Kiteworks

GUIDE

Kiteworks' Data-layer Guide to Qatar National Information Assurance Standard Compliance

Securing Sensitive Data With NIAS 2.1

Introduction

The Qatar National Information Assurance Standard (NIAS) Version 2.1 is a comprehensive framework designed to regulate and govern data assurance and security in organizations within the State of Qatar. Developed by the National Cyber Security Agency (NCSA), this standard aims to provide organizations with the necessary foundation and tools to implement a robust Information Security Management System. The NIAS impacts all organizations operating within Qatar, particularly those that handle sensitive or classified information, government agencies, critical infrastructure operators, financial institutions, healthcare providers, and any organization dealing with personal data or information crucial to national security is required to comply.

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

The standard is built upon the National Data Classification Policy and covers a wide range of security domains, including but not limited to: Security Governance, Risk Management, Third Party Security Management, Data Classification, Change Management, Personnel Security, Incident Management, Business Continuity Management, Access Control, Cryptographic Security, and Physical Security. To comply with the NIAS, organizations must first classify their information assets according to the National Data Classification Policy. They are then required to implement baseline security controls as specified in the standard, with additional controls necessary for assets classified at higher sensitivity levels.

The NIAS is enforced by the NCSA, and organizations are required to undergo certification to demonstrate compliance. The standard became effective upon its publication in May 2023, coinciding with the release of the National Data Classification Policy v3.0. The Assurance Standard maintains that organizations are fully responsible for adopting and implementing the standard, and that the NCSA does not take responsibility for any damages related to uninformed decisions in adopting and implementing the standard or actions outside its scope. Given the comprehensive nature of the standard and its alignment with Qatar's cybersecurity strategy, noncompliance could potentially result in significant consequences that might include regulatory penalties, loss of government contracts, reputational damage, and increased vulnerability to cyber threats. Additionally, in the event of a security breach, noncompliant organizations may face more severe legal and financial repercussions. Organizations seeking exceptions or deviations from the standard must communicate with the NCSA through official correspondence, providing justifications, risk assessments, and management plans. The NCSA, in coordination with sector regulators where applicable, will assess these exception requests.

This guide showcases how Kiteworks can support global organizations looking to be compliant with the Qatar National Information Assurance Standard.

The Kiteworks Secure File Sharing and Governance Platform

The Kiteworks Private Content Network empowers organizations to share sensitive content with trusted parties by email, file sharing, file transfer, and other channels at the highest levels of security, governance, and compliance while maintaining full visibility and control over their file sharing activities. The Kiteworks platform provides:

Protection of Unstructured Data

Kiteworks provides comprehensive protection for unstructured data through its advanced content firewall and zero-trust file sharing capabilities that ensures sensitive unstructured data remains secure throughout its life cycle, whether at rest or in transit across various communication channels.

Governance and Compliance

Kiteworks reduces compliance risk and cost by consolidating advanced content governance capabilities into a single platform. Whether employees send and receive content via email, file share, automated file transfer, APIs, or web forms, it's covered.

Simplicity and Ease of Use

Kiteworks offers a user-friendly interface that simplifies secure file sharing and collaboration, enabling users to easily send, receive, and manage sensitive content without compromising security. The platform's intuitive design and seamless integration with existing workflows ensures high user adoption rates and minimizes the learning curve for organizations implementing robust data protection measures.

The Kiteworks Platform and Qatar National Information Assurance Standard

Data Classification Label [DL]

This domain provides a high-level data labelling methodology for all Organizations for the purpose of understanding and managing data and information assets about their level of classification. The domain explains the methodology and the processes for effective data labelling. The rationale for labelling information assets per their classification levels is to ensure the Organization and the designated users of the information assets will be able to correctly identify and adequately allocate resources for the protection of the information assets.

Domain Requirements	Kiteworks Solution
DL 1. *Serve as a labelling authority for the data and information that it collects or maintains. DL 2. *Rate all information assets in accordance with [IAP-NAT-DCLS]. All assets rated with a Confidentiality rating of C1, C2, C3, or C4 SHALL be suitably marked the data label of Internal, Restricted, Secret or Top Secret respectively. DL 3. *By default, label information assets as 'Internal' unless they are specifically for public release or consumption or rated to a higher confidentiality level. DL 4. Establish the data labelling system to support the "Need-To-Know" requirement, so that information will be protected from unauthorized disclosure and use.	Kiteworks supports compliance through its robust content-based risk policy framework. This system enables organizations to effectively classify and manage their information assets in accordance with the IAP-NAT-DCLS ratings. Kiteworks allows for the configuration of asset classification based on various attributes such as folder path, sensitivity labels, file type, and creator, aligning with the standard's confidentiality ratings of C1 to C4 (Internal, Restricted, Secret, or Top Secret). The platform can be set to label information assets as 'Internal' by default, unless specified otherwise, meeting the standard's default labeling requirement. In addition, role-based access controls and least-privilege principle defaults support the "Need-to-Know" requirement, ensuring that information is protected from unauthorized disclosure and use. This comprehensive approach to data labeling and access control enables organizations to serve as effective labeling authorities for their collected and maintained data.

Personnel Security [PS]

The objective of this domain is to ensure that personnel (staff, vendors, contractors, and others) deployed with the Organizations are aware of their security responsibilities and that suitable controls are in place to mitigate risks arising out of human element.

Domain Requirements	Kiteworks Solution
PS 3. *Obtain, manage, and retain information related to personnel with due care and due diligence, in line with the requirements for handling Personal Information as specified in the Personal Data Privacy and Protection Law. PS 7. Ensure that adequate controls are in place to prevent personnel (employees, vendors, contractors, and visitors) from making unauthorized disclosures, misusing or corrupting information as per Organization security policies. PS 8. Ensure that users access rights are restrictive to the information they need to fulfill their job requirements as per least privilege and need to have principles. PS 12. *Ensure that a change request from the HR department is generated when a change of duties or termination of contract of an employee, contractor or third party occurs. This ensures that employees, contractors and third parties return Organization assets and physical & logical access are amended/removed as appropriate.	Kiteworks' robust data protection features, including encryption at rest and in transit, access controls, and detailed audit logging, ensure that personnel information is managed and retained securely, aligning with data privacy laws. The platform's multi-layered security approach, featuring SafeVIEW file viewer and DLP scanning, effectively prevents unauthorized disclosures and information misuse. Implementation of role-based access controls and the principle of least privilege ensures that user access rights are strictly limited to job-specific requirements, adhering to the 'need-to-have' principle. Kiteworks' integration capabilities with LDAP and Active Directory facilitate automatic user management, including prompt updates to access rights when roles change or employment is terminated. This comprehensive set of features enables organizations to maintain tight control over personnel information security, mitigating risks associated with the human element in information management.

Incidents Management [IM]

An information security incident is an event that impacts on the confidentiality, integrity, or availability of an information system or network, through an act that contravenes prescribed security policy and or applicable laws or regulations. For the purposes of this standard, an incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. This standard intends to provide a reference for the Organization's management, administration, and other technical and operational staff to facilitate the development of information security incident management capability, and to be used for preparation for, detection of, and response to information security incidents.

Domain Requirements	Kiteworks Solution
IM 2. Establish an information security incident response capability, based on the [IAP-NAT-DCLS] which can make a periodic risk assessment (from threat, vulnerability, and asset value) of data, processes, systems and networks in accordance with this Information Assurance Standard. IM 3. *Define procedures to detect, evaluate and respond to incidents. IM 7. Co-ordinate with NCSA to create a repository of incidents in the Organization.	Kiteworks' comprehensive logging and monitoring capabilities, including an Intrusion Detection System (IDS) and anomaly detection, provide a strong foundation for establishing an effective information security incident response capability. These features enable real-time alerts and detailed audit logs, facilitating quick detection, evaluation, and response to potential incidents. The system's SIEM integration further enhances incident management capabilities, allowing for rapid assessment of threats, vulnerabilities, and asset values. Kiteworks doesn't directly coordinate with NCSA, however, the standardized, detailed activity logs can be easily exported or integrated into external systems, supporting the creation of an organizational incident repository. This supports organizations as they effectively prepare for, detect, and respond to information security incidents in alignment with the IAP-NAT-DCLS and the Information Assurance Standard.

Logging and Security Monitoring [SM]

The aim of this domain is to provide requirements for logging and monitoring to identify unauthorized data, application and resource access and to detect unauthorized changes or access privileges abuse.

Domain Requirements	Kiteworks Solution
SM 1. *Adequate set of technical control implementations, or processes exist for logging, identification and continuous monitoring of access, changes, command execution to, any/all information assets for protection of business sensitive information. SM 2. *Monitoring practices are established in accordance with criticality of the infrastructure, data, and applications. It is RECOMMENDED to provide a 7/24 monitoring for C3, I3 and A3 classified infrastructures and ensure that monitoring responsibilities are allocated as specified in clause PS 9, section 4-6, Personnel Security [PS]. SM 4. *They enable logging on all infrastructure and data processing equipment, and applications that are associated with the access, transmission, processing, security, storage, and/or handling of information classified with a confidentiality rating of C2 and above. SM 5. They classify all security logs with a confidentiality rating of C3, while application and system logs SHALL be classified in accordance with the confidentiality rating of the system. SM 6. Logs containing Personal Information have appropriate privacy protection measures in place, in accordance with the Proposed Information Privacy & Protection Legislation. SM 7. *These logs are retained for a minimum of hundred and twenty (120) days and a maximum depending on criticality assessments and sector specific laws and regulations. SM 8. Organizations MUST enable audit logging or log capture, to record date, time, authentication activity with unique user and system identifiers, including all failure or change actions, further including commands issued and output generated to provide enough information to permit reconstruction of incidents and move system to its original state.	Kiteworks' comprehensive logging and monitoring capabilities provide a solid foundation for identifying unauthorized access and detecting privilege abuse. The system maintains detailed audit logs of all activities, supports real-time monitoring through the CISO Dashboard, and integrates with SIEM systems for continuous, 24/7 monitoring of critical infrastructure and sensitive data. Kiteworks logs all system interactions, regardless of data classification, ensuring comprehensive coverage for information rated C2 and above. While not explicitly classifying logs as C3, Kiteworks treats all logs as highly sensitive, protecting them with strong encryption and strict access controls. The system's configurable log retention periods, with the ability to retain logs for 120 days or longer, supports regulatory requirements. Additionally, detailed audit logs capture all essential activity details, providing the necessary information for incident reconstruction and forensic analysis. This comprehensive approach to logging and monitoring enables organizations to effectively protect their sensitive information assets and maintain compliance with the Standard's requirements.

Data Retention and Archival [DR]

The objective of the domain is to provide direction on setting up the retention period for information and the necessary security controls to protect information in its lifetime.

Domain Requirements	Kiteworks Solution
DR 2. *Data, which needs to be retained, is stored ensuring confidentiality, integrity and availability and that it can be accessed for defined future purposes. DR 4. Processes for backup, archival and recovery of data have corresponding procedures which ensure that the integrity and confidentiality of the data is retained. DR 5. *Archived data retains it classification markings and is secured accordingly. DR 6. The archiving technology deployed is regularly reviewed to ensure that it does not suffer from obsolescence and archived data is maintained in a state that allows successful recovery.	The platform employs double encryption (file-level and disk-level) for data at rest, along with encryption in transit and strong access controls, ensuring the confidentiality, integrity, and availability of retained data. These security measures extend to backup and recovery processes, maintaining data protection throughout its life cycle. The content-based risk policy framework enables the retention of data classifications even in an archived state, with security measures consistently applied based on these classifications. Kiteworks supports modern archiving practices through its advanced data management features. Regular system updates ensure that data storage and recovery capabilities remain current and effective, mitigating the risk of technological obsolescence. This comprehensive approach to data retention and archival enables organizations to securely maintain their information assets for defined future purposes.