Adobe Document Cloud security

Adobe Document Cloud is the only complete solution for achieving end-to-end digital transformation of your most critical document processes. Working with Adobe Acrobat DC, Adobe eSign services, web and mobile apps, and your business systems and processes—Document Cloud services help you deliver better customer experiences, accelerate business and compete more effectively.

The security of our customers is a priority for Adobe. We employ a set of security engineering practices and processes to build our products and services, and we respond to security issues as part of our data security protocols.

Security at its core
Adobe understands that the confidentiality, integrity and availability of our customers’ information are important to their business operations. Adobe Document Cloud services called eSign services and PDF services use a rigorous approach to protecting that key information. We are constantly monitoring and improving our applications, systems and processes to meet the growing demands and challenges of security.

Adobe takes the security of your digital experiences seriously.

- We use a practice known as the Adobe Secure Product Lifecycle (SPLC)—a set of specific security activities spanning software development practices, processes and tools—that is integrated into multiple stages of the product lifecycle.
- On a physical level, we have a foundational framework of security processes and controls to protect our infrastructure, applications and services, helping us comply with industry-accepted standards and certifications.

Physical data center security
All customer data stored in Adobe Document Cloud is geographically dispersed in data centers across the United States. Adobe Document Cloud uses hosting infrastructures from Amazon Web Services (AWS) and Rackspace. Each of these data centers include state-of-the-art physical and environmental access controls. Adobe is also planning to add data centers in other regions beginning later this year.

Disaster recovery
Adobe maintains a high level of operational excellence and works to ensure that customers are not impacted by unplanned outages. If there is an unplanned outage, Adobe Document Cloud operations personnel work as quickly as possible to restore full access to the service as soon as possible. The data centers are designed to tolerate system or hardware failures with minimal impact.

Environmental controls
The data centers are equipped to detect environmental hazards and utilize climate control systems to maintain a consistent operating temperature and humidity level.

Logical security
Adobe Document Cloud requires management authorization for employees accessing any critical applications and systems. Access is granted according to a user’s role and business need. Logical and physical access is revoked for employees who have left the organization. Continuous monitoring of sensitive logs is in effect at all times, and system audits are conducted periodically to detect inappropriate access to critical assets.
Data protection
Adobe Document Cloud services use AES 256-bit encryption for data at rest and support HTTPS
TLS v1.0 or higher for protecting data in transit. Only during certain business and support functions,
or as required by law, does Adobe access customer data.

Intrusion detection, response and monitoring
Adobe Document Cloud uses a variety of monitoring systems to detect network security anomalies,
denial of service, IP spoofing, port scanning and other advanced attacks. When an incident occurs
with an Adobe cloud-based service, including Adobe Document Cloud, Adobe centralizes incident
response, decision-making and external monitoring in its Security Coordination Center (SCC),
providing cross-functional consistency and fast resolution of issues.

Internal and third-party testing and assessments
New product features are reviewed for design flaws that impact security, and security testing is
integrated into the application development lifecycle. Additional vulnerability testing is conducted
in the form of source code reviews and static and dynamic analysis scans. Every major Adobe
Document Cloud service release is subjected to independent third-party application penetration
testing prior to release, and critical bugs are addressed before release.

Regulatory compliance
Adobe Document Cloud is designed and certified to meet many compliance regimes for various
industry sectors. The threat landscape is ever evolving and increasingly challenging, and customers
can rely on Document Cloud to stay ahead of the threats. The data centers and facilities at
RackSpace and AWS hosting Adobe Document Cloud services are compliant with the following
security certifications:
- Payment Card Industry Data Security Standard (PCI DSS) Level 1 (merchant and service provider)
- Health Insurance Portability and Accountability Act (HIPAA)
- U.S.-EU Safe Harbor Framework
- ISO 27001
- SOC 2 Type 2 (Trust Services Principles: security and availability)

Adobe Document Cloud business processes that use eSign services are also compliant with
industry security standards, including ISO 27001, SOC 2 Type 2, HIPAA and PCI v3.0 used by the
Payment Card Industry.