Kiteworks

COMPLIANCE BRIEF

# Kiteworks Complies With ISO 27001, 27017, and 27018

## Protect Sensitive Data From Cyber Risk in Digital Communications

Kiteworks achieved three certifications in less than five months, a feat that most organizations take 6 to 12 months to accomplish. Enjoy the peace of mind that ISO has validated Kiteworks to effectively protect your sensitive data from cyber risk (ISO 27001), including when deployed as a cloud service (ISO 27017), and to shield your organization from damaging leaks of personally identifiable information (PII) as validated by ISO 27018. These certifications, along with the platform's single-tenant architecture, a library of compliance certifications, and multilayered hardening, further validate Kiteworks' ability to mitigate data risk with their content management system.

### Kiteworks: ISO-certified Protection for Confidentiality, Integrity, and Availability of Information

Certification in all three ISO levels validates Kiteworks protection across 175 controls. The 175 controls cover information security management that preserves the confidentiality, integrity, and availability of information by applying a risk management process. It also gives guidance on the framework for cloud computing environments. This includes additional controls surrounding security measures and implementation guidance, specifically applying to principles regarding the protection of PII in public clouds. ISO 27001 helps organizations to identify and protect their information assets and to establish a process for regularly reviewing and improving their information security program. ISO 27017 provides guidance on the specific security controls that should be in place when an organization is using cloud services. ISO 27018 provides guidance on how to apply the principles of the EU General Data Protection Regulation (GDPR) to the use of PII in cloud services. These three standards provide guidelines and best practices to ensure the security and privacy of information.

### ISO 27001: Certified Protection for Information Assets

ISO 27001 is a standard that provides guidelines for organizations to set up an information security management system (ISMS), reduce IS risk, and effectively manage the security of various assets, including financial information, intellectual property, employee details, and more. Kiteworks has demonstrated a commitment to its ISMS with investments in rigorous security governance, processes, and controls. Additionally, Kiteworks has enhanced its risk assessment and mitigation processes to meet ISO/IEC requirements and incorporate risk analysis into overall governance and institution of its security objectives for the organization. Reviewing and improving the security program is also an important aspect of the Kiteworks platform, which includes annual internal and external penetration testing, an ongoing bounty program, and audits for SOC 2, FedRAMP, and other regulations. Protecting information is an important aspect of ISO 27001, which is why Kiteworks includes perimeter protection that minimizes the external attack surface and an assume-breach architecture that slows attackers and rapidly alerts SecOps.

### ISO 27017: Achieving Cloud Security Through Private Data Network and Advanced Security Measures

The ISO 27017 standard provides guidelines for the management of information security in the cloud. To be ISO 27017 certified, an organization must develop and implement a formal ISMS that meets the requirements of the ISO 27017 standard. The ISMS should address the specific security risks associated with using cloud services and should include controls to mitigate those risks. It is designed to help organizations secure their sensitive information when using cloud services by providing guidance on the

selection, use, and management of cloud services. The Kiteworks Private Data Network boasts defense-in-depth security with built-in hardening, encryption of data, and zero trust between services. These features ensure that the company is well-equipped to manage the specific security risks associated with using cloud services and mitigate those risks.

## ISO 27018: Complete Protection for PII in Cloud Services

To be ISO 27018 compliant, an organization must develop and implement a formal ISMS to include controls to protect PII when using cloud services. Some of the controls to be ISO 27018 compliant are: encrypting PII in transit and at rest, implementing access controls, regularly testing the security of the cloud environment, establishing policies and procedures for the use of cloud services in relation to PII, selecting and evaluating cloud service providers carefully, and monitoring the security of the cloud environment. Kiteworks meets those requirements by offering services that protect PII. For instance, Kiteworks customers can respond to PII modification requests and retain sole ownership of encryption keys. Furthermore, Kiteworks uses encryption of PII at rest with TLS 1.2 and in transit with AES-256.

These certifications provide guidelines for information security management, protecting the confidentiality, integrity, and availability of information and for protecting PII in cloud computing environments. Kiteworks has demonstrated a commitment to its ISMS with investments in establishing improved security governance, processes, and controls, making it a leader in the field of data security and compliance. These certifications, along with the platform's single-tenant architecture, a library of compliance certifications, and multilayered hardening, further validate Kiteworks' ability to mitigate risk.