Adobe Acrobat DC with Document Cloud services security overview

Table of contents

Although Adobe Sign is part of Document Cloud PDF Services, its security functionality is independent.

Executive summary

At Adobe, we take the security of your digital experience very seriously. Security practices are deeply ingrained into our internal software development, operations processes, and tools. These practices are strictly followed by our cross-functional teams to help prevent, detect, and respond to incidents in an expedient manner. We keep up to date with the latest threats and vulnerabilities through our collaborative work with partners, leading researchers, security research institutions, and other industry organizations. We regularly incorporate advanced security techniques into the products and services we offer.

Adobe services that touch customer content have completed numerous industry certifications. For a detailed list of all compliance certifications and standards as well as government regulations currently supported by Adobe products and solutions, please see the Current List of Certifications, Standards, and Regulations. For information on GDPR, please see the GDPR readiness page.

This white paper describes the defense-in-depth approach and security procedures implemented by Adobe to enhance the security of Adobe Acrobat DC, Acrobat Reader DC, Document Cloud, Document Cloud services, and associated data.

Acrobat DC with Document Cloud services overview

Adobe Acrobat DC combines the latest Acrobat desktop software with premium features in the Acrobat Reader mobile app and Adobe Document Cloud online services to help organizations meet end-user demand for connectivity and productivity on any device while helping to ensure security across devices. Using Adobe Acrobat DC and Document Cloud services, customers can turn content into an electronic document that can be shared with others and easily generate, manipulate, and transform PDF files from any Adobe cloud service, desktop application, or mobile app.

Acrobat document security features

Redaction

Adobe Acrobat DC includes a set of redaction tools that help customers protect sensitive or confidential information, including permanent deletion of both text and graphic images in a document before distribution. In addition, users can search and redact content based on patterns, such as phone numbers, credit card numbers, and email addresses. The redacted information is completely removed from the file, not just masked as with other tools or methods. Using the document sanitization feature, customers can also remove hidden information and non-graphic objects, such as metadata that may be present in the PDF.

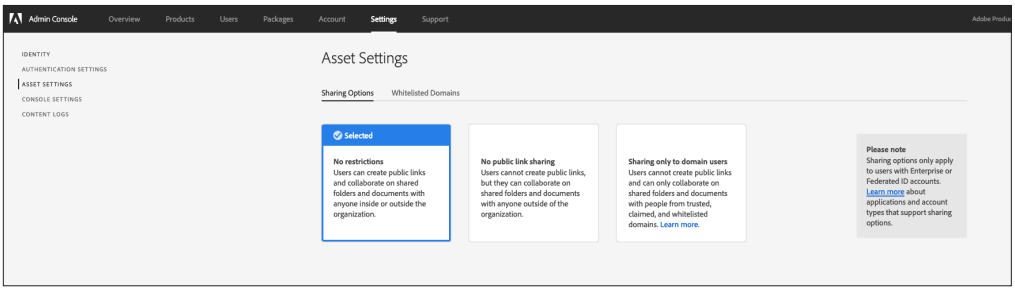
File sharing

All Document Cloud files stored in the cloud are automatically labeled "Private," which means the content is only visible to the end user who uploaded it. An end user must take explicit actions to share that content, or it will remain private. All Document Cloud content sharing is completed by sending a link to the Document Cloud content to the recipient(s) via email, text, or any collaboration software.

Users of Document Cloud services may share files with two options: View Only or Review. If the user sends the link with the View Only restriction, the recipient may only view the content as a read-only document. Alternatively, if the user sends the document for review, the recipient may comment on the document, but may not edit or alter it in any way.

Asset settings and sharing restrictions

Asset settings give an organization control over how employees share assets outside the organization. The IT administrator can select a restrictive setting that limits employees from using specific sharing features within Document Cloud, including restricting invitation-based sharing to recipients in the claimed, trusted, and whitelisted domains. When this policy is set, users are prevented from sharing organization-owned assets with external users who are not in the list of allowed domains.



Asset settings in the Admin Console

Microsoft Information Protection (MIP)

For customers using Acrobat DC or Acrobat Reader DC to open files protected with Microsoft Information Protection (MIP) solutions, including Azure Information Protection (AIP) and Information Protection using Microsoft Office 365, please see this document.

Protected Mode in Acrobat Reader DC

To help protect customers from malicious code that attempts to use the PDF format to write to or read from a computer's file system, Adobe delivers an implementation of sandboxing technology called Protected Mode, which was introduced in Adobe Reader X.

Sandboxing is a security method that creates a confined execution environment in which to run programs with low rights or privileges. Sandboxes help protect users' systems from being harmed by untrusted documents that contain executable code. In the context of Acrobat Reader DC, the untrusted content would be any PDF file and the process that it might invoke. Acrobat Reader DC treats all PDF files as potentially corrupt and confines all processing that the PDF file invokes to the sandbox.

Acrobat Reader DC Protected Mode helps defend against attackers attempting to install malware on a computer system, which supports organizations' efforts to prevent malicious actors from accessing and extracting sensitive data and intellectual property from their networks. Protected Mode is enabled by default whenever a user launches Acrobat Reader DC and limits the level of access granted to the program, safeguarding systems running Microsoft Windows from malicious PDF files that might attempt to write to or read from the computer's file system, delete files, or otherwise modify system information.

Protected Mode on Windows 8 and above can also run in a Windows AppContainer, providing an even stronger locked-down environment for customers who enable Protected Mode.

Protected View in Acrobat DC

Similar to Protected Mode in Acrobat Reader DC, Protected View is an implementation of sandboxing technology for the rich Acrobat DC feature set. In Acrobat DC, Adobe extends the functionality of Protected Mode beyond blocking write-based attacks that attempt to execute malicious code on a computer system using the PDF file format to also include read-based attacks that attempt to steal sensitive data or intellectual property via PDF files.

Like Protected Mode, Protected View confines the execution of untrusted programs (for example, any PDF file and the processes that it invokes) to a restricted sandbox to avoid malicious code using the PDF format from writing to or reading from the computer's file system. Protected View assumes that all PDF files are potentially malicious and confines processing to the sandbox, unless the user specifically indicates that a file is trusted.

Protected View is supported in both scenarios in which users open PDF documents—within the standalone Acrobat DC application and within a browser. Protected View on Windows 8 and above always runs in an AppContainer. This provides an even stronger locked-down environment for customers who enable Protected View.

When a user opens an untrusted file within Protected View, Acrobat DC displays a message bar at the top of the viewing window. The message bar indicates that the file is untrusted and reminds the user that they are in Protected View, thereby disabling many Acrobat DC features and limiting user interaction with the file. Essentially, the file is in "read-only" mode, and Protected View defends against embedded or tag-along content tampering with the system.

To trust the file and enable all Acrobat DC features, the user can click the Enable All Features button in the message bar. This action exits Protected View and provides permanent trust for the file by adding it to Acrobat's list of privileged locations. Each subsequent opening of the trusted PDF file disables Protected View restrictions.

Document Cloud services architecture

Adobe Document Cloud services include:

- **Organize PDF**—Insert, delete, reorder, or rotate pages in a PDF
- **Create PDF**—Convert Word, Excel, and PowerPoint documents, and images or photos into PDF files
- **Export PDF**—Easily convert PDFs into editable Microsoft Word, Excel, PowerPoint, or RTF files
- **Edit PDF**—Easily edit existing PDFs from your mobile device or laptop
- **Combine PDF**—Combine multiple files into a single PDF and assemble document packages from anywhere
- **Send & Track**—Send, track, and confirm delivery of documents
- **Adobe Scan**—Capture and convert anything into a searchable, high-quality PDF
- **Adobe Sign**—Prepare and send documents for secure and trusted, legally binding e-signatures on any device

Document Cloud services security

Entitlement and identity management

IT administrators entitle end-user access to Adobe Document Cloud services by utilizing named user licensing in the Adobe Admin Console. Acrobat Document Cloud supports three (3) different types of user-named licensing:

- **Adobe ID**—For Adobe-hosted, user-managed accounts that are created, owned, and controlled by individual users. Adobe ID accounts only have access to Acrobat Document Cloud services if an IT administrator enables access.
- **Enterprise ID**—An Adobe-hosted, enterprise-managed option for accounts that are created and controlled by IT administrators from the customer's enterprise organization. The organization owns and manages the user accounts and all associated assets.
- **Federated ID**—An enterprise-managed account where all identity profiles are provided by the customer's single sign-on (SSO) identity management system and are created, owned, and controlled by the customer's IT infrastructure. Adobe integrates with most SAML 2.0 compliant identity providers.

Most enterprise organizations use Enterprise IDs or Federated IDs for their employees, contractors, and freelancers, provided the email address is within the company domain, because it lets them maintain control of both the entitlements and the user-generated content (UGC) stored on behalf of that ID. For more information about each identity type, please see the Adobe customer support site.

Adobe ID and Enterprise ID password storage both leverage the SHA-256 hash algorithm in combination with password salts and a large number of hash iterations. Adobe continually monitors Adobe hosted accounts for unusual or anomalous account activity, and evaluates this information to help quickly mitigate threats to security. For Federated ID accounts, Adobe does not manage users' passwords. For more information, please refer to the Adobe Identity Management Services Security Overview.

Electronic and digital signatures

With Document Cloud services, users can choose between two different tools to work securely with signatures:

- **Fill & Sign tool**—Powered by Adobe Sign, lets users manage end-to-end signing processes designed to help comply with e-signature laws in the United States, the European Union, and most industrialized nations worldwide. With it, they can request signatures from others, track the signing process, and automatically archive signed documents and audit trails. Security measures are applied to the entire process, and documents and audit trails are certified by Adobe with a tamper-evident seal.

Tracking is not available on mobile.

For more information on Adobe Sign and its security functionality, please see the Adobe Sign technical overview.

- **Certificates tool**—Enables users to sign documents with certificate-based digital signatures from trusted service providers on either the Adobe Approved Trust List (AATL) or the European Union Trusted List (EUTL). Signing with a certificate ID issued by a trusted third-party certificate authority (CA) is generally recognized as a secure method of signing documents electronically. The ID is uniquely linked to and capable of identifying the signer. The signer's certificate is cryptographically bound to the document during the signing step using the private key uniquely held by that signer.

  Acrobat DC validates the signer's signature—and the authenticity of the document he or she signed—by connecting automatically with the CA for verification. This type of signature complies with PDF electronic signature standards, including PDF Advanced Electronic Signature (PAdES) Parts 2, 3, and 4, as well as the U.S. Department of Defense Joint Interoperability Test Command (JITC) usage of cryptography and Public Key Infrastructure (PKI) with AES-256, RSA-4096, SHA-512, and RSA-PSS. The Certificates tool also lets users add timestamps to documents and certify them with a tamper-evident seal.

Document Cloud services content storage

Although administrators allocate individual cloud storage for Enterprise ID and Federated ID accounts through the Adobe Admin Console, they do not have direct access to any files in the user's Document Cloud services storage. Deleting an Enterprise ID or Federated ID with existing shared services storage renders any data in cloud storage inaccessible to the end user and that user's data will be deleted after 90 days.

Administrators can also use the Admin Console to allocate storage to Adobe ID accounts. While they cannot delete Adobe ID accounts, administrators can revoke both the granted enterprise storage quota as well as application and service access. The data associated with those accounts is deleted after 90 days.

Adobe Document Cloud services leverage multitenant storage. Customer content is processed by an Amazon Elastic Compute Cloud (Amazon EC2) instance and stored on a combination of Amazon Simple Storage Services (Amazon S3) buckets and through a MongoDB instance on an Amazon Elastic Block Store (Amazon EBS). The content itself is stored in Amazon S3 buckets, and the metadata about the content is stored in Amazon EBS via MongoDB—all protected by Identity and Access Management (IAM) roles within that Amazon Web Services (AWS) Region.

Metadata and support assets that are stored in Amazon EBS are encrypted with AES 256-bit encryption using Federal Information Processing Standards (FIPS) 140-2 approved cryptographic algorithms consistent with National Institute of Standards and Technology (NIST) 800-57 recommendations.

Data is redundantly stored in multiple data centers and on multiple devices in each data center. All network traffic undergoes systematic data verification and checksum calculations to prevent corruption and ensure integrity. Finally, stored content is synchronously and automatically

replicated to other data center facilities within that customer's region so that data integrity will be maintained even if there were loss of data in two locations.

For more information on the underlying Amazon services, please see:

- MongoDB
- Amazon S3
- AWS Key Management Service (KMS)
- Amazon EC2 service

Dedicated encryption key

By default, the content and assets stored in Amazon S3 are encrypted with AES 256-bit symmetric security keys, which are unique to each customer and each customer's claimed domain. If administrators wish to add an additional layer of control and security for some or all of the domains in their organization, they can use a dedicated encryption key that is managed by the AWS KMS and is automatically rotated on an annual basis.

Administrators can also revoke this dedicated encryption key via the Admin Console, which will render all data encrypted with that key inaccessible to end users, and prevent both content upload and download until the encryption key is re-enabled.

Note: While Adobe Document Cloud files can be encrypted using the dedicated encryption key, metadata cannot be encrypted using the key.

For more information on managing encryption using a dedicated key, please see these Adobe help pages:

- Managing encryption
- Dedicated encryption keys FAQ

Amazon Web Services

As previously mentioned, all components of Adobe Document Cloud services are hosted on AWS, including Amazon EC2 and Amazon S3, in the United States. Amazon EC2 is a web service that provides automatically scalable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is generally recognized as a highly reliable data storage infrastructure for storing and retrieving any amount of data.

The AWS platform provides services in accordance with industry-standard practices and undergoes regular industry-recognized certifications and audits. You can find more detailed information about AWS and Amazon's security controls on the AWS Cloud Security website.

Operational responsibilities of AWS and Adobe

AWS operates, manages, and controls the components from the hypervisor virtualization layer down to the physical security of the facilities in which Adobe Document Cloud services operate. In turn, Adobe assumes responsibility and management of the guest operating system (including updates and security patches) and application software, as well as the configuration of the AWS-provided security group firewall.

AWS also operates the cloud infrastructure used by Adobe to provision a variety of basic computing resources, including processing and storage. The AWS infrastructure includes facilities, network, and hardware, as well as the operational software (for example, host OS, virtualization software, and so on) that supports the provisioning and use of these resources. Amazon designs and manages AWS according to industry-standard practices as well as a variety of security compliance standards.

Secure management

Adobe uses Secure Shell (SSH) and Secure Sockets Layer (SSL) for management connections to manage the AWS infrastructure.

Geographic location of customer data on the AWS network

All UGC uploaded to Document Cloud is stored in AWS US-East (Virginia) regional data centers. Content is backed up within each data center, and in other data centers within the region, for load balancing and redundancy.

Geographic location of identity data on the AWS network

Identity data is stored in multiregion, load-balanced AWS data centers located in Virginia (US-East), Oregon (US-West), Ireland (EU-West), and Singapore (AP-Southeast). Identity data is replicated across all data centers. Adobe complies with applicable laws regarding cross-border data transfers, as outlined in greater detail at https://www.adobe.com/privacy/eudatatransfers.html.

Isolation of customer data/segregation of customers

AWS uses strong tenant isolation security and control capabilities. As a virtualized, multitenant environment, AWS implements security management processes and other security controls designed to isolate each customer from other AWS customers. Adobe uses the AWS Identity and Access Management (IAM) to further restrict access to compute and storage instances.

Secure network architecture

AWS employs network devices, including firewalls and other boundary devices, to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACLs), and configurations to enforce the flow of information to specific information system services. ACLs, or traffic flow policies, exist on each managed interface to manage and enforce the flow of traffic.

Amazon Information Security approves all ACL policies and automatically pushes them to each managed interface using the AWS ACL-Manage tool, helping to ensure these managed interfaces enforce the most up-to-date ACLs.

Network monitoring and protection

AWS uses a variety of automated monitoring systems to provide a high level of service performance and availability. Monitoring tools help detect unusual or unauthorized activities, and conditions at ingress and egress communication points. The AWS network provides significant protection against traditional network security issues:

- Distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MITM) attacks
- IP spoofing
- Port scanning
- Packet sniffing by other tenants

For more information about network monitoring and protection, please see the AWS Cloud Security website.

Intrusion detection

Adobe actively monitors Adobe Document Cloud services using industry-standard intrusion detection systems (IDSs) and intrusion prevention systems (IPSs).

Logging

Adobe conducts server-side logging of Adobe Document Cloud services customer activity to diagnose service outages, specific customer problems, and reported bugs. The logs only store Adobe IDs to help diagnose specific customer issues and do not contain username/password combinations. Only authorized Adobe technical support personnel, key engineers, and select developers can access the logs to diagnose specific issues that may arise.

Service monitoring

AWS monitors electrical, mechanical, and life support systems and equipment to help with the immediate identification of service issues. In order to maintain the continued operability of equipment, AWS performs ongoing preventative maintenance.

Data storage and backup

Adobe stores all Adobe Document Cloud services data in Amazon S3, which provides a storage infrastructure with high durability. To help provide durability, Amazon S3 PUT and COPY operations synchronously store customer data across multiple facilities and redundantly store objects on multiple devices across multiple facilities in an Amazon S3 region.

Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. Data replication for Amazon S3 data objects occurs within the regional cluster where the data is stored and is not replicated to data center clusters in other regions.

Metadata is replicated by taking snapshots of Amazon EBS volumes and is stored similar to Amazon S3. For detailed information about AWS security, please see the AWS Cloud Security website.

Change management

AWS authorizes, logs, tests, approves, and documents routine, emergency, and configuration changes to existing AWS infrastructure in accordance with industry standards for similar systems. Amazon schedules updates to AWS to minimize any customer impact. AWS communicates with customers, either via email or through the AWS Service Health Dashboard, when service use is likely to be adversely affected. Adobe also maintains an Adobe System Status for Adobe Document Cloud.

Patch management

AWS maintains responsibility for patching systems that support the delivery of AWS services, such as the hypervisor and networking services. Adobe is responsible for patching its guest operating systems (OS), software, and applications running in AWS. When patches are required, Adobe supplies a new, pre-hardened instance of the OS and application rather than an actual patch.

AWS physical and environmental controls

AWS physical and environmental controls are specifically outlined in SOC Type 1 and SOC Type 2 reports. The following section outlines some of the security measures and controls in place at AWS data centers around the world. For more detailed information about AWS security, please see the AWS Cloud Security website.

Physical facility security

AWS data centers use industry standard architectural and engineering approaches. AWS data centers are housed in nondescript facilities, and Amazon controls physical access both at the perimeter and at building ingress points using professional security staff, video surveillance, IDSs, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification, and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if he or she continues to be an employee of Amazon or AWS. All physical access to data centers by AWS employees is logged and audited routinely.

Fire suppression

AWS installs automatic fire detection and suppression equipment in all AWS data centers. The fire detection system uses smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms, and generator equipment rooms. These areas are protected by either wet-pipe, double- interlocked pre-action, or gaseous sprinkler systems.

Controlled environment

AWS employs a climate control system to maintain a constant operating temperature for servers and other hardware, preventing overheating and reducing the possibility of service outages. AWS data centers maintain atmospheric conditions at optimal levels. AWS personnel and systems monitor and control both temperature and humidity at appropriate levels.

Backup power

AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations—24 hours a day, seven days a week. Uninterruptible power supply (UPS) units provide backup power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide backup power for the entire facility.

Disaster recovery

AWS data centers include a high level of availability, and tolerate system or hardware failures with minimal impact. Built in clusters in various global regions, all data centers remain online 24x7x365 to serve customers—no data center is "cold." In case of failure, automated processes move customer data traffic away from the affected area.

Core applications are deployed in an N+1 configuration, so that in the event of a data center failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites. For more information about AWS disaster recovery protocols, please see AWS Cloud Security website.

Adobe risk and vulnerability management

Adobe strives to ensure that our risk and vulnerability management, incident response, mitigation, and resolution process is nimble and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help achieve the highest levels of security for all Adobe products and services.

Penetration testing

Adobe approves and engages with leading third-party security firms to perform penetration testing that can uncover potential security vulnerabilities and improve the overall security of Adobe products and services. Upon receipt of the report provided by the third party, Adobe documents these vulnerabilities, evaluates the severity and priority, and then creates a mitigation strategy or remediation plan. Adobe conducts a full penetration test annually and performs vulnerability scans on a monthly basis.

Internally, the Adobe Document Cloud security team performs a risk assessment of all Document Cloud components and services quarterly and prior to every release. The Document Cloud security team partners with technical operations and development leads to help ensure all high-risk vulnerabilities are mitigated prior to each release. For more information on Adobe penetration testing procedures, please see the Adobe Secure Engineering Overview.

Incident response and notification

New vulnerabilities and threats evolve each day, and Adobe strives to respond to and mitigate newly discovered threats. In addition to subscribing to industry-wide vulnerability announcement lists, including the United States Computer Emergency Readiness Team (US-CERT), Bugtraq, and SANS, Adobe also subscribes to the latest security alert lists issued by major security vendors.

For more details about Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

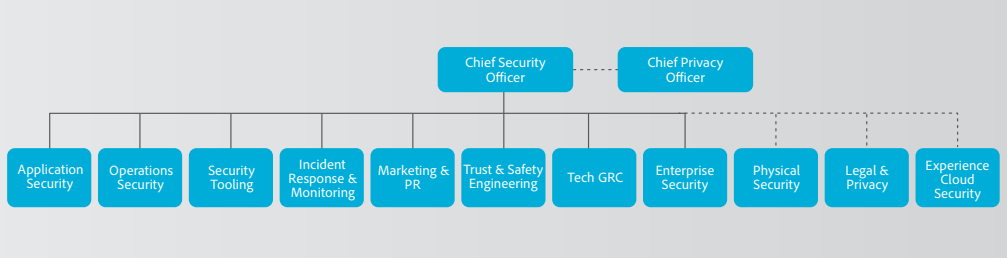
Forensic analysis

For incident investigations, the Document Cloud team adheres to the Adobe forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe holding, and chain-of-custody recording(s).

The Adobe security organization

As part of our commitment to the security of our products and services, Adobe coordinates all security efforts under the chief security officer (CSO). The office of the CSO coordinates all product and service security initiatives, and the implementation of the Adobe Secure Product Lifecycle (SPLC).

The CSO also manages the Adobe Secure Software Engineering Team (ASSET), a dedicated, central team of security experts who serve as consultants to key Adobe product and operations teams, including the Adobe Document Cloud team. ASSET researchers work with individual Adobe product and operations teams to strive to achieve the right level of security for products and services, and advise these teams on security practices for clear and repeatable processes for development, deployment, operations, and incident response.



Adobe security organization

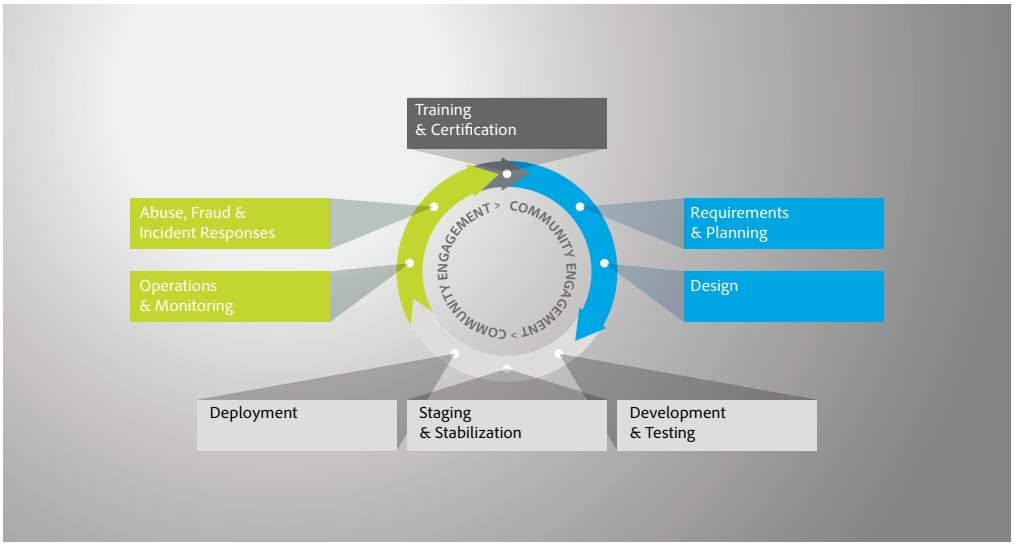
Adobe Secure Product Development

As with other key Adobe product and service organizations, the Adobe Document Cloud organization employs the Adobe SPLC process. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC is integrated into multiple stages of the product lifecycle, from design and development to quality assurance, testing, and deployment. ASSET security researchers provide specific SPLC guidance for each key product or service based on an assessment of potential security issues. Complemented by continuous community engagement, the Adobe SPLC evolves to stay current as changes occur in technology, security practices, and the threat landscape.

Adobe Secure Product Lifecycle

The Adobe SPLC activities include, depending on the specific Adobe Document Cloud component, some or all of the following recommended best practices, processes, and tools:

- Security training and certification for product teams
- Product health, risk, and threat landscape analysis
- Secure coding guidelines, rules, and analysis
- Service roadmaps, security tools, and testing methods that guide the Adobe Document Cloud security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security risks and CWE/SANS Top 25 most dangerous software errors
- Security architecture review and penetration testing
- Source code reviews to help eliminate known flaws that could lead to vulnerabilities
- UGC validation
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials



Adobe Secure Product Lifecycle

Adobe Software Security Certification Program

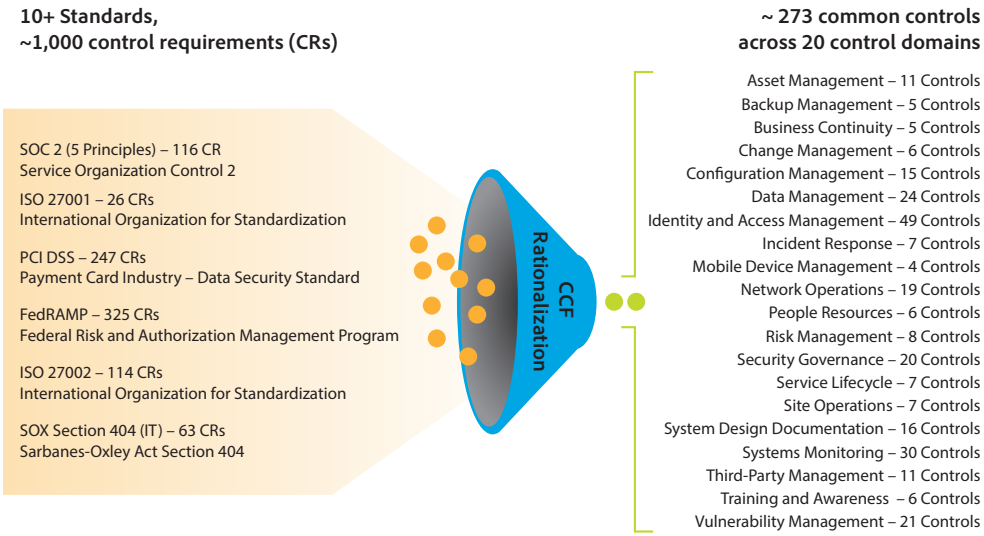
As part of the Adobe SPLC, Adobe conducts ongoing security training within development teams to enhance security knowledge throughout the company and improve the overall security of our products and services. Employees participating in the Adobe Software Security Certification Program attain different certification levels by completing security projects. For more information about our product security practices, please see the Adobe Secure Engineering Overview.

For more information on the Adobe Software Security Certification Program, please see the Adobe security culture white paper.

Document Cloud services compliance

The Adobe Common Controls Framework (CCF) is a set of security activities and compliance controls that are implemented within our product operations teams as well as in various parts of our infrastructure and application teams.

In creating the CCF, Adobe analyzed the criteria for the most common security certifications for cloud-based businesses and rationalized the more than 1,000 requirements down to Adobe specific controls that map to approximately a dozen industry standards.



Adobe Common Controls Framework

Current regulations and compliance for Adobe Document Cloud services

SOC 2 is a set of security principles that define leading practice controls relevant to security, confidentiality, and privacy. Adobe Document Cloud services are SOC 2 Type 2 (security and availability) compliant.

ISO 27001 is a set of globally adopted standards that outline stringent security requirements and provide a systematic approach to managing the confidentiality, integrity, and availability of customer information. Adobe Document Cloud services are compliant with ISO 27001:2013.

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle payment card information, such as credit card numbers. Being a PCI DSS–compliant service provider enables Adobe to help customers meet PCI requirements for the safe handling of personally identifiable data associated with a cardholder.

The Gramm-Leach-Bliley Act (GLBA) requires that financial institutions safeguard their customers' personal data. Adobe Document Cloud services are GLBA ready, meaning they enable our financial customers to comply with GLBA requirements for using service providers.

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Adobe Document Cloud services are FedRAMP Tailored, meaning they enable our customers to comply with FedRAMP requirements.

The U.S. Family Educational Rights and Privacy Act (FERPA) is designed to preserve the confidentiality of U.S. student education records and directory information. Under FERPA guidelines, Adobe can contractually agree to act as a "school official" when it comes to handling regulated student data, enabling our education customers to comply with FERPA requirements.

The SAFE-BioPharma standard describes requirements for standardized identity trust for either identity authentication or for digital signing. Adobe Document Cloud is certified to be compliant with the SAFE-BioPharma digital identification standard. Adobe Acrobat DC is safe to use within and compliant with SAFE-BioPharma workflows. In addition, Adobe Document Cloud services and Adobe Sign are SOC Type 2 compliant.

For information about the current compliance posture for Adobe Sign, please see the Adobe Sign technical overview.

Ultimately, customers are responsible for ensuring compliance with their legal obligations, and making sure that our solutions meet their compliance needs and are secured in an appropriate way.

Adobe employees

Adobe has employees and offices around the world, and implements the following processes and procedures company-wide to protect the company against security threats.

Employee access to customer data

Adobe maintains segmented development and production environments for Adobe Document Cloud, using technical controls to limit network- and application-level access to live production systems. Employees have specific authorizations to access development and production systems, and employees with no legitimate business purpose are restricted from accessing these systems.

Background checks

Adobe obtains background-check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks includes inquiries regarding educational background, work history, and court records, including criminal conviction records and references obtained from professional and personal associates, each as permitted by applicable law. These background-check requirements apply to regular U.S. new hire employees, including those who will be administering systems or have access to customer information. New U.S. temporary agency workers are subject to background-check requirements through the applicable temporary agency, in compliance with Adobe's background screen guidelines. Outside the United States, Adobe conducts background checks on certain new employees in accordance with Adobe's background check policy and applicable local laws.

Employee termination

When an employee leaves Adobe, the employee's manager submits an exiting worker form. Once approved, Adobe People Resources initiates an email workflow to inform relevant stakeholders to take specific actions leading up to the employee's last day. In the event that Adobe terminates an employee, Adobe People Resources sends a similar email notification to relevant stakeholders, including the specific date and time of the employment termination.

Adobe Corporate Security then schedules the following actions to help ensure that, upon conclusion of the employee's final day of employment, he or she can longer access Adobe confidential files or offices:

- Email access removal
- Remote VPN access removal
- Office and data center badge invalidation
- Network access termination

Upon request, managers may ask building security to escort the terminated employee from the Adobe office or building.

Facility security

Every Adobe corporate office location employs on-site guards to protect the premises 24x7. Adobe employees carry a key card ID badge for building access. Visitors enter through the front entrance, sign in and out with the receptionist, display a temporary visitor ID badge, and are accompanied by an employee. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environment-controlled server rooms accessible only by appropriate authorized staff members.

Virus protection

Adobe scans all inbound and outbound corporate email for known malware threats.

Customer data confidentiality

Adobe always treats all customer data as confidential. Adobe does not use or share the information collected on behalf of a customer except as may be allowed in a contract with that customer and as set forth in the Adobe Terms of Use and the Adobe Privacy Policy.

Conclusion

Adobe's proactive approach to security and stringent procedures described in this paper help protect the security of Adobe Acrobat DC, Acrobat Reader DC, and Document Cloud services—and your confidential data. At Adobe, we take the security of your digital experience very seriously. We continuously monitor the evolving threat landscape to stay ahead of malicious activities and help ensure the security of our customers' data.

For more information, please visit the Adobe Trust Center.

Adobe

Adobe Inc.
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

5/19