Adobe Document Cloud

Adobe

Adobe Acrobat with Document Cloud Services Security Overview

Table of Contents

Adobe Security

At Adobe, we know the security of your digital experiences is important. Security practices are deeply ingrained into our internal software development and operations processes and tools and are rigorously followed by our cross-functional teams to prevent, detect, and respond to incidents in an expedient manner. Furthermore, our collaborative work with partners, leading researchers, security research institutions, and other industry organizations helps us keep up to date with the latest threats and vulnerabilities, and we regularly incorporate advanced security techniques into the products and services we offer.

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

Acrobat with Document Cloud Services Overview

Acrobat with Document Cloud services is the complete PDF solution for today's multi-device, connected world. Using Acrobat desktop software and the Adobe Acrobat Reader mobile app (enhanced with premium mobile features) with Document Cloud services, organizations can build smarter document workflows and meet end-user demand for mobile solutions while helping ensure document security across devices.

Acrobat with Document Cloud services enables customers to turn virtually any content into an electronic document that can be shared with others and easily automate the generation, manipulation, and transformation of PDF files from any Acrobat cloud service, desktop application, or mobile app.

Acrobat User Experiences

Customers can use Document Cloud services with a variety of Acrobat user experiences:

- Acrobat Pro — Desktop application for laptop and desktop users

- Acrobat online — Web app within supported browsers on desktop and mobile devices, including Chrome, Microsoft Edge, Firefox, and Safari

- Acrobat Reader mobile client — Free downloadable app from the Apple App Store and Google Play for mobile and tablet users

Adobe has also integrated Acrobat into several Microsoft productivity tools. The behavior of document storage for these integrations is different than for standalone Acrobat. The security information for each integration is detailed in the "Acrobat Microsoft Integrations" section.

Document Cloud Services

Adobe Document Cloud services include the following:

- Send PDF — Send a PDF to a recipient using an email client

- Organize PDF — Insert, delete, reorder, or rotate pages in a PDF

- Create PDF — Convert Word, Excel, and PowerPoint documents, as well as images or photos, into PDF files

- Export PDF — Convert PDFs into editable Microsoft Word, Excel, PowerPoint, or RTF files

- Edit PDF — Edit existing PDFs from a mobile device or laptop

- Combine PDF — Combine multiple files into a single PDF and assemble document packages from anywhere

- Fill & Sign — Complete a form and add a signature

- Adobe Scan — Capture and convert anything into a searchable, high-quality PDF

- Adobe Acrobat Sign — Prepare and send documents for trusted e-signatures on any modern device — from simple signatures to digital signatures in the cloud.

Adobe continually adds new offerings to Document Cloud services. An up-to-date list of all Document Cloud services is available on Adobe.com.

Acrobat Document Security Features

Redaction

Adobe Document Cloud services 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 based on patterns, such as phone numbers, credit card numbers, and email addresses. The information selected 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

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 the link to the URL of the Document Cloud content to the recipient(s).

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. Links may be sent to recipients via email, text, or any collaboration software.

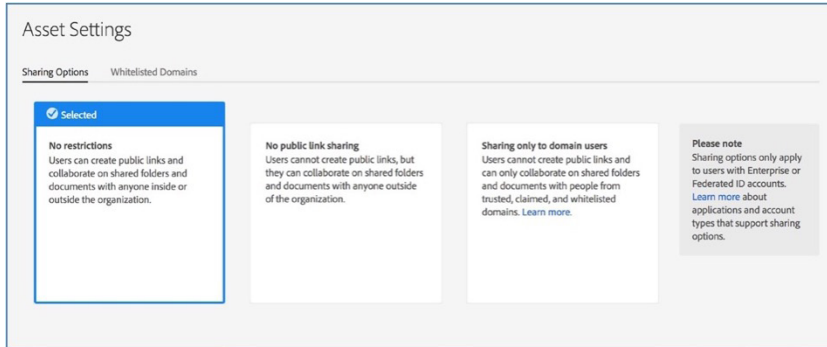## Asset Settings and Sharing Restrictions

Figure 1: Document Cloud Services Asset Settings

Content stored in Document Cloud can also have sharing restrictions enabled through the Asset Settings feature in the Adobe Admin Console. This feature allows enterprise IT to turn off public link sharing as well as force DC Collaboration only within the enterprise-claimed domain and any other allowed domains. When sharing restrictions are enabled, recipients must sign in. If "Sharing only to domain users" mode is turned on, users additionally can only share content with other users within their organization or other trusted domains; external sharing is completely disabled.

Microsoft Purview Information Protection

Microsoft Purview Information Protection is a Microsoft rights management solution. Users of Azure Information Protection and other Microsoft Purview Information Protection solutions can use Acrobat or Acrobat Reader to read labeled and protected content. The most current versions of Acrobat and Acrobat Reader (version 22.001.20142 and later) include the Microsoft plug-in and do not require a separate installation. Customers using older versions of Acrobat or Acrobat Reader should download the plug-in from Adobe.com.

Protected Mode

To 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 a cutting-edge implementation of sandboxing technology called Protected Mode.

In Acrobat Reader, Protected Mode extends the protection against attackers who attempt to install malware on a computer system to include blocking malicious individuals from accessing and extracting sensitive data and intellectual property from the corporate network as well. Protected Mode is enabled by default whenever a user launches Acrobat Reader 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.

Acrobat Reader Protected Mode (on Windows 8.1 and above) can run in isolation in an [AppContainer](#).

Protected View

Sandboxing is a highly respected 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, untrusted content is any PDF file and the processes that it invokes. Reader treats all PDF files as potentially corrupt and confines all processing that the PDF file invokes to the sandbox. Like Protected Mode in Acrobat Reader, Protected View is an implementation of sandboxing technology for the rich Acrobat feature set.

In Acrobat, Adobe extends the functionality of Protected View beyond blocking write-based attacks that attempt to execute malicious code on a computer system using the PDF file format to 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 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 a potentially malicious file within Protected View, Acrobat displays a yellow message bar (YMB) at the top of the viewing window. The YMB indicates that the file is untrusted and reminds the user that they are in Protected View, thereby disabling many Acrobat features and limiting user interaction with the file. Essentially, the file is in "read-only" mode, and Protected View prevents embedded or tag-along malicious content from tampering with the system.

To trust the file and enable all Acrobat features, the user can click the "Enable All Features" button in the YMB. 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.

Adobe Document Cloud Services Security

User Authentication

Administrators entitle end-user access to Adobe Document Cloud services by utilizing named user licensing in the Adobe Admin Console. Acrobat with Document Cloud services supports four (4) different types of user-named licensing, including Adobe ID, Business ID, Enterprise ID, and Federated ID. For more information about these identity types and Adobe Identity Management Services, please see the Adobe Identity Management Services security overview.

Document and User-Generated Content Storage

Adobe Document Cloud services leverages multi-tenant storage. User-generated content and documents are 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 help ensure integrity. Finally, stored content is synchronously and automatically replicated to other data center facilities within that customer's region so that data integrity is maintained even with the loss of data in two locations.

Administrators can allocate individual cloud storage for some Enterprise ID and Federated ID accounts through the Adobe Admin Console but do not have direct access to any of the end-user's documents or content stored in Document Cloud services storage. However, admins can assume ownership for the user's account as well as revoke access. Deleting these types of accounts 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 control Adobe ID accounts, admins can delete them, removing both the granted enterprise storage quota as well as application and service access from end-user accounts, with the data also being deleted after 90 days.

Data Encryption

By default, Document Cloud services user-generated content and documents are encrypted in transit with HTTPS TLS 1.2 encryption. Document Cloud services content is encrypted at-rest using AES 256-bit symmetric security keys that are unique to each customer and each customer's claimed domain. These encryption methods apply to both permanent and temporary document storage.

Dedicated Encryption Keys

In addition to standard, built-in encryption capabilities, administrators can add another layer of control and security for documents at-rest with a dedicated encryption key for some of or all the domains in the customer organization. Document Cloud services content can then be encrypted at-rest using that dedicated encryption key, and, if required, can be revoked from the Admin Console. Revoking the key will render all content encrypted with that key inaccessible to all end users and will prevent both content upload and download until the encryption key is re-enabled.

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

More information on managing encryption using a dedicated key is available on Adobe.com.

Electronic and Digital Signatures

With Document Cloud services, users can use different tools to work with signatures, including:

- **Fill & Sign tool** — Lets users open a PDF, fill in form fields, and sign the document electronically.

- **Certificates tool** — Enables users to sign documents with an e-signature backed by a digital certificate that is cryptographically bound to the signature field. Each digital certificate (or digital ID) uniquely identifies the signer and is issued by a trust service provider (TSP) or certificate authority (CA) listed on the Adobe Approved Trust List (AATL) or the European Union Trusted Lists (EUTL). The Certificates tool also allows users to add timestamps to documents and certify documents with a tamper-evident seal.

Acrobat Microsoft Integrations

Adobe has partnered with Microsoft to create integrations with their leading productivity tools, enabling Acrobat with Document Cloud services to be accessed natively from within:

- Microsoft SharePoint and OneDrive

- Microsoft Teams

- Microsoft Word, Excel, and PowerPoint (Create and Protect PDF only)

With each of these integrations, Adobe only creates a temporary copy of the PDF document and does not collect any customer information or personal identifying information from the user.

Acrobat for SharePoint and OneDrive

Acrobat for SharePoint and OneDrive gives users access to PDF workflows within Microsoft 365 and enables them to view, create, and modify PDFs in the cloud.

Using this integrated version of Acrobat, documents are stored in their original location on SharePoint or OneDrive. Actions such as viewing, commenting, and search occur on the

user's machine. When the user makes any changes to their document, the document is again stored in their SharePoint or OneDrive account.

If the user creates, organizes, combines, or exports a document, it is sent to Adobe Document Cloud servers in the region in which the user is located (e.g., United States., Europe, or Japan) for transient processing and is then deleted within 24 hours. The document remains encrypted both in transit and at rest during this process (see the "Data Encryption" section). The modified document is saved back to the user's SharePoint or OneDrive account.

More information about the specific functionality of Acrobat for SharePoint and OneDrive is available at Adobe.com.

Acrobat for Microsoft Teams

Acrobat for Microsoft Teams gives users access to PDF workflows within Microsoft Teams and enables them to view, create, and modify PDFs in the cloud. Customers can use Acrobat for Microsoft Teams as a Personal Tab, Bot, Tab, Message Action, or Message Extension.

Any PDF shared in a Microsoft Teams chat or channel is stored in the user's OneDrive or SharePoint by default. However, when a PDF is shared and then collaborated on (i.e., shared commenting) in Acrobat for Microsoft Teams, the document is sent to Adobe Document Cloud servers in the region in which the user is located (e.g., United States, Europe, or Japan) for transient processing and is then deleted within 24 hours. The document remains encrypted both in transit and at rest during this process (see the "Data Encryption" section). The modified document is saved back to the original location.

If the customer's administrator turns off Document Cloud services, end users will be able to preview and comment on their own documents but will not be able to collaborate using shared commenting capabilities.

More information about the specific functionality of Acrobat available in the Microsoft Teams integration is available on Adobe.com.

Acrobat for Word, Excel, and PowerPoint

Users can use the Create PDF add-in to easily convert a Microsoft 365 document to a high-quality PDF and save the PDF to OneDrive or download it to their personal hard drive. Users can also protect the PDF by adding a password to prevent unauthorized access to the document.

Adobe Security Program Overview

The integrated security program at Adobe is composed of five (5) centers of excellence, each of which constantly iterates and advances the ways we detect and prevent risk by leveraging new and emerging technologies, such as automation, AI, and machine learning.

Figure 2: Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

- **Application Security** — Focuses on the security of our product code, conducts threat research, and implements bug bounty

- **Operational Security** — Helps monitor and secure our systems, networks, and production cloud systems

- **Enterprise Security** — Concentrates on secure access to and authentication for the Adobe corporate environment

- **Compliance** — Oversees our security governance model, audit and compliance programs, and risk analysis

- **Incident Response** — Includes our 24x7 security operations center and threat responders

Illustrative of our commitment to the security of our products and services, the centers of excellence report to the office of the Chief Security Officer (CSO), who coordinates all current security efforts and develops the vision for the future evolution of security at Adobe.

The Adobe Security Organization

Based on a platform of transparent, accountable, and informed decision-making, the Adobe security organization brings together the full range of security services under a single governance model. At a senior level, the CSO closely collaborates with the Chief Information Officer (CIO) and Chief Privacy Officer (CPO) to help ensure alignment on security strategy and operations.

In addition to the centers of excellence described above, Adobe embeds team members from legal, privacy, marketing, and PR in the security organization to help drive transparency and accountability in all security-related decisions.
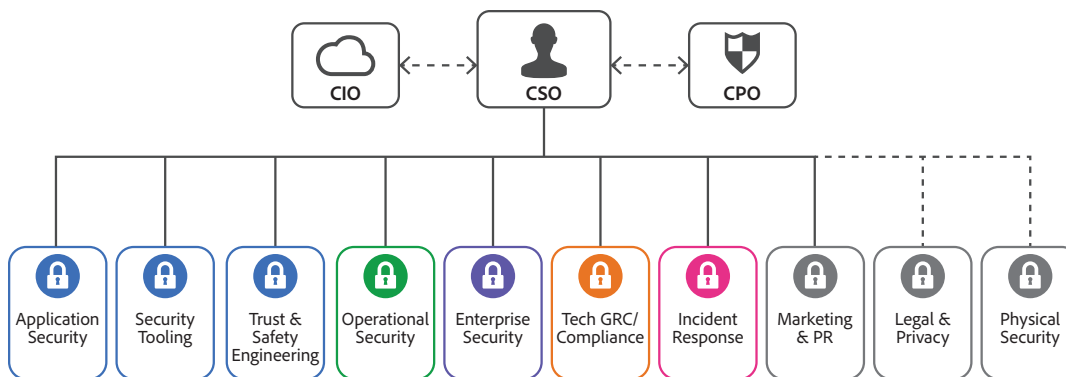
Figure 3: The Adobe Security Organization

As part of our company-wide culture of security, Adobe requires that every employee completes our security awareness and education training, which requires completion and recertification on an annual basis, helping ensure that every employee contributes to protecting Adobe corporate assets as well as customer and employee data. On hire, our technical employees, including engineering and technical operations teams, are auto-enrolled in an in-depth "martial arts-style" training program, which is tailored to their specific roles. For more information on our culture of security and our training programs, please see the Adobe Security Culture white paper.

The Adobe Secure Product Lifecycle

Integrated into several stages of the product lifecycle—from design and development to quality assurance, testing, and deployment— the Adobe Secure Product Lifecycle (SPLC) is the foundation of all security at Adobe. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC defines clear, repeatable processes to help our development teams build security into our products and services and continuously evolves to incorporate the latest industry best practices.
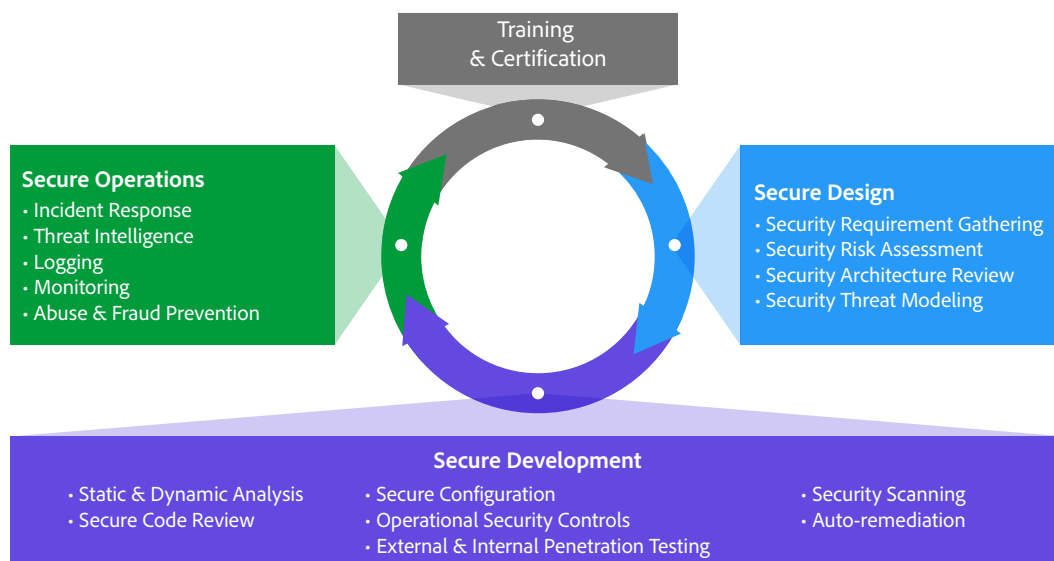

Figure 4: The Adobe Secure Product Lifecycle

Adobe maintains a published Secure Product Lifecycle Standard that is available for review upon request. More information about the components of the Adobe SPLC can be found in the Adobe Application Security Overview.

Adobe Application Security

At Adobe, building applications in a "secure by default" manner begins with the Adobe Application Security Stack. Combining clear, repeatable processes based on established research and experience with automation that helps ensure consistent application of security controls, the Adobe Application Security Stack helps improve developer efficiency and minimize the risk of security mistakes. Using tested and pre-approved secure coding blocks that eliminate the need to code commonly used patterns and blocks from scratch, developers can focus on their area of expertise while knowing their code is secure. Together with testing, specialized tooling, and monitoring, the Adobe Application Security Stack helps software developers to create secure code by default.

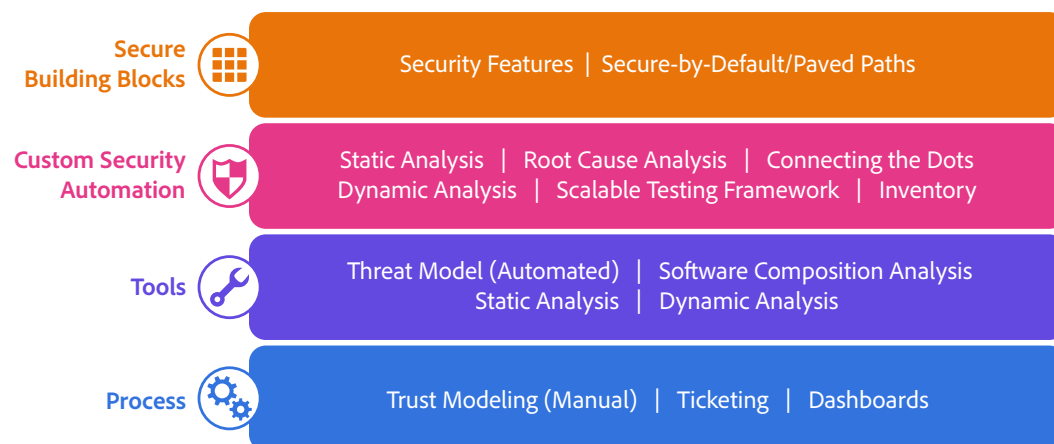|	
Secure Building Blocks	Security Features | Secure-by-Default/Paved Paths
Custom Security Automation	Static Analysis | Root Cause Analysis | Connecting the Dots Dynamic Analysis | Scalable Testing Framework | Inventory
Tools	Threat Model (Automated) | Software Composition Analysis Static Analysis | Dynamic Analysis
Process	Trust Modeling (Manual) | Ticketing | Dashboards

Figure 5: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of public cloud infrastructure. These standards are available for view upon request. For more information on Adobe application security, please see the Adobe Application Security Overview.

Adobe Operational Security

To help ensure that all Adobe products and services are designed from inception with security best practices in mind, the operational security team created the Adobe Operational Security Stack (OSS). The OSS is a consolidated set of tools that help product developers and engineers improve their security posture and reduce risk to both Adobe and our customers while also helping drive Adobe-wide adherence to compliance, privacy, and other governance frameworks.

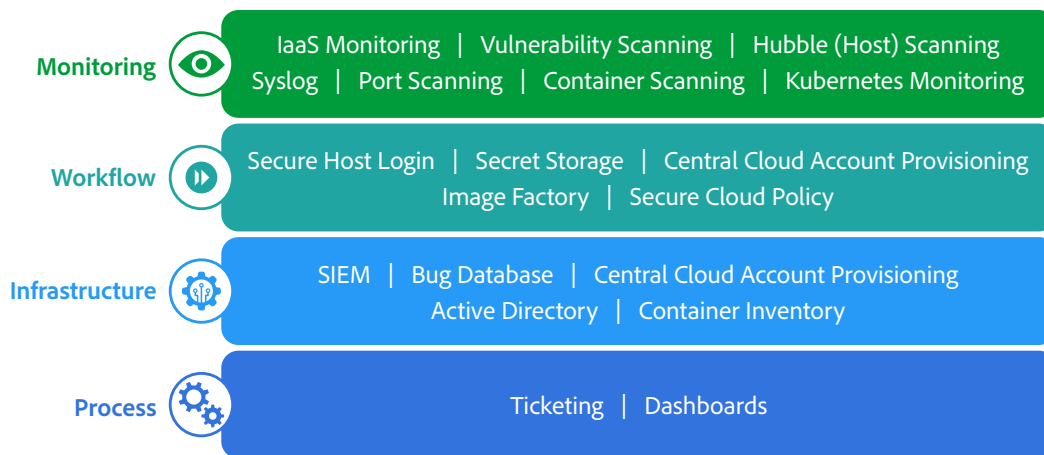| Monitoring | IaaS Monitoring \| Vulnerability Scanning \| Hubble (Host) Scanning Syslog \| Port Scanning \| Container Scanning \| Kubernetes Monitoring |
Workflow	Secure Host Login | Secret Storage | Central Cloud Account Provisioning Image Factory | Secure Cloud Policy
Infrastructure	SIEM | Bug Database | Central Cloud Account Provisioning Active Directory | Container Inventory
Process	Ticketing | Dashboards

Figure 6: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. For a detailed description of the Adobe OSS and the specific tools used throughout Adobe, please see the Adobe Operational Security Overview.

Adobe Enterprise Security

In addition to securing our products and services as well as our cloud hosting operations, Adobe also employs a variety of internal security controls to help ensure the security of our internal networks and systems, physical corporate locations, employees, and our customers' data.

For more information on our enterprise security controls and standards we have developed for these controls, please see the Adobe Enterprise Security Overview.

Adobe Compliance

All Adobe products and services adhere to the Adobe Common Controls Framework (CCF), 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. As much as possible, Adobe leverages leading-edge automation processes to alert teams to possible non-compliance situations and help ensure swift mitigation and realignment.

Adobe products and services either meet applicable legal standards or can be used in a way that enables customers to help meet their legal obligations related to the use of service providers. Customers maintain control over their documents, data, and workflows, and can choose how to best comply with local or regional regulations, such as the General Data Protection Regulation (GDPR) in the EU.

Adobe also maintains a compliance training and related standards that are available for review upon request. For more information on the Adobe CCF and key certifications, please see the Adobe Compliance, Certifications, and Standards List.

Incident Response

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution processes are 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.

We also maintain internal standards for incident response and vulnerability management that are available for view upon request. For more detail on Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

Business Continuity and Disaster Recovery

The Adobe Business Continuity and Disaster Recovery (BCDR) Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which help ensure the continued availability and delivery of Adobe products and services. Our ISO 22301-certified BCDR Program enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions. More information can be found in the Adobe Business Continuity and Disaster Recovery Program Overview.

Conclusion

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

For more information about Adobe security, please go to the Adobe Trust Center.

Information in this document is subject to change without notice. For more information on Adobe solutions, controls, and licensing options, please contact your Adobe sales representative.