Kiteworks

Protect Customer Data With a Kiteworks-enabled PCN for FTC Safeguards Rule Compliance

Our platform offers a range of features and tools to help you implement and maintain the necessary safeguards to control the risks of exposure of customer information, and our commitment to security and compliance means you can trust us to help you protect your customers' personal and financial information.

Meeting the Safeguards Rule's Access Control Requirements With a PCN

One critical requirement of the Safeguards Rule is for financial institutions to implement and periodically review access controls, including technical and physical controls, to authenticate and permit access only to authorized users and to limit authorized users' access to only the customer information they need to perform their duties and functions.

The Kiteworks platform provides a range of features to help financial institutions protect and manage their content and communication, including granular content access controls, email policies with features like non-forwarding and auto-encrypt, and support for Microsoft MIP. The role-based permissions system allows financial institutions to control access to their content and tools based on the role of the user, and it offers features like file type filtering and account expiration dates to help secure access. The system includes a range of policies to help financial institutions secure and manage access to their account, including block and allow lists, geofencing, password security measures, and key rotation. The platform is designed to support the separation of admin duties and offers features like user management, app and system configuration tools, eDiscovery and analytics, and storage management tools to help financial institutions effectively manage and secure access to their sensitive customer content.

Managing Customer Data and Protecting Against Unauthorized Access

Further, the FTC Safeguards Rule requires financial institutions to identify and manage customer data in order to protect against unauthorized access.

The platform provides financial institutions with tools to organize and manage their information, including creating folders with customizable permissions and adding tags or metadata to files for easy classification. It also includes a file versioning feature to track changes and maintain transparent history of a file. User access controls allow institutions to specify who can access certain files and what actions they can take with them. Additionally, activity logs or audit trails can be used to monitor user activity for compliance purposes.

Protecting Customer Data in Transit and at Rest With Encryption

The Rule also requires financial institutions to protect customer information in transit and at rest through the use of encryption.

The Kiteworks platform uses various methods of encryption to protect customer data at rest and in transit. These include double encryption at the volume and file level, TLS for secure communication over networks, and SFTP encryption for data transfer between computers. Additionally, Kiteworks has received FedRAMP Moderate Authorization and undergoes annual audits to ensure compliance with various regulations and controls. Continuous monitoring and vulnerability scanning is also in place to identify and address potential security issues. Customers can benefit from compliance with a number of regulatory frameworks through Kiteworks' FedRAMP authorization.

Ensuring Secure Development and Testing of In-house and Externally Developed Applications

The safeguards rule additionally requires the adoption of secure development practices for in-house developed applications used to transmit, access, or store customer information, as well as procedures for evaluating and testing the security of externally developed applications used for the same purposes.

Kiteworks has a hardened virtual appliance designed to protect against application layer attacks and secure customer data. Its security features include an embedded network firewall and web application firewall, least-privilege access controls, minimized attack surface, AI-based anomaly detection, advanced intrusion detection and alerts, and zero-day threat blocking. Kiteworks also provides a unified system with visibility, tracking, and reporting across all major communication channels, including a unified audit log recording events like file access, modification, and sharing, as well as user activity. This centralized record can be used for various purposes such as tracking changes to files, monitoring user activity, troubleshooting issues, and demonstrating compliance with regulations or policies.

Additionally, the technology that enables Kiteworks customers to deploy a dedicated Private Content Network complies, itself, with the following requirements of the Safeguards Rule. For example:

Multi-factor Authentication

The rule requires multi-factor authentication (MFA) for any individual accessing any information system. Access to the Kiteworks system, as either an administrator or a user, can be set up with an MFA requirement that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. With Kiteworks, MFA takes the form of "something the user knows," in this case a password, along with "something the user has," in the case of Kiteworks, a digital token sent to a device such as a phone or computer.

Meeting Annual Penetration Testing and Vulnerability Assessment Requirements

Additionally, there is a requirement for annual penetration testing of your information systems and vulnerability assessments, including any systemic scans or reviews of information systems at least every six months and whenever there are material changes to your operations or business arrangements, and whenever there are circumstances you know or have reason to know may have a material impact on your information security program. The Kiteworks application development team follows secure development practices and incorporates "Shift Left and Extend Right" DevSecOps best practices in order to identify and prioritize vulnerabilities in the code during the development process and remediate them before deployment into production. In addition to these proactive measures, the Kiteworks appliance is hardened through continuous monitoring, "always-on" periodic penetration testing, and vulnerability assessments. To further ensure the security of the application, ongoing bounty programs and embedded WAF and firewall technology are used for continuous monitoring and remediation of potential threats in production. By utilizing these technologies and practices, Kiteworks is able to maintain the highest level of protection and continuously manage risk to the lowest possible level.

As outlined, it's easy to see why a Kiteworks-enabled Private Content Network offers a range of security measures to protect sensitive customer data and help financial institutions comply with the Safeguards Rule. Kiteworks is unequivocally the first choice for any financial institution looking to minimize risk and provide a secure platform for customer data within file and email data.