Top 5 Ways Kiteworks Protects ITAR Critical Content for Government Contractors

International Traffic in Arms Regulations (ITAR) are a set of regulations implemented by the U.S. government to control the export and import of defense-related materials, services, and technologies. These regulations aim to protect U.S. national security and foreign policy interests by controlling the export of defense-related items, services, and information to foreign countries and entities.

1. Comprehensive Audit Logging for Streamlined Tracking

Comprehensive audit logging makes it simple and efficient to facilitate ongoing monitoring to run internal audits on ITAR-related file and email technical data. The administrative interfaces utilize logs for human-readable dashboards, as well as custom and standard reports. The platform provides user-friendly tracking displays so end-users can determine whether recipients have accessed, edited, or uploaded content via secure shared folders, secure email, or SFTP.

2. Enhance Data Security With Zero-trust Principles

Classifying and tagging technical data within Kiteworks is made efficient through integrations into Microsoft MIP tagging as well as any DLP classification system. Additionally, through the use of folder and user-based access policies, file and email technical data can be segmented and permissions assigned to secure content. Kiteworks leverages zero-trust principles, allowing organizations to define and enforce user access levels for all controlled unclassified information (CUI), and set policies for view-only access, watermarking, and more. This helps to ensure that sensitive data is protected, and access is granted only to those who need it.

3. Streamline Compliance With Secure Web Forms

Customers can leverage Kiteworks' secure web forms to get necessary authorizations before allowing ITAR-related technical data to leave their possession. With Kiteworks' secure web forms, customers and other external parties conveniently upload their sensitive information, while IT professionals set policies to protect the data and ensure regulatory compliance. Processing delays and compliance gaps due to incorrect and missing information become a thing of the past and uploads can flow seamlessly into automated or manual processes. With a straightforward, point-and-click authoring tool, admins quickly create secure web forms they can trust, knowing they use the security, role-based permissions and compliance policies enforced by the Kiteworks platform. This enables simple and secure submissions, which reduces errors and enforces security and compliance automatically with platform logs of all form submissions for full visibility in audits, reporting, CISO Dashboard, SIEM, and eDiscovery.

4. Ensure Compliance With Accurate Records

Additionally, reporting on the comprehensive audit logs enables customers to maintain 100% accurate records of all content. Kiteworks' audit logs serve the dual purpose of ensuring that an organization can investigate data breaches and provide evidence of compliance during audits. Our secure systems include all necessary logging to help serve as a forensics tool for any issues you may have, as well as a preventative tool to help you utilize the Kiteworks platform easily within your risk management positioning.

5. Protect Data With Anomaly Detection and User Authentication

And finally, anomaly detection and user authentication allow for immediate insight into unauthorized access. AI technology detects suspicious events, such as possible exfiltration, and sends an alert via email and the syslog. Through the platform's immutable audit logs, organizations can trust that attacks are detected sooner and maintain the correct chain of evidence to perform forensics. Since the system merges and standardizes entries from all implemented communication channels, Kiteworks' unified syslog and alerts save security operations center teams crucial time while helping compliance teams to prepare for audits.

The Kiteworks platform provides comprehensive governance and protection for government contractors to ensure ITAR compliance. It includes features such as secure web forms for easy data upload and reporting, compliant encryption in the cloud, and 24/7 content protection. Kiteworks also meets all security requirements listed in NIST 800-171 and FedRAMP for controlled unclassified information (CUI) protection. The platform enables organizations to define and enforce user access levels, set policies for view-only access and watermarking, and provides comprehensive logging and audit for efficient compliance.

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.

February 2023

www.kiteworks.com