer (GCRO) and the Head of Information, Cyber and Physical Threat Management, who acts as the Bank's Chief Information Security Officer (CISO) equivalent.
- A **dedicated Security Steering Committee** comprising senior management that meets quarterly to review security posture, emerging threats, and investment priorities.
- **Regular reporting to the Board** on cybersecurity metrics, incident trends, and program effectiveness.

4. Information Security Policy Summary

AlRayan Bank maintains a comprehensive Information Security Policy that:

- Applies to all employees, contractors, third parties, and all information assets of the Bank.
- Establishes a **risk-based approach** to identifying, protecting, detecting, responding to, and recovering from information security threats, aligned with the Qatar NIST Cybersecurity Framework.
- Defines mandatory standards for **access control, identity management, network security, endpoint protection, application security, and cloud security**.
- Is **reviewed and updated at least annually**, with interim updates triggered by material changes in the threat landscape or regulatory requirements.
- Is subject to **independent external audit annually**.

5. Data Collection, Minimization & Retention

AlRayan Bank adheres to the policy requirements for personal information to be identified and recorded in an information register, processed under defined data controller and data processor responsibilities, protected through appropriate technical, physical, and contractual controls, and subject to periodic oversight, while also supporting stakeholder rights such as access, update, objection, withdrawal of consent, and right to be forgotten.

AlRayan Bank retains personal data in accordance with applicable legal and regulatory requirements and only for as long as necessary to fulfil the purposes for which the data was collected. Upon expiry of the applicable retention period, personal data is securely deleted, destroyed, or anonymized in line with the Bank's data retention and information governance policies.

Additionally, the Bank maintains policies and procedures governing the retention, storage, and destruction of data, guaranteeing that information is retained only for as long as necessary for legitimate business, legal, or regulatory purposes.

6. Consent Policy for Secondary Use of Data

AlRayan Bank does not rent, sell, or disclose personal data to third parties except where necessary to facilitate banking transactions, deliver services, or comply with applicable legal and regulatory obligations. The Bank is committed to ensuring that any sharing of information is conducted in a secure and controlled manner, consistent with its data protection and confidentiality standards.

ARB has terms and conditions accepted by customers prior to any use or sharing of personal data for purposes beyond those for which it was originally collected, including marketing, analytics, or any secondary commercial use.

7. Data Subject Rights

As outlined in the Data Privacy and Protection Policy, ARB is committed to safeguarding the rights of individuals in relation to their personal data. These rights, as defined within the Bank's policy framework, ensure that customers and other data subjects have clear mechanisms to access, review, rectify, and request deletion of their personal information, subject to applicable legal and regulatory obligations.

8. Privacy-Enhancing Technologies

AlRayan Bank employs privacy-enhancing technologies, including data encryption at rest and in transit, pseudonymization and anonymization techniques, access-control mechanisms, and data loss prevention (DLP) tools to minimize the risk of unauthorized access, disclosure, or misuse of personal data. The Bank regularly evaluates and adopts emerging privacy-enhancing technologies as part of its continuous improvement program.

9. Data Breach Prevention, Response & Notification

AlRayan Bank addresses data breaches through a robust policy framework comprising its Information Security Policy, Information Classification Policy, and Data Privacy and Protection Security Policy. In the event of a breach, the crisis management team is responsible for promptly notifying relevant authorities. All staff and contractors must log breaches in the operational risk management system, strengthening accountability across the organization. Furthermore, vendors are contractually required to adhere to AlRayan Bank 's policies, reinforcing consistent standards for data protection and breach response.

AlRayan Bank conducts annual independent audits of its information security management system and data protection controls, complemented by quarterly internal vulnerability assessments and penetration testing, to validate the effectiveness of controls and ensure compliance with applicable standards and regulations.

10. Audit & Assurance Program

AlRayan Bank 's audit and assurance program for information security and data protection consists of:

- Annual independent external audits of the information security management system (ISMS), conducted by accredited certification bodies.
- Quarterly internal vulnerability assessments across all critical systems and infrastructure.
- Quarterly penetration testing of externally facing and internally critical applications.
- Continuous monitoring via the Bank's Security Operations Centre (SOC) for real-time threat detection.
- Annual PCI DSS compliance assessments by qualified security assessors.
- Results of all audits and assessments are reported to the Security Steering Committee and the Board Risk & Compliance Committee.

11. Data Protection Programs for Suppliers & Business Partners

AlRayan Bank's Data Privacy and Protection policy formally extends to all suppliers and business partners. Third-party engagements are subject to appropriate due diligence, contractual safeguards, and ongoing monitoring to ensure alignment with the Bank's information security, privacy, and data handling standards.

All suppliers and business partners handling personal data on behalf of AlRayan Bank are contractually required to maintain their own data protection policies that meet or exceed ARB's standards. AlRayan Bank conducts periodic inspections, including on-site and remote audits, to verify

supplier compliance with data protection requirements. Non-compliance triggers remediation plans and, where appropriate, escalation measures including contract termination.

12. Information Security Management System Certifications

AlRayan Bank 's achievement in securing ISO/IEC 27001:2022 certification for its IT and operational risk management system stands as a testament to the Bank's dedication to world-class information security standards. Furthermore, the successful audit and certification under Payment Card Industry Data Security Standard (PCI DSS) Version 4.0.1 highlight ARB's unwavering commitment to protecting sensitive payment card data, ensuring robust safeguards across all systems. These prestigious certifications not only demonstrate ARB's proactive approach to cybersecurity but also reinforce the Bank's reputation for exceptional security and operational resilience within the financial sector.

AlRayan Bank's ISO/IEC 27001:2022 certification covers certain critical processes of the Bank, including digital channels and data centers. The Bank targets maintaining certification coverage of at least 80% of all owned operations, in line with international best practice.

13. Employee Training & Awareness

Recognizing that employee awareness is a critical component of effective data protection, AlRayan Bank delivers mandatory annual Information privacy and data security training to all employees, including contractors, supplemented by role-based modules tailored to specific responsibilities and risk exposures. The Bank also promotes ongoing awareness through regular internal communications and updates covering emerging cyber risks, evolving regulatory requirements, and industry best practices.

Among AlRayan Bank 's recent training initiatives, a collaborative awareness workshop was delivered in partnership with the National Cyber Security Agency. This program focused on the principles of data classification and emphasized the importance of compliance with the National Information Assurance (NIA) standard. The workshop aimed to raise cybersecurity awareness across the Bank's workforce, enhance understanding of regulatory obligations, and strengthen AlRayan Bank 's overall compliance posture. By equipping employees with practical knowledge and reinforcing the criticality of safeguarding both the Bank's and clients' information, this initiative supports the ongoing protection of sensitive data and operational resilience.

In addition to the aforementioned initiatives, AlRayan Bank recently conducted a specialized training program in collaboration with Microsoft, focusing on strengthening cybersecurity and raising IT employees' awareness of best practices in IT security and cloud network protection. The workshop covered strategies for countering cyber threats, with particular emphasis on safeguarding the Bank's systems and data assets from evolving risks. Through practical sessions and expert-led discussions, the training aimed to familiarize staff with the latest tools and techniques in cybersecurity, ensuring that ARB's IT workforce is well-equipped to identify, mitigate, and respond to cyber incidents effectively.

Training coverage and completion rates are tracked and reported to the Security Steering Committee on a quarterly basis. The Bank targets a 100% completion rate for mandatory annual information security and privacy training across all employees and contractors.

14. Quantitative Key Performance Indicators

AlRayan Bank discloses the following key performance indicators to provide stakeholders with transparent, quantitative evidence of the effectiveness of its data privacy and information security programs:

Metric	Disclosure
Data security breaches	In 2025, AlRayan Bank recorded **0** material data security incidents, of which **0** required regulatory notification.
Customers affected by breaches	**0** customers were affected by data security incidents in 2025.
Penetration tests conducted	**24** penetration tests were conducted in 2025.
Vulnerability assessments	**4** quarterly vulnerability assessments were completed in 2025.
ISO 27001 certification scope	Certification covers **100%** of security operations.

These metrics are reviewed and updated annually and are reported to the Board Risk & Compliance Committee.

15. Awards & External Recognition

AlRayan Bank is proud to announce the successful completion of its compliance requirements for the National Information Assurance (NIA) standard, officially obtaining the NIA Certificate of Compliance. This achievement marks ARB as only the second bank in Qatar to secure this prestigious qualification, underscoring its commitment to rigorous data protection and information security standards. The certification recognizes ARB's dedication to maintaining robust cybersecurity controls and reinforces the Bank's position as a leader in safeguarding client and organizational data within the region