Kiteworks

COMPLIANCE BRIEF

Empowering Secure Collaboration With ITSG-33 Compliance for Protected A and B Information

Strengthening Canadian National Security and Trust Through Kiteworks' Comprehensive Security Controls and Reliable Platform for Safeguarding Sensitive Data in Accordance With ITSG-33

Kiteworks and Protected A & B Information

Protected A and B are classifications in Canada's system for safeguarding sensitive information, where A represents data whose unauthorized disclosure may cause minor harm, and B denotes information that could cause serious harm if leaked. The Information Technology Security Guidance (ITSG-33), a security guideline aligned with international standards like the U.S. NIST SP 800-53, aids Canadian agencies in establishing comprehensive security measures for their IT systems and data. This framework outlines a catalog of security controls, organized into technical, operational, and management classes, specifically designed to protect such classified information. Ensuring compliance with these guidelines, particularly for Protected A and B information, is vital for national security, privacy protection, legal obligations fulfillment, and maintaining trust. The Kiteworks Private Content Network (PCN) provides public and private sector organizations a secure platform for sharing sensitive information with trusted third parties via email, file sharing, managed file transfer, SFTP, mobile, and more. Kiteworks is FedRAMP Authorized for Moderate Impact Level CUI and helps organizations comply with NIST 800-53, and thereby ITSG-33, by providing several features and functionalities:

Enhance Compliance and Safeguard Sensitive Data With Robust Technical Controls

Kiteworks delivers substantial value to organizations aiming to comply with ITSG-33 guidelines and secure Protected B information. The platform's central, role-based policies and access controls ensure that only authorized personnel can access sensitive data, integrating seamlessly with LDAP/AD and SSO/2FA/MFA for secure authentication. Detailed audit logs and records maintained by Kiteworks offer invaluable insights for administrative reporting, compliance audits, and threat detection, promoting swift remedial action. Advanced integrations with LDAP/AD, SSO/2FA/MFA, and authenticators like Google and Microsoft fortify user identification and authentication, reinforcing the security of sensitive data.

Solution Highlights

- Secure authentication and access control
- Zero-trust communication
- Robust firewalls
- Centralized control and configuration management
- Real-time monitoring and incident response

Moreover, Kiteworks provides a robustly protected environment with its hardened virtual appliance, implementing enterprise-grade encryption, network and web application firewalls, intrusion detection systems, file integrity monitoring, and zero-trust communication principles. This layered defense strategy safeguards system communications, upholding data protection during transmission and storage. In essence, Kiteworks ensures comprehensive security management, reinforcing compliance with ITSG-33 and the protection of sensitive data.

Reinforce Security Controls With Kiteworks' Comprehensive Platform

Kiteworks offers an all-encompassing platform tailored to meet diverse cybersecurity needs in accordance with ITSG-33 and the safeguarding of Protected B information. By providing centralized control over user access and security settings, the platform reinforces configurations management, thereby reducing the risk of unauthorized access or data breaches. Kiteworks also supports contingency planning via secure data backup and recovery options, facilitating business continuity in case of system failure or disaster. Incident response is streamlined with real-time monitoring and detailed logs, aiding compliance with incident notification and record-keeping requirements. The platform also protects sensitive data, whether at rest or in transit, through encryption. For physical and environmental protection, Kiteworks offers deployment options ranging from on-premises to private cloud solutions. Lastly, by continuously monitoring for potential threats, Kiteworks maintains the integrity of system and information, assuring the platform's security and reliability.

Effective Management Controls With Kiteworks' Comprehensive Approach

Kiteworks exemplifies a comprehensive approach to securing Protected B information in compliance with ITSG-33. Kiteworks undergoes meticulous security assessment and authorization by a Third Party Assessor Organization (3PAO), validating plans based on NIST 800-53 and performing annual audits for continued security assurance. Integral to Kiteworks' operation is its commitment to security-centered planning, ensuring compliance with industry standards like NIST 800-53 and FedRAMP Moderate, and encompassing vital areas such as vulnerability and configuration management. It further fortifies its platform by conducting regular risk assessments, thus proactively identifying and mitigating potential security threats. Kiteworks also emphasizes secure and reliable system and service acquisition, partnering with trusted providers to uphold the highest security standards. Through these stringent measures, Kiteworks ensures a robust, secure, and up-to-date platform that effectively safeguards sensitive data while meeting customer requirements.

Unlock the power of secure collaboration and protect your organization's sensitive information with Kiteworks. As Canada's system for safeguarding Protected A and B information becomes increasingly vital for national security, privacy protection, and legal obligations fulfillment, compliance with the Information Technology Security Guidance (ITSG-33) is paramount. Kiteworks, a FedRAMP Moderate Authorized platform, offers an all-encompassing solution that aligns with ITSG-33 and NIST 800-53 standards, ensuring comprehensive security controls for your classified data. With Kiteworks, you can effortlessly manage user access, enforce role-based policies, and integrate with LDAP/AD, SSO, and MFA for secure authentication. Robust encryption, audit logs, and advanced threat detection capabilities provide valuable insights for compliance audits and swift remedial action. Kiteworks' commitment to security-centered planning, risk assessments, and regular audits guarantees a robust and up-to-date platform. Safeguard your organization's sensitive information, meet compliance requirements, and maintain trust with Kiteworks. Take the first step toward secure collaboration by harnessing the power of Kiteworks today.