

# Kiteworks Preserves Data for eDiscovery

## Properly Identify, Collect, and Process Electronically Stored File and Email Data for eDiscovery Compliance

eDiscovery is a crucial aspect of modern litigation that involves identifying, collecting, reviewing, and producing electronically stored information (ESI). The process is governed by various rules and regulations, including the Federal Rules of Civil Procedure (FRCP), which mandate the preservation, collection, and production of ESI in legal proceedings. Compliance regulations vary depending on the jurisdiction and type of case, and include laws such as the Electronic Communications Privacy Act (ECPA), the Health Insurance Portability and Accountability Act (HIPAA), the Federal Trade Commission Act (FTCA), and state laws. Properly identifying, collecting, and producing relevant ESI is crucial in gaining a better understanding of the evidence in a case and being better prepared for trial.

Reduce compliance risk and cost by consolidating advanced data governance capabilities into the Kiteworks platform. Legal teams can perform legal holds for eDiscovery with all communication sent through Kiteworks, including the ability to send and receive data via email, file share, automated file transfer, and application programming interfaces (APIs). Streamline eDiscovery by monitoring, processing, and archiving communications centrally to preserve evidence and simplify legal hold.

## Identify and Protect Data

Kiteworks allows customers to track all files sent through Kiteworks and produce an immutable audit log showing all the metadata around who is sending and receiving information. Organizations can collect content communicated through all external channels, from file sharing, collaboration, and virtual data rooms, to email, forms, SFTP, MFT, and enterprise applications. Admins set granular policy controls like view-only access and watermarking to protect sensitive content and enforce compliance policies yet increase user productivity and collaboration as business owners easily manage content, folders, invitations, and access controls to data.

Kiteworks provides legal teams the ability to set policies for password complexity while allowing administrators to reset user passwords and enforce password changes during login. Kiteworks protects data via a hardened virtual appliance that is architected to reduce the number of potential vulnerabilities in its libraries and increase the attack complexity required to exploit them. An embedded network firewall and web application firewall (WAF), zero-trust access, and minimized attack surface all work to significantly reduce security risk. The Kiteworks Private Data Network also invokes multiple layers of protection to reduce the impact on confidentiality, integrity, and availability with AI-based anomaly detection, advanced intrusion detection and alerts, as well as zero-day threat blocking. This means better protection for private customer content and a stronger security posture in the face of advanced persistent threats.

## Automatic Data Review and Collection

The Kiteworks platform captures and logs events such as who accessed a file, at what time, from what location, and whether a file was modified, downloaded, viewed, or shared. Kiteworks customers can set up legal hold data collection and preservation automatically, guaranteeing integrity of evidence without the need for training or additional involvement. Plus, customers can integrate legal hold archives with eDiscovery systems via REST APIs. With the Kiteworks immutable audit log, customers can process and review all eDiscovery items for litigation and even fulfill chain-of-custody requirements with complete visibility and auditability of file activity. Reports can be customized to see live views of files tied to cases and trials, allowing legal teams to stay ready for any court date.

## Successful and Efficient Production

Kiteworks ensures successful production of eDiscovery content by first preserving all content securely, then collecting the necessary content, and finally producing the eDiscovery content when needed. Reports for eDiscovery content can be generated to properly pull all corresponding content within a designated date range containing all files, activities, and emails. From these reports, Kiteworks customers can securely download and email all content, enabling successful investigations by providing chain of custody with a full audit trail of all access, administrative, and transfer activities. When eDiscovery content is ready to be archived, customers can confidently export all content to archiving systems automatically via SMTP to archive each file, its corresponding version, emails, and all user activity.

Kiteworks provides advanced data governance capabilities that help legal teams reduce compliance risk and cost by centralizing the monitoring, processing, and archiving of communications. With the ability to track all files and produce an immutable audit log, Kiteworks enables organizations to identify and protect sensitive data, and set granular policy controls to enforce compliance policies. The platform also provides automatic data review and collection, ensuring the integrity of evidence. In addition, Kiteworks increases efficiency with automatic reports for eDiscovery content generation, secure downloads, and protected emails with large content attachments. With Kiteworks, legal teams can streamline the eDiscovery process, simplify legal hold, and stay ready for any court date.