Kiteworks

COMPLIANCE BRIEF

Compliance Support for Dubai Government Information Security Regulation

Technical Controls and Audit Capabilities for Dubai Government Compliance

The Dubai Government Information Security Regulation (ISR) Version 3.1 establishes comprehensive cybersecurity requirements for all Dubai Government Entities under Dubai Law No. 11 of 2014, administered by the Dubai Electronic Security Center. This mandatory framework impacts government agencies, contractors, consultants, and employees who handle sensitive government information across Dubai's public sector. Organizations must achieve compliance across thirteen critical security domains including governance frameworks, access controls, risk management, incident response, and cloud security protocols. Implementation deadlines align with the regulation's phased enforcement schedule, requiring immediate assessment and remediation planning. Noncompliance exposes entities to severe consequences including revocation of system access rights, disciplinary actions under UAE federal laws, and potential legal liability for data breaches or security incidents. Kiteworks supports Dubai ISR compliance through the Private Data Network (PDN) platform that addresses mandatory requirements across all multiple domains with detailed technical controls and audit capabilities. Here's how:

Data Protection and Classification Controls

Dubai ISR Domains 1, 6, 8, and 11 establish comprehensive data protection requirements including governance frameworks, operational security controls, secure development practices, and regulatory compliance mechanisms to safeguard information throughout its complete life cycle from creation through disposal. The regulation mandates proper data classification, encryption implementations, malware protection, and privacy controls. Kiteworks enables data protection through Microsoft MIP sensitivity labels and custom classification tags, ensuring proper data handling aligned with regulatory requirements, while double encryption for data at rest with customer-owned keys and TLS 1.3/1.2 for in transit protection of secure information throughout its life cycle. Advanced protection capabilities include SafeVIEW technology for secure document viewing with watermarks, SafeEDIT for possessionless editing, and embedded antivirus with mandatory malware scanning providing real-time file protection.

Solution Highlights

- **Access control management**
- **Administrative role segregation**
- **Comprehensive audit logs**
- **Customer-owned encryption keys**
- **Strong double encryption**

Access Control and Infrastructure Security

Domains 5, 7, and 13 of the Dubai ISR require comprehensive access control frameworks, business continuity capabilities, and cloud security protocols including multi-factor authentication, role-based permissions, backup strategies, and disaster recovery procedures. The regulation establishes requirements for least-privilege access principles, session management controls, environmental protection mechanisms, encrypted backup capabilities, and mandatory data residency restrictions within UAE boundaries for cloud deployments. Kiteworks implements access control through multiple authentication methods including multi-factor authentication, SAML SSO, certificate-based authentication, and Active Directory integration. Administrative role segregation includes eight default roles with customizable permissions supporting separation of duties requirements while session management encompasses timeout controls, lockout policies, and connection time restrictions with continuous activity monitoring. Business continuity support includes encrypted backup and storage strategies, media library protection with role-based access controls, and hardened virtual appliance deployment with multiple security layers protecting against environmental and cyber threats. Cloud security compliance features data residency controls that ensure critical information remains within UAE boundaries, customer-owned encryption keys provide data privacy control, and single-tenant private cloud architecture eliminates data sharing across databases, file systems, and operating systems while supporting periodic compliance audits and contractual requirement verification.

Data Tracking and Visibility Requirements

Dubai ISR mandates comprehensive data tracking capabilities across Domains 2, 3, 4, and 12 requiring detailed information asset management, continuous risk monitoring, incident evidence preservation, and performance measurement through integrated security dashboards and audit systems. The regulation establishes requirements for complete activity logging, SIEM integration capabilities, threat intelligence collection, and real-time security event monitoring to maintain visibility into all data interactions and security events. Kiteworks' tracking through detailed activity logging captures all data interactions including views, downloads, uploads, and modifications with complete audit logs for individual files and folders. The platform provides enterprise-grade SIEM integration with normalized data streams, optional embedded Managed Detection and Response capabilities with 24x7 monitoring, and comprehensive compliance reporting. Evidence-gathering capabilities include legal hold and eDiscovery access controls through a specialized Data Leak Investigator administrative role, while integrated security dashboards display cyber resilience status, audit findings, and risk assessments. Risky settings detection supports continuous security program assessment and regulatory compliance verification across organizational functions.

Kiteworks delivers support for the Dubai Government Information Security Regulation through the PDN that addresses critical requirements across multiple domains with integrated technical controls and audit capabilities. The platform enables organizations to maintain proper data governance through classification tags and role-based access controls while ensuring complete information life-cycle protection with double encryption, TLS 1.3/1.2 protocols, and advanced document-viewing technologies. Tracking and visibility capabilities include detailed activity logging, SIEM integration, and specialized administrative roles that support evidence gathering and incident response requirements. Access control implementation encompasses multiple authentication methods, session management controls, and administrative role segregation that enforces separation of duties across organizational functions. Business continuity support includes encrypted backup, media library protection, and hardened virtual appliance deployment with environmental protection mechanisms. Cloud security compliance features ensure critical data remains within UAE boundaries through single-tenant architecture, customer-owned encryption keys, and data residency controls that support regulatory compliance verification and periodic audit requirements.