



What Accellion FedRAMP-Authorization Can Do For Commercial Businesses

Accellion kiteworks is a FedRAMP Moderate authorized solution that enables both private and public sector organizations to securely share information with full control, visibility, and confidence.

As a FedRAMP-authorized cloud solution, U.S. Federal agencies have official validation that Accellion kiteworks is a superior solution for enabling Government employees to securely access and share sensitive information.

Government agencies however aren't the only beneficiaries of a FedRAMP-authorized solution. Many businesses in the private sector contract with government agencies and are strongly encouraged, and in some cases required, to use a FedRAMP-authorized solution to share information. Whether encouraged or required, using a FedRAMP-authorized solution to share sensitive information is a best practice.

Organizations that require the highest level of security or are required by the Federal Government to have a compliant security plan for sharing data can benefit from Accellion's turn-key FedRAMP offering, which meets all of the Government's security requirements for a FedRAMP Moderate authorized system. The Accellion FedRAMP solution has also been deployed to ensure ITAR compliance.

A FedRAMP Moderate authorized kiteworks solution can help other private sector businesses as well. Commercial businesses who require the highest level of data security to protect customer data, intellectual property, legal documents or other types of sensitive information, also have access to Accellion's FedRAMP Moderate authorized kiteworks solution.

Organizations using kiteworks have full control of their sensitive content: AES256 and FIPS encryption on all content in transit and at rest, encryption key ownership, AV and DLP scanning on file uploads and downloads, role-based permissions, and much more. In addition, kiteworks integrates with an organization's existing security infrastructure, including LDAP/AD, SSO, MFA, DLP, ATP, SIEM and more. Lastly, organizations have full visibility into where sensitive content is stored, who has access to it and what's being done with it. All file activity is auditable and allows organizations to demonstrate compliance with GDPR, ITAR, HIPAA, HITECH, FISMA, GLBA, SOX and other rigorous government regulations.

Accellion's FedRAMP Moderate authorized solution is available to Government agencies and commercial businesses in isolated environments on Amazon Cloud. Accellion has assembled a team of security and IT experts to support FedRAMP customers and, per FedRAMP requirements, this team is comprised of US citizens, based within the United States.

When commercial businesses choose Accellion's FedRAMP Moderate authorized kiteworks solution, they demonstrate to their partners and customers that data security is a top priority. And having FedRAMP Moderate authorization as a baseline set of security controls provides commercial businesses a distinct competitive advantage. It's a commitment to the highest level of content security.

A Brief Primer on Accellion and FedRAMP

The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The goal with FedRAMP is to help the Federal Government quickly, rigorously, and consistently assess the security capabilities of cloud solutions that are used or are being considered for use by federal agencies and ultimately increase cloud adoption across the Federal Government.

FedRAMP authorization requires an extensive application process involving thorough documentation of Accellion's security processes, assessments of related systems, creation of a System Security Plan, and training and certification of Accellion employees who have access to the FedRAMP environment. As part of the authorization process, Accellion had to achieve over 400 controls in personnel, IT, and physical security.

In order to retain FedRAMP Authorization status, Accellion undergoes continuous monitoring, vulnerability scanning, and annual audits of our controls. These audits are performed by a Third Party Assessment Organization (3PAO), which is also FedRAMP authorized.

Accellion kiteworks is available to Federal Government and commercial clients in isolated environments on Amazon Cloud. The kiteworks FedRAMP package features:

- Separate customer virtual private cloud (VPC) for all processing
- Dedicated servers
- Data isolated from all other customers
- Encrypted file storage and transfer with sole encryption key ownership
- Remote wipe for all mobile clients
- Reporting and audit trails
- Continuous monitoring for intrusions and other threats
 - Includes vulnerability and penetration scanning as well as rigorous, proactive remediation, plan of action and milestones for mediation tracking

These features, plus FIPS 140-2 Level 1 validation, enable organizations to comply with several industry and government regulations, including ITAR, SOX, HIPAA (with signed BAA), SOC2, PCI DSS Level 1, ISO27001, ANSSI, and CJIS.

For more information, please visit:
<https://www.accellion.com/fedramp>