Kiteworks

COMPLIANCE BRIEF

How Kiteworks Supports Qatar NIAS 2.1 Data-level Compliance

Secure Content Communications and Governance for Qatar's Information Assurance Standard

The Qatar National Information Assurance Standard (NIAS) Version 2.1 is a comprehensive framework developed by the National Cyber Security Agency (NCSA) to regulate data assurance and security within Qatar. This standard affects all organizations operating in Qatar, especially those handling sensitive or classified information, including government agencies, critical infrastructure operators, financial institutions, and healthcare providers. NIAS covers a wide range of security domains, from risk management and data classification to incident management and cryptographic security. Organizations must classify their information assets according to the National Data Classification Policy and implement baseline security controls, with additional measures for higher sensitivity levels. The standard became effective in May 2023, coinciding with the release of the National Data Classification Policy v3.0. Noncompliance can result in significant consequences, including regulatory penalties, loss of government contracts, reputational damage, and increased vulnerability to cyber threats. The Kiteworks platform offers robust features to support organizations in achieving and maintaining compliance with NIAS 2.1. Here's how:

Data Classification Label via Content-based Risk Policy Framework and Role-based Access Controls

The Data Classification Label domain mandates a comprehensive data labeling methodology for organizations to manage and protect their information assets effectively. It requires organizations to serve as labeling authorities, rate assets according to confidentiality levels (C1 to C4), default to 'Internal' labeling, and establish a system supporting the "Need-to-Know" principle. Kiteworks addresses these requirements through its content-based risk policy framework, which enables precise asset classification aligned with IAP-NAT-DCLS ratings. The platform allows configuration based on various attributes like folder path, sensitivity labels, file type, and creator, corresponding to the C1 to C4 confidentiality ratings. Kiteworks can be set to label assets as 'Internal' by default, fulfilling the standard's requirement. Additionally, role-based access controls and the least-privilege principle support the "Need-to-Know" requirement, preventing unauthorized disclosure. This enables organizations to maintain effective control over their data classification and access.

Solution Highlights

- Role-based access controls
- Double encryption
- CISO Dashboard
- SIEM Integration
- SafeVIEW

Personnel Security With Encryption at Rest and in Transit

The Personnel Security domain focuses on ensuring staff awareness of security responsibilities and implementing controls to mitigate human-related risks. It requires organizations to manage personnel information securely, prevent unauthorized disclosures, restrict access rights, and update access when roles change. Kiteworks' encryption at rest and in transit, along with detailed audit logging, secures personnel information in compliance with data privacy laws. The SafeVIEW file viewer and DLP scanning prevent unauthorized disclosures and information misuse. Kiteworks implements role-based access controls and the principle of least privilege, limiting user access to job-specific requirements. The platform's integration with LDAP and Active Directory enables automatic user management, including prompt access right updates during role changes or employment termination. These features allow organizations to maintain strict control over personnel information security, effectively mitigating risks associated with the human element in information management.

Logging and Security Monitoring Enabled by Comprehensive Audit Logs and CISO Dashboard

Comprehensive logging and monitoring practices are required withing the Logging and Security Monitoring domain to identify unauthorized access, detect privilege abuse, and protect sensitive information. It requires continuous monitoring, 24/7 surveillance for critical infrastructures, logging of all activities related to C2 and above classified information, and retention of logs for at least 120 days. Kiteworks addresses these requirements through advanced logging and monitoring capabilities with detailed audit logs of all activities and supports real-time monitoring via the CISO Dashboard. It integrates with SIEM systems for 24/7 monitoring of critical infrastructure and sensitive data. Kiteworks logs all system interactions, protecting logs with strong encryption and strict access controls. The platform offers configurable log retention periods, allowing organizations to keep logs for 120 days or longer. Detailed audit logs capture essential activity details, facilitating incident reconstruction and forensic analysis.

Data Retention and Archival Supported With Double Encryption and Content-based Risk Policy Framework

Establishing appropriate retention periods and security controls for information throughout its life cycle is the focus of the Data Retention and Archival domain. It requires organizations to ensure confidentiality, integrity, and availability of retained data, maintain data classifications in archives, and keep archiving technology current. Kiteworks addresses these requirements through multiple features. The platform implements double encryption (file-level and disk-level) for data at rest and encryption in transit, coupled with strong access controls. This approach ensures the confidentiality, integrity, and availability of retained data, extending to backup and recovery processes. Kiteworks' content-based risk policy framework maintains data classifications in archived states, applying consistent security measures based on these classifications. The platform's advanced data management features support modern archiving practices, while regular system updates keep data storage and recovery capabilities current and effective. This comprehensive approach allows organizations to securely maintain their information assets for defined future purposes.

Kiteworks offers a comprehensive suite of features that align with the Qatar National Information Assurance Standard (NIAS) Version 2.1 requirements. The platform's content-based risk policy framework and role-based access controls support effective data classification and protection. Robust encryption measures, both at rest and in transit, coupled with detailed audit logging, ensure secure management of personnel information. The CISO Dashboard and integration with SIEM systems enable real-time monitoring and 24/7 surveillance of critical infrastructure. Kiteworks' double encryption and advanced data management features address data retention and archival requirements, maintaining data classifications and security measures throughout the information life cycle. By implementing Kiteworks, organizations are supported in meeting NIAS 2.1 compliance standards, mitigating security risks, and protecting sensitive information assets. This holistic approach to data security and compliance positions organizations to confidently operate within Qatar's regulatory framework.

Kiteworks

October 2024

www.kiteworks.com