Kiteworks

COMPLIANCE BRIEF

Saudi Arabia NDMO Standards Compliance Support With Kiteworks

Advanced File Sharing Platform Delivers Comprehensive Data Governance and Security

The Saudi Arabia National Data Management and Personal Data Protection Standards represent a comprehensive regulatory framework that governs data management practices across the Kingdom's public sector. Established by the National Data Management Office (NDMO) in January 2021 under Cabinet Resolution 292, these standards apply to all Saudi Arabian public entities, including government organizations, public authorities, and companies operating public utilities or national infrastructure. The regulation also extends to business partners handling government data within their operations. Organizations must implement 191 detailed specifications across fifteen data management domains according to a three-year phased approach, with Priority 1 specifications required by the end of year one, Priority 2 by year two, and Priority 3 by year three. The NDMO conducts annual compliance assessments using a binary pass-fail system for each specification, with noncompliance triggering potential ad hoc audits and corrective actions that can significantly impact organizational operations and reputation. Kiteworks' secure file sharing and governance platform provides essential capabilities that help organizations meet these stringent requirements across multiple compliance domains. Here's how:

Data Catalog and Metadata Domain—Comprehensive Metadata Management Through Consolidated Activity Logging and Automated Tracking

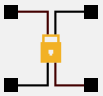
The Data Catalog and Metadata Domain establishes automated data catalog tools as the central reference point for organizational metadata, enabling effective access to high-quality integrated metadata that supports data discovery, understanding, and management. This domain requires entities to implement comprehensive technical controls including automated workflows for metadata population, updates, and quality management, along with processes for handling user annotations, tags, and trust certificates. Organizations must deploy automated notification systems, comprehensive audit log capabilities, and systematic version management while maintaining defined SLAs for issue remediation. Kiteworks addresses these requirements through its consolidated activity logging system that captures metadata with key-value pairs for every tracked activity, recording dates, users, activities, and IP addresses. The platform manages file metadata through versioning capabilities, comments, and both MIP and custom tags while supporting standard file metadata like creation dates and file types. Kiteworks exports reports via CSV and API integrations for metadata review and storage. The system provides automated notifications for real-time metadata change monitoring and implements certificate-based authentication with automatic OCSP/CRL handling.

Solution Highlights

Comprehensive audit logs

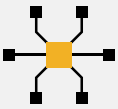
Multi-factor authentication

Role-based and attribute-based access controls



Least-privileged defaults

DevSecOps secure development



SIEM integration

Comprehensive audit capabilities track user activities without data throttling, while one-click updates through the hardened virtual appliance maintain current tool versioning with cryptographic verification and secure offline processes for air-gapped deployments.

Document and Content Management Domain—Secured Through Role-Based Access Controls and File Versioning

The Document and Content Management Domain controls the capture, storage, access, and use of documents and content stored outside relational databases, establishing processes for managing unstructured information, implementing digitization initiatives, and ensuring proper lifecycle management of organizational documents and multimedia content. Controls DCM.4.4 and DCM.4.5 require entities to implement comprehensive document management automation with integrated metadata publishing capabilities, mandating Document Management Systems with OCR functionality, document indexing, version control with change history tracking, secured access controls, global search capabilities, and workflow development tools. Kiteworks addresses these requirements through comprehensive file storage capabilities and file versioning that tracks document changes over time, directly supporting the version control mandate. The platform implements secured access to documents through role-based access controls featuring Owner, Manager, Collaborator, Downloader, and Viewer roles, meeting the secured access control specifications. Kiteworks offers collaboration capabilities that enable users to share folders and files while tracking who accessed or modified documents, supporting the workflow and change tracking requirements. The system's comprehensive audit logging captures document activities with date, user, activity, and IP address information, providing the tracking capabilities essential for document lifecycle management and compliance verification across the organization's document repositories.

Data Security and Protection Domain—Multi-Layer Security Through Advanced Authentication Systems and Embedded Threat Detection

The Data Security and Protection Domain encompasses comprehensive security measures including secure system design, identity and access management, information asset inventory, and security operations management to protect entity data from unauthorized access and disclosure. Organizations must implement robust authentication systems, maintain detailed asset inventories, and establish continuous monitoring capabilities. Kiteworks supports these requirements through multiple authentication methods including multi-factor authentication, SAML 2.0 SSO, certificate-based authentication, and integration with LDAP and Active Directory systems. Kiteworks implements comprehensive DevSecOps with "shift left" security practices, including security training, design reviews, secure code reviews, and automated testing throughout development. The platform provides role-based and attribute-based access controls with least-privileged defaults. Kiteworks maintains detailed inventories of all information assets through consolidated activity logs that track every data interaction, including uploads, downloads, and access permissions. Finally, operational security management is supported through comprehensive audit logging, real-time monitoring, intrusion detection systems, automated notifications, and continuous security information feeds to SIEM systems, enabling personnel to monitor, assess, and protect information assets effectively.

Kiteworks provides comprehensive support for Saudi Arabia's National Data Management and Personal Data Protection Standards through the Private Data Network. The solution addresses critical compliance requirements across multiple domains through consolidated activity logging that captures detailed metadata with key-value pairs for every system interaction, including dates, users, activities, and IP addresses. Role-based access controls with Owner, Manager, Collaborator, Downloader, and Viewer roles ensure secured document access while comprehensive file versioning tracks all document changes over time. Multi-factor authentication, SAML 2.0 SSO, and certificate-based authentication systems provide robust identity management capabilities. The platform's DevSecOps approach implements secure development lifecycle practices with automated testing and security reviews. Real-time monitoring, intrusion detection systems, and continuous SIEM feeds enable effective operational security management. Through these integrated capabilities, Kiteworks helps Saudi Arabian entities achieve compliance with the NDMO's stringent regulatory requirements while maintaining operational efficiency and data security.