Kiteworks

COMPLIANCE BRIEF

Kiteworks Supports Oman's National Data Governance and Management Policies

How Kiteworks Addresses Personal Data Protection, Access Governance, and Audit Traceability Requirements Across the MTCIT Framework

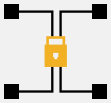
Oman's National Data Governance and Management Policies, published in 2024 by the Ministry of Transport, Communications, and Information Technology (MTCIT), establish a comprehensive framework for standardizing how government entities collect, manage, classify, share, and protect data across 13 active policy domains. This regulation applies exclusively to the Sultanate of Oman, mandating compliance across all government entities within the state's administrative apparatus, with private sector organizations subject to enforcement through their respective sector regulators. The framework spans public administration, digital services, open data initiatives, personal data protection, and data monetization. Government entities must begin implementing most policy domains immediately upon adoption, while the Personal Data Protection Policy takes effect 24 months after MTCIT's formal circulation date. Organizations that fail to meet compliance requirements risk assessment findings reported to the Council of Ministers, reputational damage, and operational disruption from inadequate data life-cycle controls. Kiteworks supports organizations working toward compliance with Oman's National Data Governance and Management Policies. Here's how:

Personal Data Protection and Secure Storage

Oman's Personal Data Protection Policy (PDP.1.4, PDP.1.5) requires controlling entities to implement security and organizational measures protecting personal data from unauthorized destruction, loss, alteration, disclosure, and hacking across all systems and storage media. Kiteworks addresses these requirements through a hardened virtual appliance that contains all necessary software within multiple protection layers, minimizing the attack surface available to external threats. The platform applies file and disk encryption at rest to reduce exposure from operating system-level intrusions and uses TLS 1.3 and TLS 1.2 with AES-256 encryption to secure data in transit. An embedded network firewall blocks all unused ports from outside traffic, while the embedded Web Application Firewall neutralizes known attack signatures, SQL injection attempts, and exfiltration activity. AI-based intrusion and anomaly detection continuously monitors the network and virtual appliance for suspicious activity, and customer-owned encryption keys ensure that neither Kiteworks staff nor outside actors can decrypt private data.

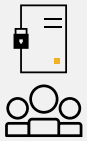
Solution Highlights

Hardened virtual appliance

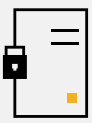


Strong double encryption

Embedded network firewall and web application firewall



Intrusion and anomaly detection with customer-owned encryption keys



Data Policy Engine with RBAC and ABAC

Kiteworks tagging

Consolidated audit log

Access Governance and Classification-Based Controls

The framework's Data Operations Policy (DO.1.4) and Data Classification Policy (CL.4.1) require entities to enforce role-based access controls aligned to data classification labels and maintain a structured register tracking assigned labels, supplementary markers, validity periods, and classification activity logs. Kiteworks enforces these requirements through its Data Policy Engine, which governs access to files and folders via pre-defined sharing roles including Owner, Manager, Collaborator, Downloader, Viewer, and Uploader, assigned separately from user profiles to support least-privilege access. The ABAC Data Policies capability allows Compliance Administrators to define dynamic rules based on data asset attributes, user attributes such as domain or profile, and the action the user attempts to perform. Kiteworks tags automatically classify files as they enter the system, enabling differentiated access controls for data labeled Confidential versus Internal Use Only. Time and expiration controls enforce retention durations tied to classification validity periods, directly supporting the register requirements under CL.4.1.

Audit Logs and Version-Controlled Traceability

Oman's Data Catalog Policy (DC.1.5, DC.2.5, DC.3.3), Data Architecture Policy (DA.1.9, DA.2.9), and Reference and Master Data Policy (RMD.1.7, RMD.2.7, RMD.3.5) require entities to maintain complete audit trails and version control mechanisms for all updates made to data dictionaries, business glossaries, data lineage records, architecture documents, data models, and reference and master data records. Kiteworks tracks all user, data, and system activities in a single consolidated audit log that can be searched, filtered, and sorted without throttling log volume, capturing all messages in full with original logging data intact. Log entries append immediately with no delay, enabling real-time monitoring and rapid response. File versioning provides per-file activity logs showing all changes including deletions, and individual file version histories support granular traceability of edits. Compliance administrators receive all data necessary for regulatory audits from this unified log, which records file edits, permission changes, and all actions on data assets, directly satisfying the version control and traceability requirements across multiple policy domains.

Kiteworks equips Oman government entities with the technical capabilities to support the National Data Governance and Management Policies across three critical compliance domains. The platform's hardened virtual appliance, layered encryption, and threat detection address the Personal Data Protection Policy's security mandates and prevent unauthorized access across all systems and storage media. The Data Policy Engine, with its role-based and attribute-based access controls and automated tagging, enforces the classification-aligned access requirements that the Data Operations and Data Classification policies demand. Kiteworks' consolidated audit log, real-time log capture, and per-file version histories satisfy the traceability and version control obligations spanning the Data Catalog, Data Architecture, and Reference and Master Data policies. Together, these capabilities give compliance administrators a unified, auditable, and defensible platform for meeting the framework's most demanding technical requirements.