Kiteworks

GUIDE

Kiteworks Compliance Guide to Dubai Government Information Security Regulation

Addresses Dubai ISR Requirements Across Domains

Introduction

The Dubai Government Information Security Regulation (ISR) Version 3.1 represents a comprehensive cybersecurity framework established under Dubai Law No. 11 of 2014 and Executive Council Resolution No. 13 of 2012, administered by the Dubai Electronic Security Center (DESC). This regulation establishes mandatory information security standards for all Dubai Government Entities (DGEs), including their employees, consultants, contractors, and visitors who handle government information in any form.

The regulation's primary purpose centers on ensuring the continuity of critical business processes while minimizing information security risks through prevention and mitigation of security incidents. The framework establishes government-wide regulatory approaches to information security, prescribes mechanisms to identify and prevent security compromises, and defines responsibilities for maintaining effective information security practices. The regulation operates as a technology-neutral framework, requiring each entity to develop specific policies and procedures aligned with the regulation's requirements.

The ISR applies universally to all Dubai Government Entities and encompasses all government information regardless of type or medium, including printed, electronic, and verbal communications. The regulation covers four critical components: storage systems (electronic devices and paper documents), infrastructure (hardware, applications, networks), organizational elements (processes and policies), and personnel (administrators, employees, visitors). Dubai Government maintains complete ownership of all processed information, with employees acting as temporary custodians under appropriate authorizations.

The framework organizes requirements into thirteen domains spanning governance, operational, and assurance classes. Governance domains establish high-level structural requirements for information security management. Operational domains provide technical and non-technical controls based on risk assessment results. Assurance domains ensure implemented solutions function as intended. Key domains include Information Security Management and Governance, Risk Management, Access Control, Operations Management, Business Continuity Planning, and Cloud Security.

Noncompliance with the regulation exposes entities to significant risks including unauthorized disclosure of critical information, provision of incorrect information to clients, and prevention of access to critical information. Entities and personnel found guilty of violations may face revocation of information system access rights and disciplinary actions under UAE and Dubai Government laws and policies. The regulation requires formal written requests to DESC for any exemptions, including detailed justification and risk assessment approval from top management.

مركز دبي للأمن الإلكتروني
DUBAI ELECTRONIC SECURITY CENTER

The ISR aligns with international information security standards from organizations including ISO, BSI, NIST, and ISACA, while incorporating distinctive requirements specific to Dubai Government contexts. The regulation establishes mandatory compliance with relevant UAE federal laws and Dubai regulations, including cybercrime legislation, electronic transaction laws, and data protection requirements. This comprehensive framework positions Dubai Government as a leader in proactive cybersecurity governance, protecting both government operations and citizen data through enforceable security standards.

The Kiteworks Secure File Sharing and Governance Platform

The Kiteworks Private Data Network empowers organizations to share sensitive data 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 firewall and zero-trust file sharing capabilities that ensure 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 data governance capabilities into a single platform. Whether employees send and receive data 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 data 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 The Dubai Government Information Security Regulation

Control Specifications	Kiteworks Solution
Domain 1: Information Security Management and Governance requires comprehensive governance frameworks with role-based access controls, incident response capabilities, compliance reporting systems, and administrative role segregation to ensure proper organizational security oversight and management accountability.	Kiteworks supports organizational security requirements through comprehensive administrative role segregation with admin roles that enable proper separation of duties. The platform provides automated risky settings detection with authorization workflows, ensuring security changes require proper approval. Role-based access controls (RBAC) and attribute-based access controls (ABAC) enable dynamic risk policy enforcement based on data attributes, user profiles, and attempted actions. Incident management capabilities include comprehensive compliance reporting, audit log generation for risk policy tracking, and real-time incident response support. The system's compliance summary reports provide oversight for various regulatory requirements, while the risky settings dashboard gives administrators visibility into security configurations and their current status across the organization.
Domain 2: Information and Information Assets Management mandates detailed information asset tracking with comprehensive logging systems, access controls, data classification tagging mechanisms, secure disposal procedures, data residency controls, and advanced data protection techniques including masking and synthetic data generation for sensitive information handling.	Comprehensive activity logging tracks all data interactions including views, downloads, uploads, and edits to deliver robust information asset management. Admin tracking capabilities provide detailed audit logs for individual files and folders, including version histories and change logs. The platform supports Microsoft MIP sensitivity labels and custom Kiteworks tags for proper data classification and handling requirements. Role-based access controls ensure least-privilege access with review capabilities through shared folder tracking and permission management. Data residency controls prevent critical data processing outside UAE boundaries through single-tenant private cloud architecture. Advanced data protection includes SafeVIEW for secure viewing with watermarks, SafeEDIT for possessionless editing, and comprehensive disposal controls for secure asset life-cycle management.
Domain 3: Information Security Risk Management focuses on systematic risk assessment requiring threat intelligence collection capabilities, comprehensive audit logging with SIEM integration, vulnerability analysis systems, and continuous security monitoring to identify and analyze information system threats and vulnerabilities effectively.	Kiteworks addresses risk management requirements through audit logging with SIEM integration capabilities, providing normalized and standardized security data streams. The platform offers embedded Managed Detection and Response (MDR) within an Enterprise subscription with 24x7 monitoring and automatic security updates. Compliance reporting features enable insider and outsider threat tracking with detailed behavioral analysis and communication monitoring. Log export capabilities support multiple SIEM and SOAR platforms through syslog and Splunk Universal Forwarder integration. Intrusion and anomaly detection logging captures security events including failed access attempts, file integrity monitoring, and network attack signatures. The system's threat intelligence capabilities automatically update security rules and provide real-time protection against emerging vulnerabilities and attack patterns.

Control Specifications	Kiteworks Solution
Domain 4: Incident and Problem Management establishes structured incident response requiring evidence preservation systems, legal hold capabilities, knowledge base development for threat tracking, incident documentation procedures, and coordinated response mechanisms to handle security breaches and suspicious activities systematically.	Comprehensive evidence-gathering capabilities including legal hold and eDiscovery access controls. The Data Leak Investigator (DLI) admin role provides specialized access to deleted files, emails, and activity logs for litigation support. The platform maintains complete audit logs with full message capture and immediate log entry creation, enabling real-time incident response. Threat-tracking capabilities include insider and outsider threat compliance reports with detailed behavioral analysis. The system's knowledge base functionality aggregates security incident data from multiple sources, supporting centralized threat intelligence and preventive action planning. Integration with external archiving tools and eDiscovery software ensures comprehensive incident evidence management and regulatory compliance support.
Domain 5: Access Control implements extensive authentication and authorization controls including multi-factor authentication systems, role-based permissions management, session timeout controls, remote access security protocols, mobile device management capabilities, wireless access controls, and comprehensive user lifecycle management processes.	Kiteworks implements access control through multiple authentication methods including credential-based, certificate-based, multi-factor authentication, SAML SSO, Kerberos, OAuth, and LDAP/Active Directory integration. The platform provides specialized user management for internal and external users with least-privilege permissions and automated onboarding/offboarding. Administrative role segregation includes eight default roles with customizable permissions supporting separation of duties requirements. Session management features include timeout controls, lockout policies, and connection time restrictions. Remote access security encompasses VPN client controls, authentication requirements, and comprehensive activity monitoring. Mobile computing support includes encryption, remote wipe capabilities, and device management controls. Wireless access management provides proper authentication controls and continuous monitoring of unauthorized access attempts.
Domain 6: Operation, Systems and Communication Management covers comprehensive operational protection requiring embedded malware protection systems, network security with encryption protocols, comprehensive logging and monitoring systems, data center security controls, email protection gateways, and media handling procedures to ensure secure daily operations.	Embedded antivirus capabilities with mandatory malware scanning and real-time file protection support operational security. Network security features include TLS 1.3/1.2 encryption in transit, zero-trust architecture with default-deny policies, and embedded Web Application Firewall (WAF) protection. The platform provides comprehensive logging and monitoring with clock synchronization, fault logging across all system levels, and secure log file protection against unauthorized changes. Email protection mechanisms ensure confidentiality, integrity, and availability through the Email Protection Gateway (EPG) with rule engines, encryption enforcement, and automatic disclaimer stamping. Media handling controls include proper labeling, storage security, and transit protection mechanisms.

Control Specifications	Kiteworks Solution
Domain 7: Business Continuity Planning addresses organizational resilience through backup encryption capabilities, comprehensive testing procedures, media library protection with proper storage controls, environmental protection mechanisms, and recovery verification processes to ensure operational continuity during disruptions and disasters.	Kiteworks supports business continuity requirements through backup and storage strategies with encryption capabilities for backups and archives. The platform provides media library protection with role-based access controls and continuous monitoring of storage resources. Environmental protection controls include hardened virtual appliance deployment with multiple security layers and protection against various threats. Physical media transit protection ensures secure handling during movement with proper accountability measures. The system's backup testing and restoration capabilities support periodic verification of recovery processes. Integration capabilities enable coordination with external disaster recovery systems and support continuity planning requirements through comprehensive data protection and availability measures.
Domain 8: Information Systems Acquisition, Development and Management focuses on secure development lifecycle requiring comprehensive encryption implementations, data masking capabilities, information leakage prevention controls, cryptographic key management systems, and application security measures throughout the development and deployment process.	Secure development requirements are enabled through encryption capabilities including TLS 1.3/1.2 for data in transit and double encryption for data at rest with customer-owned keys. The platform provides data masking and synthetic data capabilities through SafeVIEW technology that converts documents to static images with optional watermarking. Information leakage prevention includes Data Leak Investigator capabilities, legal hold controls, and eDiscovery integration. Embedded Web Application Firewall protection secures applications against attacks with zero maintenance requirements. The system supports secure processing of information with integrity controls and validation checks. Cryptography controls include Hardware Security Module (HSM) integration, FIPS 140-3 validated encryption options, and comprehensive key management capabilities for government and enterprise environments.
Domain 11: Compliance and Audit ensures regulatory adherence through comprehensive privacy protection mechanisms, data leak prevention systems, proper information asset handling procedures, disposal controls with documented processes, and privacy controls aligned with legal requirements and information classification schemes.	Kiteworks supports regulatory compliance through privacy protection mechanisms with role-based access controls that restrict and monitor access to personal and private data on a need-to-know basis. The platform provides data leak prevention capabilities through specialized administrative roles and comprehensive monitoring systems. Protection techniques include data masking, SafeVIEW watermarking, and synthetic data generation for secure sharing scenarios. Information asset protection encompasses proper storage, retention, and disposal controls with documented procedures for media library management. The system supports legal compliance requirements through comprehensive audit logs, policy controls, and integrated disposal mechanisms. Privacy controls include principle of least privilege implementation and comprehensive data-handling procedures aligned with information classification schemes.

Control Specifications	Kiteworks Solution
Domain 12: Information Security Assurance and Performance Assessment requires performance monitoring through integrated security dashboards, key performance indicator tracking, compliance summary reporting capabilities, comprehensive audit log management, real-time monitoring systems, and administrative reporting features for continuous security program assessment.	Security measurements capabilities are provided by integrated dashboards that display cyber resilience status, audit findings, and risk assessments. The platform combines security KPIs for periodic management review with risky settings detection and automated authorization workflows. Compliance summary reports show adherence to various regulations based on individual policy controls with audit log capabilities for risk policy tracking. Comprehensive audit log management includes SIEM feeds with cleaned, normalized, and standardized data streams. Log export capabilities support multiple business units through configurable syslog and Splunk feeds. Administrative reporting features provide built-in and custom reports with scheduling capabilities and CSV export options. Real-time monitoring enables immediate response to security events with comprehensive activity tracking and detailed audit logs.
Domain 13: Cloud Security establishes cloud-specific controls including data residency restrictions within UAE boundaries, single-tenant architecture requirements, customer-owned encryption key management, data portability mechanisms, service agreement specifications, and compliance monitoring capabilities for cloud service providers.	Kiteworks addresses cloud security requirements through data residency controls ensuring critical data remains within UAE legal boundaries with formal agreements preventing cloud service provider data ownership. The platform's single-tenant private cloud architecture eliminates data sharing with other customers across databases, file systems, and operating systems. Customer-owned encryption keys ensure complete data privacy control with protection against unauthorized access by staff or external actors. Data portability and continuity support includes comprehensive backup testing and restoration capabilities with periodic verification processes. Compliance monitoring capabilities enable periodic audits of security policies and contractual requirements with comprehensive reporting and verification mechanisms.

The information provided in this guide does not, and is not intended to, constitute legal advice; instead, all information, content, and materials available in this guide are for general informational purposes only. Information in this guide may not constitute the most up-to-date legal or other information. Add-on options are included in this guide and are required to support compliance.