Adobe Creative Cloud for teams Security Overview

Table of contents

Adobe Security

At Adobe, we take the security of your digital experience seriously. From our rigorous integration of security into our internal software development process and tools to our cross-functional incident response teams, we strive to be proactive and nimble. What's more, our collaborative work with partners, researchers, and other industry organizations helps us understand the latest threats and security best practices, as well as continually build security into the products and services we offer.

This white paper describes the proactive approach and procedures implemented by Adobe to increase the security of your Creative Cloud experience and your data.

About Creative Cloud for teams

Creative Cloud for teams includes the entire collection of Creative Cloud desktop applications (such as Adobe Photoshop CC, Adobe Illustrator CC, etc.) plus services and business features for teams and small to medium-sized organizations. Creative Cloud for teams is available via two plans — complete and single app — both of which are easily purchased, managed, and deployed via an intuitive Admin Console.

Creative Cloud for teams Storage and Storage Options

With Creative Cloud for teams, each complete membership includes up to 100 GB of cloud-based storage (single app members get 20GB) using Amazon S3 (Amazon Simple Storage Service), which provides a highly reliable data storage infrastructure for storing and retrieving data.

While the default storage option stores customer data in the cloud, customers can choose not to store on the cloud or to block the network connection within their corporate network. More information on *storage options* can be found on the Adobe.com website.

Administrative Tools for Creative Cloud for teams

Admin Console

Creative Cloud for teams includes a web-based Admin Console for IT administrators to easily purchase seats, add users, manage licenses, and deploy the Creative Cloud applications and updates. Administrators send emails asking users to create their own Adobe IDs.

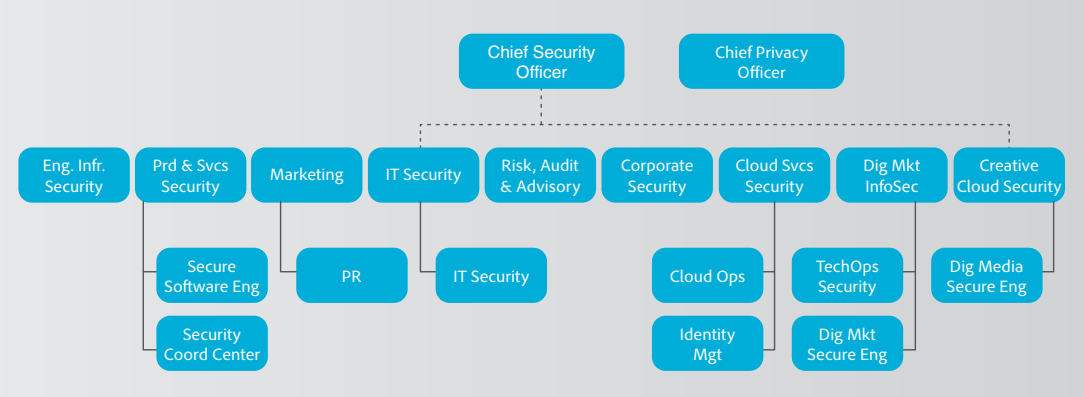
Creative Cloud Packager

Available via the Creative Cloud for teams Admin Console, Creative Cloud Packager is a tool that enables IT administrators to centrally deploy all – or a customized subset of – the Creative Cloud applications. Creative Cloud Packager ensures that every user is on the same version of the software, saving support costs, and eliminating multiple users downloading the same software at the same time, reducing network congestion. IT administrators log into Creative Cloud Packager using their Adobe ID, which they create when first registering for a Creative Cloud for teams plan. More information on *Creative Cloud Packager* and *deployment options* can be found on the Adobe.com website.

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 Creative Cloud teams. 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

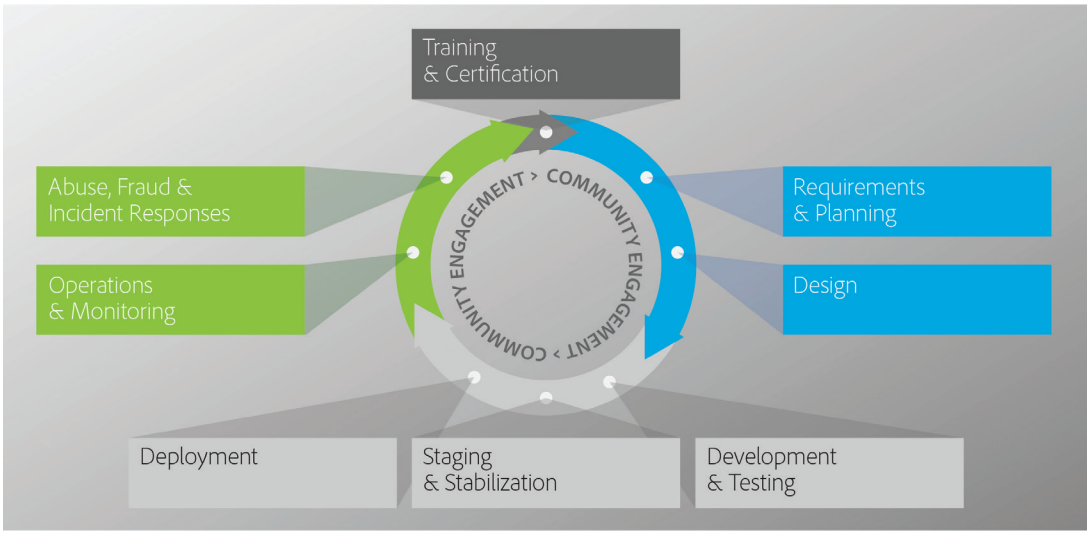
Adobe Secure Product Development

As with other key Adobe product and service organizations, the Creative Cloud organization employs the Adobe Secure Product Lifecycle (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 Creative Cloud service, some or all of the following recommended 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 Creative Cloud security team to help address the Open Web Application Security Project (OWASP) Top 10 most critical web application security flaws 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
- User-generated content validation
- Static and dynamic code analysis
- Application and network scanning
- Full readiness review, response plans, and release of developer education materials



Adobe Secure Product Lifecycle (SPLC)

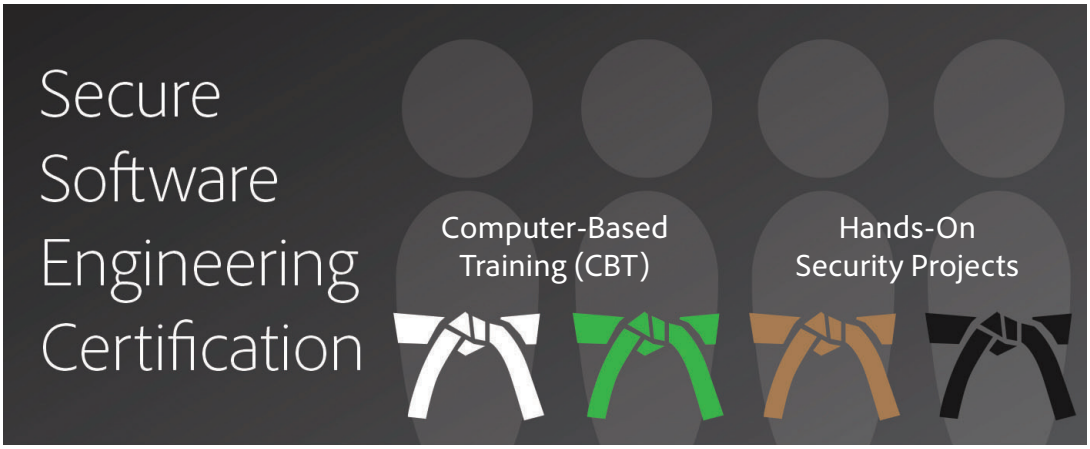
Adobe Security Training

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.

The program has four levels, each designated by a colored 'belt': white, green, brown, and black. The white and green levels are achieved by completing computer-based training. The higher brown and black belt levels require completion of months- or year-long hands-on security projects. Employees attaining brown and black belts become security champions and experts within their product teams. Adobe updates training on a regular basis to reflect new threats and mitigations, as well as new controls and software languages.

Various teams within the Creative Cloud organization participate in additional security training and workshops to increase awareness of how security affects their specific roles within the organization and the company as a whole.



Adobe Software Security Certification Program

Creative Cloud Architecture

Adobe is working toward a converged, hosted infrastructure for all Creative Cloud for teams components; however, the company currently utilizes two (2) primary hosting infrastructures for various components of Creative Cloud for teams:

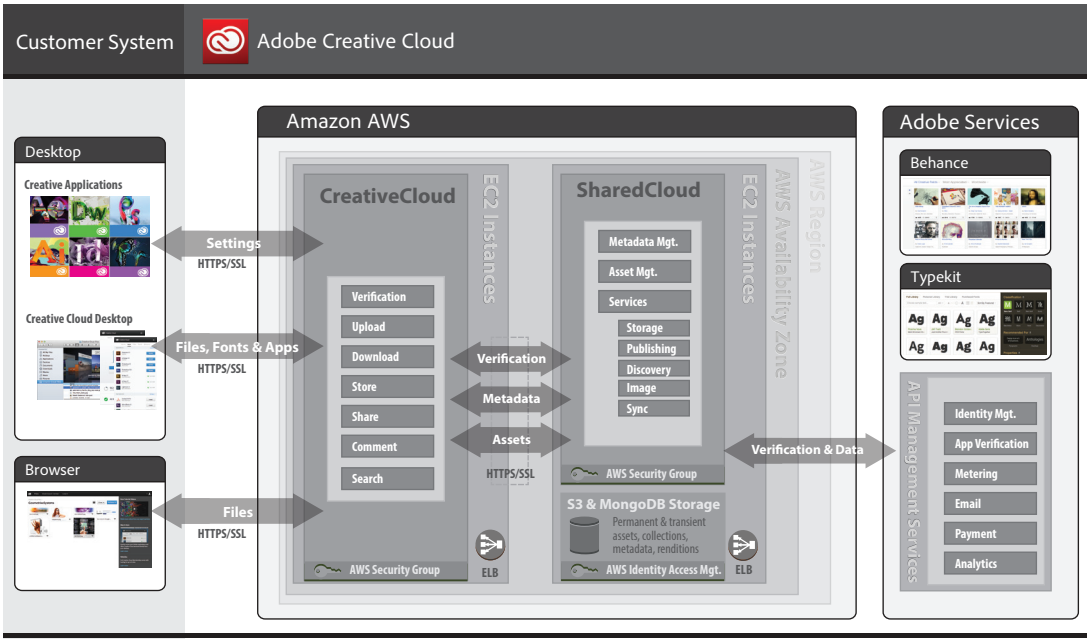
- Amazon Web Services (AWS): Most components of Creative Cloud for teams are hosted on AWS, including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3), in the United States, EU, and Asia Pacific. Amazon EC2 is a web service that provides automatically scalable compute capacity in the cloud, making web-scale computing easier. Amazon S3 is a highly reliable data storage infrastructure for storing and retrieving any amount of data.

  AWS offers a reliable platform for software services used by thousands of businesses worldwide, provides services in accordance with security best practices, and undergoes regular industry-recognized certifications and audits. More information can be found in the *AWS Security White Paper*.

- Leased Data Center Facilities: Adobe also currently hosts some services for Adobe Creative Cloud, including Adobe ID, in secure, unmarked, leased data center facilities. These data centers employ industry standard infrastructure and physical security measures.

* Adobe Behance, an online platform to showcase and discover creative work, resides on a secure, leased data center owned by Rackspace.

* Typekit is hosted on both *Rackspace* and AWS. Rackspace hosts the Typekit web application in its Chicago data center. The web application interacts with source fonts, which are stored on AWS, and creates custom font "kits." In most instances, these kits reside on AWS, although some customers have custom kit origin servers hosted by Rackspace.



Creative Cloud for teams Logical Architecture

Creative Cloud applications are built on the Adobe Shared Cloud platform within AWS. Uploaded files are processed by an Amazon Elastic Compute Cloud (EC2) instance and stored in an Amazon Simple Storage Service (S3) bucket that's protected by Identity and Access Management (IAM) roles within an AWS Region. As part of the S3 redundancy functionality, files are replicated across AWS Availability zones for backup.

The Creative Cloud includes a set of services that allow validated users access to desktop and web applications.

As a whole, these services and applications are accessed from a customer system through three endpoints:

- Applications, such as Adobe Photoshop
- The Creative Cloud desktop application
- A browser

The services available are dependent on how the customer is accessing the Adobe Creative Cloud. For example, the individual applications can access the Creative Cloud to validate the user, synchronize settings, and, optionally, share content through Adobe Behance. Similarly, the Creative Cloud desktop application allows users to download and update their desktop applications, download web fonts through Typekit, and upload or download files to their local system from Creative Cloud storage.

Regardless of the customer endpoint, all Creative Cloud access is controlled through a public set of services available on Adobe.com. Once a user has been validated, he/she can then perform whichever actions are allowed by his/her endpoint. You can find a description of the *tools and services available* on the Adobe.com 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 Creative Cloud for teams components 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 operational software (e.g., host OS, virtualization software, etc.), which supports the provisioning and use of these resources. Amazon designed and manages according to security best 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.

About Amazon Web Services (AWS)

Geographic Location of Customer Data on AWS Network
For customer data stored in the cloud in Amazon S3, Adobe designates the physical region in which individual customers' data and servers are located. Adobe operates Creative Cloud out of three regions: United States, EU, and Asia Pacific. 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. Content that customers store in Creative Cloud is not replicated to other data centers in other regions. For example, by default, Creative Cloud stores all EU customer content uploaded to Creative Cloud in the EU.

Isolation of Customer Data/Segregation of AWS Customers
Creative Cloud data stored by Adobe on AWS includes strong tenant isolation security and control capabilities. As a virtualized, multi-tenant environment, AWS implements security management processes and other security controls designed to isolate each customer, such as Creative Cloud, from other AWS customers. AWS Identity and Access Management (IAM) is used to further lock down access to compute and storage instances.

Secure Transmission
Adobe submits a REST/Query request over HTTP/HTTPS, or calls a wrapper function in one of the AWS SDKs, to connect to an AWS access point. HTTPS uses Secure Sockets Layer (SSL), a cryptographic protocol designed to protect against eavesdropping, tampering, and message forgery. Adobe uploads data to and downloads data from Amazon S3 via the SSL encrypted endpoints. Accessible both from the Internet and from within Amazon EC2, the encrypted endpoints enable data to transfer securely within AWS as well as to and from sources outside of AWS.

Secure Network Architecture
AWS employs network devices, including firewall 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 (ACL), 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 AWS's 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

You can find more information about Network Monitoring and Protection in the *AWS Security Whitepaper* on the Amazon website.

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

Data Storage and Backup
Creative Cloud for teams stores data in Amazon S3, which provides a storage infrastructure with 99.999999999% durability and 99.99% availability of objects over a given year, according to Amazon. 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. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data.

Change Management
AWS authorizes, logs, tests, approves, and documents routine, emergency, and configuration changes to existing AWS infrastructure in accordance with industry norms 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 a *Status Health Dashboard* for Creative 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.

Creative Cloud for teams Authentication (Adobe ID)

After receiving an invitation to join the team from their administrator, users must create an Adobe ID, which is used each time they access Creative Cloud for teams. Adobe ID leverages the SHA 256 hash algorithm in combination with password salts and a large number of hash iterations. Adobe continually monitors Adobe ID accounts for unusual or anomalous account activity and evaluates this information to help quickly mitigate threats to the security of your Adobe ID account.

Adobe Risk & Vulnerability Management

Penetration Testing
Adobe engages with approved third-party vendors to perform penetration testing that can uncover potential security vulnerabilities and improve the overall security of Adobe products and services. The vendors complete the tests according to industry best practices. Upon receipt of the report provided by the third party, Adobe documents these vulnerabilities, evaluates severity and priority, and then creates a mitigation strategy or remediation plan.

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

When a significant announced vulnerability puts the Adobe Creative Cloud at risk, the Adobe PSIRT (Product Security Incident Response Team) communicates the vulnerability to the appropriate teams within the Creative Cloud organization to coordinate the mitigation effort.

For incidents, vulnerabilities, and threats that impact the AWS Data Center, the Amazon Incident Management team employs industry-standard diagnostic procedures to drive resolution during business-impacting events. Staff operators provide 24x7x365 coverage to detect incidents, manage the impact and resolution, and inform Adobe and other AWS customers.

For Adobe cloud-based services, including Adobe Creative Cloud, we centralize incident response, decision-making, and external monitoring in our Security Coordination Center (SCC), providing cross-functional consistency and fast resolution of issues.

When an incident occurs with an Adobe product or service, the SCC works with the involved Adobe product incident response and development teams to help identify, mitigate, and resolve the issue using the following proven process:

- Assess the status of the vulnerability
- Mitigate risk in production services
- Quarantine, investigate, and destroy compromised nodes (cloud-based services only)
- Develop a fix for the vulnerability
- Deploy the fix to contain the problem
- Monitor activity and confirm resolution

Forensic Analysis
For incident investigations, Adobe uses industry-standard tools and methodologies. The company adheres to a forensic analysis process that includes complete image capture or memory dump of an impacted machine(s), evidence safe-holding, and chain-of-custody recording. Adobe may engage with law enforcement or third-party forensic companies when it determines it is necessary.

AWS Data Center Physical and Environmental Controls

AWS physical and environmental controls are specifically outlined in a SOC 1, Type 2 report. The following section outlines some of the security measures and controls in place at every AWS data center around the world. You can find more detailed information about AWS and *Amazon's security controls* on the Amazon security website.

Physical Facility Security
AWS data centers utilize state-of-the-art, innovative architectural and engineering approaches. Amazon applied its many years of experience designing, constructing, and operating its own large-scale data centers to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and Amazon strictly controls physical access both at the perimeter and at building ingress points using professional security staff, video surveillance, intrusion detection systems, 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 Amazon Web Services. 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 utilizes 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 back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Video Surveillance
Professional security staff strictly controls physical access both at the perimeter and at building ingress points for AWS Data Centers using video surveillance, intrusion detection systems, and other electronic means.

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 24/7/365 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. You can find more information about *AWS disaster recovery protocols* on the Amazon Security website.

Adobe Corporate Locations

Adobe maintains offices around the world and implements the following processes and procedures company-wide to protect the company against security threats:

Physical 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 at all times. 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 in-bound and out-bound corporate email for known malware threats.

Adobe Employees

Employee Access to Customer Data
Adobe maintains segmented development and production environments for Creative 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.

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; 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 U.S., 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 no longer access Adobe confidential files or offices:

- Email Access Removal
- Remote VPN Access Removal
- Office and Datacenter Badge Invalidation
- Network Access Termination

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

Customer Data Confidentiality

Adobe always treats 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*.

Security Compliance

Amazon Web Services (AWS) and Rackspace maintain their own compliance and assertions with an ISO27001, SOC2, and other industry Security Frameworks.

Adobe is currently in the process of developing, implementing, and refining the security processes and controls for Creative Cloud operations in order to comply with the requirements for SOC2 Trust principles and the ISO 27001 security standard.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of your Creative Cloud data. At Adobe, we take the security of your digital experience seriously.

For more information, please visit: *http://www/adobe.com/security*

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

4/14