Kiteworks

COMPLIANCE BRIEF

Secure Saudi Data as a Trusted Compliance Partner

Kiteworks Supports NCA Data Cybersecurity Controls

The National Cybersecurity Authority (NCA) of Saudi Arabia has implemented stringent Data Cybersecurity Controls (DCC) to safeguard valuable physical and digital data. These controls mandate encryption, access controls, data retention policies, and regular auditing to maintain integrity and confidentiality. As part of the Kingdom's efforts to enhance cybersecurity resilience and ensure a robust national cybersecurity workforce, DCC compliance is compulsory for public and private sector organizations across banking, energy, healthcare, and other critical industries. Noncompliance can increase vulnerability to threats, data breaches, and legal consequences. Failing to adhere to DCC may incur penalties, loss of public trust, and reputation damage. Therefore, upholding DCC requirements is imperative for entities operating in Saudi Arabia to mitigate cyber risks and meet national data security standards. Kiteworks supports compliance. Here's how:

The Cybersecurity Governance domain covers conducting periodic reviews and audits, managing cybersecurity in human resources, and implementing awareness and training programs to ensure compliance with policies, laws, and data protection. Kiteworks' multilayered approach to protecting, monitoring, and removing data aids compliance through its robust access controls, principle of least privilege, encryption protections, activity logging, and administrative controls. It enables organizations to limit access, monitor user activities, and prove adherence to regulations. Features like granular access policies, DLP scanning, logs tracking all system and user actions, and administrative separation of duties facilitate audits. With configurable retention policies, detailed activity logs, and the ability to permanently erase files, Kiteworks gives organizations tools to meet deletion, privacy, and data security mandates.

The Cybersecurity Defense domain covers protecting systems and facilities, securing mobile devices, safeguarding data confidentiality and availability, enabling cryptography, securely disposing data, and securing printers and copiers. Kiteworks supports compliance through rapid patching via one-click updates, administrative controls and permissions limiting data access, and multiple data protection methods. Features like automatic updates, admin roles restricting activity, remote wipe for lost devices, SafeEDIT's dynamic watermarking, DLP integration to identify sensitive data, and DRM policies blocking downloads facilitate adherence to regulations. Together these capabilities allow organizations to quickly mitigate risks, monitor administrator actions, prove policy conformance, and safeguard sensitive information through layers of access limitations and data protections.

Solution Highlights

- Granular access controls
- Least-privilege principles
- Detailed activity logs
- Administrative controls
- Double encryption
- Intrusion detection

The Third-party and Cloud Computing Cybersecurity domain covers requirements for protecting assets when utilizing third-party services, including vetting employees, contractual data disposal commitments, justifying and documenting data sharing, verifying data hosting capabilities, requiring breach notifications, masking sensitive data, and imposing additional restrictions around consultancy services for strategic projects. Kiteworks facilitates third-party compliance through features like Enterprise Connect for external repository integration, predefined collaboration roles governing access, principles of least privilege, activity logging, intrusion detection, anomaly monitoring, data classification, and flexible policy assignment. Together these capabilities allow organizations to securely collaborate with partners, limit data exposure, detect suspicious activities, categorize sensitive assets, determine risk levels based on custom criteria, monitor user actions, and prove adherence to regulations related to third-party services and external sharing.

By enabling robust access controls, detailed activity logs, stringent data protections, and secure integrations, Kiteworks provides organizations the capabilities required to comply with Saudi Arabia's Data Cybersecurity Controls across governance, defense, and third-party security. With its multilayered approach upholding principles of least privilege and encryption by design, Kiteworks allows entities to limit data exposure, permanently delete unneeded files, detect attempted intrusions, mitigate risks, and prove adherence to DCC regulations safeguarding critical assets. As breaches incur steep penalties, selecting reliable technologies that meet national standards is key for organizations to avoid fines, prosecutions, and reputational damages. Kiteworks' layered controls facilitate audits while securing sensitive information, making it an ideal partner for maintaining cyber resilience and furthering the Kingdom's vision for a thriving digital future.

Kiteworks

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. The Kiteworks platform provides customers with a Private Content Network that delivers content governance, compliance, and protection. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.