Kiteworks

COMPLIANCE BRIEF

Public Companies Achieve Data Protection in Oman

Kiteworks Supports Key Requirements in the Capital Market Authority's Information Security Guidelines

Circular No. E/1/2022 is an information security guideline issued by the Capital Market Authority (CMA) for public joint stock companies in Oman. The guideline mandates the requirements to implement information security guidelines for public joint stock companies. The purpose of the guideline is to ensure that public joint stock companies in Oman have adequate measures in place to protect their information assets from unauthorized access, use, disclosure, disruption, modification, or destruction. The guideline is based on the Capital Market Law enacted by the Royal Decree No. 80/98 and the Electronic Transactions Law enacted by the Royal Decree No. 69/2008. The guideline covers various aspects of information security, including governance, risk management, access control, network security, application security, incident management, and business continuity management. The guideline is an important step toward enhancing the cybersecurity posture of public joint stock companies in Oman and protecting them from cyber threats as well as establishing baseline information to manage risks and ensure stakeholder confidence. Kiteworks supports key requirements within this guideline. Here's how:

Establish Robust Information Security Controls

The guidelines state that listed companies must implement core information security controls to protect confidentiality, integrity, and availability of data, including: access control policies to authorize user access and prevent unauthorized access; password management policies with strong password requirements; log management processes aligned with ISMS standards; data privacy measures to protect personally identifiable information; cryptography to secure sensitive data at rest, in use, and in transit; compliance with Omani regulations on data hosting; information security requirements in third-party contracts; physical and environmental security controls; incident response plans; business continuity and disaster recovery plans; security awareness training; and regular security monitoring, assessments, and testing. Companies must adopt an international ISMS standard aligned to their risk profile and business needs. The controls outline baseline requirements but companies should implement additional controls based on risk assessments. Kiteworks offers a robust set of capabilities that enable organizations to meet many of the information security guidelines outlined. For access control, Kiteworks provides granular folder permissions and integration with directory services to align with guidelines on implementing access policies and centralized identity management. Comprehensive, exportable logging with human-readable formats supports log management processes called for in the guidelines.

Solution Highlights

- **Unified access controls**
- **Strong encryption**
- **Real-time monitoring**
- **Secure mobile app**
- **Robust authorization**

Kiteworks also enables compliant password management through administrator-controlled password requirements and password history. For data protection, Kiteworks has strong AES-256-bit encryption for data in transit and at rest, aligning with cryptography guidelines. It also provides features like consent mechanisms, data portability, and configurable geographic data storage to support privacy and regulatory compliance guidelines. Breach notification capabilities further aid in complying with regulations. Kiteworks offers an on-premises private cloud option that enhances security by isolating systems and data within the customer's own infrastructure. Together, these capabilities in areas like access control, logging, encryption, consent flows, and data control provide a framework that can help companies satisfy core information security guidelines related to access management, data protection, regulatory compliance, logging, and system hardening. With its defense-in-depth approach spanning people, processes, and technology, Kiteworks allows organizations to securely collaborate and drive productivity while meeting rigorous security and compliance standards.

Manage Incidents and Monitor for Compliance in Real Time

Additionally, Circular No. E/1/2022 guidelines call for incident response plans enabling rapid containment and disclosure of cyber incidents based on severity. Prompt notification of affected parties is required for data breaches. Continuous security monitoring and regular assessments are also mandated to identify threats and vulnerabilities. Kiteworks helps organizations meet these requirements through extensive logging and auditing features. Its audit logs provide complete visibility into user activities across all system components. Logs can be analyzed in SIEM systems or Kiteworks' dashboard for real-time monitoring and early threat detection. Configurable alerts also notify administrators of potential incidents. Together, these capabilities facilitate swift incident investigation and disclosure by providing forensic audit logs and visibility into events. They support continuous oversight to identify threats early and enable regular assessments of vulnerabilities per the guidelines. With robust, unified visibility and monitoring capabilities, Kiteworks helps organizations implement effective incident response programs, continuously monitor their security posture, perform assessments, and comply with regulatory disclosure and notification mandates.

Manage and Control Changes to Data While Monitoring Workflow Procedures

Next, the document focuses on the centralized management of sensitive data and monitoring of access as well as the observation, monitoring, and reporting of workflow procedures. Kiteworks provides a unified platform enabling centralized data oversight and granular access controls. Kiteworks delivers centralized control over sensitive data through its single administrative console for managing policies, permissions, and configurations. This consolidates data security governance. Granular access control policies align with guidelines by implementing least-privilege access. Comprehensive audit logs support continuous monitoring of access and activities involving sensitive data. Logs provide complete visibility into user actions across all system components and channels. They create an immutable record that can identify policy violations or suspicious access. With robust access control policies and centralized auditing, Kiteworks enables coordinated data governance and ongoing monitoring of access. Its unified administrative console centralizes oversight, while granular access controls enforce need-to-know data access. Together with detailed activity logs, Kiteworks provides the capabilities called for in the guidelines for centralized data management, controlled access, and continuous monitoring. The platform integrates key data security components like access policies, logging, user management, and configuration. This consolidated approach to governing data and users supports centralized, consistent data protection.

Implement Strict Control and Preventative Measures to Prevent Data Leaks

Strict controls to prevent intentional or accidental unauthorized data sharing and leaks are also expressed within the document. Kiteworks has granular access controls and least-privilege policies to limit data access. Folder owners configure individual user permissions with role-based access rights and new users receive minimum permissions by default. Integration with data loss prevention (DLP) solutions enables data scanning to detect and block potential data leaks based on policies. File transfers and emails can be analyzed for sensitive data and restricted if they violate rules. Comprehensive activity logging provides an audit log of user actions, supporting leak investigation. Together, these capabilities limit the risk of both insider and accidental data sharing. Granular access controls enforce need-to-know data access. DLP integration actively detects and stops unauthorized sharing attempts. And auditing provides visibility into how leaks occurred if they arise. With layered controls spanning access, monitoring, and auditing, Kiteworks helps organizations implement strict preventive and detective controls to guard against unauthorized sharing and leakage of sensitive data across collaboration channels.

Secure Mobile App Boasts Encryption, Authentication, Remote Wipe, and More

Finally, the document and ensuing guidelines establish a need for companies to implement stringent security measures in mobile apps to protect sensitive data, including encryption, multi-factor authentication (MFA), access restrictions, and auditing. Kiteworks provides a robust set of capabilities to help secure sensitive data in mobile environments and comply with these requirements. Specifically, the Kiteworks mobile apps leverage AES-256-bit encryption to secure data at rest and TLS encryption for data in transit. Comprehensive auditing tracks all user activity within the app for investigatory and compliance purposes. Remote wipe allows admins to instantly sanitize apps and remove corporate data from lost or stolen devices. Kiteworks allows administrators to enforce geofencing by setting block-lists and allow-lists for IP address ranges. This feature can be used to restrict access to data based on the geographical location of the user, enhancing the security of sensitive data. Kiteworks provides the ability to configure a distributed system to store a user's data only in their home country. Facial or fingerprint recognition can be used as an additional layer of security set up by the administrator on a profile or individual level to access the Kiteworks mobile application. Together, these layered controls provide end-to-end security tailored for mobile access to sensitive data: encryption safeguards data at rest and in motion; MFA adds an extra layer of identity assurance; auditing creates an immutable audit log of access and usage; remote wipe protects data on compromised devices; and geofencing, biometrics, and session timeouts prevent unauthorized access. With defense-in-depth protections purpose-built for mobile collaboration, Kiteworks provides the comprehensive data security, access control, and auditing called for in the guidelines to help organizations securely enable mobility while preventing leakage of sensitive information.

Kiteworks provides integrated capabilities that help public companies in Oman comply with the Capital Market Authority's guidelines for robust data security and privacy. By delivering unified access controls, encryption, monitoring, and threat detection, Kiteworks enables organizations to implement layered protections around sensitive data, collaborate securely, respond swiftly to incidents, and maintain compliance with rigorous regulations. With its centralized platform and defense-in-depth approach spanning people, processes, and technology, Kiteworks is purpose-built to help Omani public companies manage risks, safeguard stakeholder trust, and achieve regulatory compliance as they secure sensitive data and drive secure collaboration.