Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports Qatar National Data Classification Policy Compliance

Comprehensive Data Protection and Governance Through Integrated Security Architecture

The National Data Classification Policy V3.0, established by Qatar's National Cyber Security Agency (NCSA) in May 2023, requires all Qatari government organizations and critical sector entities to implement standardized data classification practices. The policy mandates a unified five-tier classification system (C0-C4) for government entities and a minimum four-tier system for non-government organizations to protect data confidentiality, integrity, and availability. Organizations must establish internal classification policies, appoint Chief Data Officers, and complete implementation within six months of the policy's publication. Noncompliance risks include cybersecurity vulnerabilities, regulatory violations, and potential national security impacts, as the policy aligns with Qatar's Personal Data Privacy Protection Law and Right to Access Information Law. Organizations must submit detailed risk management plans to NCSA for any policy deviations. Kiteworks supports compliance with this policy through comprehensive data classification, protection, and life-cycle management capabilities that map directly to the policy's technical requirements.

Data Protection Through Double Encryption and Zero-trust Architecture

Qatar's National Data Classification Policy requires organizations to implement state-specific security controls for data in transit, at rest, and in use, while maintaining confidentiality, integrity, and availability based on classification levels. The policy creates a comprehensive security framework that protects data throughout its entire life cycle. Kiteworks delivers this multi-state protection through an integrated security architecture. For data at rest, the platform employs double encryption at both file and disk levels with customer-controlled keys. All data in transit receives TLS 1.3/1.2 encryption protection, while data in use is secured through SafeVIEW's watermarked viewer and SafeEDIT's possessionless editing. The hardened virtual appliance includes an embedded network firewall, web application firewall, and intrusion detection system operating under zero-trust principles. This security stack maintains data confidentiality through access controls, integrity through audit logging, and availability through high-availability configurations.

Solution Highlights

- Double encryption
- Customer-controlled keys
- CISO Dashboard
- Zero-trust architecture
- SafeVIEW
- SafeEDIT
- SIEM integration

Life-cycle Management and Data Governance With CISO Dashboard and Automated Controls

Qatar's National Data Classification Policy requires organizations to manage data throughout its complete life cycle while enabling Chief Data Officers (CDOs) to implement and oversee comprehensive data governance programs. The policy mandates organizations to track, control, retain, and securely delete data while maintaining visibility and accountability across all data interactions. Kiteworks empowers CDOs and organizations to meet these requirements through integrated life-cycle management capabilities. The platform's CISO Dashboard provides comprehensive visibility into all data interactions, while detailed audit logs track content access, modifications, and sharing. Role-based administration with separation of duties enables proper governance, complemented by automated retention policies and time-based access controls for life-cycle enforcement. Version control maintains data integrity, while secure deletion capabilities ensure proper data disposal. The system's SIEM integration and customizable reporting tools help CDOs monitor compliance, evaluate technology effectiveness, and demonstrate program success to stakeholders.

Kiteworks' platform supports organizations required to comply with Qatar's National Data Classification Policy V3.0. The platform's hardened virtual appliance architecture delivers multilayered protection across all data states through double encryption, zero-trust principles, and secure viewing capabilities. The CISO Dashboard enables Chief Data Officers to implement and monitor classification policies while maintaining complete visibility over data interactions. Automated controls manage retention, access, and secure deletion throughout the data life cycle. The integration of role-based administration, audit logging, and SIEM capabilities creates a robust compliance framework that maps directly to the policy's requirements for data protection and governance. Kiteworks helps organizations ensure ongoing adherence to Qatar's data classification mandates through its integrated security and management features.