Adobe Creative Cloud for enterprise security overview

Executive Summary
Adobe Creative Cloud for enterprise gives large organizations access to Adobe’s creative desktop and mobile apps, cloud services, workgroup collaboration, and license management tools. It also includes flexible deployment, identity management options including Federated ID with Single Sign-On, annual license true-ups, and enterprise-level customer support — and it works with other Adobe enterprise offerings.

At Adobe, we take the security of your digital assets 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.

We have architected Creative Cloud for enterprise with security considerations at its core. Access to Creative Cloud for enterprise, whether it’s a desktop application or cloud service, is controlled by a unique user ID that is managed by an Admin Console, and may be tied into your enterprise directory services. Content is encrypted both in transit and at rest, and content at rest can be further protected by utilizing a customer-specific encryption key.

Adobe services that touch customer content have either completed, or are in the certification stage of obtaining SOC 2, ISO27001, and PCI (where appropriate) certifications. Our cloud services are protected, managed and monitored by state of the art solutions and we utilize industry standard software security methodologies for both management and development lifecycles.

Adobe utilizes best-of-breed hosting through Amazon Web Services (AWS) in a multi-region, multi-datacenter configuration to provide you with constantly replicated data backup so that your content is available when you need it.

This whitepaper describes our proactive approach as well as the procedures and the security architecture implemented by Adobe to help increase the security of your Adobe Creative Cloud experience and your data.

Creative Cloud for enterprise overview
Creative Cloud for enterprise is a creative production solution for enterprise creative and design teams to utilize for their work-in-progress workflows. It consists of four parts: 1) desktop apps, 2) mobile apps, 3) an Admin Console, and 4) a set of cloud services.

Desktop Applications
The desktop apps, like Adobe Photoshop and Illustrator, run on the end-user workstation. They may either be packaged for deployment by IT and deployed via standard methods such as Microsoft SCCM/JAMF Casper Suite or utilized in a self-service scenario where end-users download the apps from Adobe directly. Each user is assigned a license via the Admin Console based on their identity (such as an LDAP or Microsoft Active Directory ID), and each user is assigned application and service entitlements via the Console as well. When a user launches an app such as Photoshop, the app pings the Admin Console to determine if that user is entitled to use that application. Data transmissions are encrypted and user information is handled using industry standards and best practices for security and privacy.

Mobile Apps
The mobile apps, such as Adobe Photoshop Sketch CC and Adobe Comp CC, run on an end-user’s mobile device and they may be managed by a Mobile Device Management (MDM) solution such as AirWatch. Content created by the mobile applications lives both on the mobile device, as well as in the cloud in encrypted storage (see Creative Services below for more details). Data transmissions are encrypted and access to the mobile services is determined by user identity as configured in the Admin Console.
Admin Console
The Admin Console is used to configure license and service entitlements. The Console can tie into your SAML2.0 compliant enterprise identity management system for authentication and provides a set of APIs for automated authorization. IT can setup product license groups to either mirror your enterprise directory groupings or they can be separate, tied in specifically to your creative workgroups. If you are using the cloud services as described below, the Admin Console is also where you can control your dedicated encryption key and revoke all content access, if required. Communication with the Admin Console is encrypted and administrator access is limited to key users who are set up at the start of the contract term.

Cloud Services
The cloud services include numerous productivity features that help creative users be more efficient and deliver results more rapidly. These include services that enable designers to access files, collaborate on projects, and access fonts and stock images so they can create their best work. Cloud services are entitled using the Admin Console, and access to each service is based on every user’s unique identification, so only users entitled to a service may access it. The cloud services run on a multi-tenant infrastructure built on Amazon’s AWS. Data transmissions are encrypted and user generated content is encrypted at rest, and, as noted above, may be additionally encrypted with a dedicated encryption key.

Creative Cloud for enterprise identity systems
Entitlement and Identity Management
IT administrators entitle end user access to the Creative Cloud desktop applications such as Adobe Photoshop and Adobe Illustrator as well as entitling the use of cloud services by utilizing named user licensing in the Adobe Admin Console.

Three types of named user licensing are available:

- **Adobe ID** is for Adobe-hosted, user-managed accounts that are created, owned and controlled by individual users. Adobe ID accounts only have access to Creative Cloud for enterprise resources if an IT administrator enables access.

- **Adobe Enterprise ID** is an Adobe-hosted, enterprise-managed option for accounts that are created and controlled by IT administrators from the customer enterprise organization. The organization owns and manages the user accounts and all associated assets.

- **Adobe Federated ID** is 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, controlled by IT as well as all associated assets. Adobe will integrate with most any SAML2.0 compliant identity provider.

Application and service entitlement is accomplished through the Adobe Admin Console.

Password Lockout Procedures
IT can enforce password policies for invited Adobe IDs with access to enterprise resources, Enterprise IDs, and Federated IDs with three different password policies, shown here:

![Password Lockout Procedures Table]

Adobe Creative Cloud for enterprise Security Brief
Adobe IDs and Enterprise IDs 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 their security. For Federated ID accounts, because Adobe does not manage the users' passwords, Adobe does not monitor account activity.

**Account management**

Named user accounts can be managed through the Adobe Admin Console, which is an intuitive Console for IT staff to manage their organization’s Adobe entitlements, controlling which users and groups have access to certain Creative Cloud apps and services. The Adobe Admin Console also provides user management and entitlement access to Adobe Document Cloud and Adobe Marketing Cloud. IT staff can also utilize the Console to open support cases with Adobe Customer Care, schedule Expert Services sessions and resolve issues quickly.

IT can create, manage, and delete Enterprise ID and Federated ID accounts through the Adobe Admin Console. Cloud storage for these accounts is allocated as individual storage; hence, IT does not have direct access to any files in the user’s Creative Cloud storage. However, IT can assume ownership of the employee’s account and can revoke access. Deleting an Enterprise ID or Federated ID with existing shared services storage renders any data in remote storage inaccessible to the user and that user’s data will be deleted after 90 days.

IT may also allocate storage to Adobe ID accounts via the Adobe Admin Console. IT cannot control Adobe ID accounts, but they can delete them from their enterprise, removing the granted enterprise storage quota from their accounts, with the data also being deleted after 90 days.

Adobe Creative Cloud for enterprise is a combination of desktop apps, mobile apps, and cloud services. Creative Cloud for enterprise users who are provisioned via named user deployment will access the cloud services from one or more of three endpoints:

- Desktop apps such as Adobe Photoshop and the Creative Cloud desktop application
- A web browser
- Mobile apps such as Adobe Capture CC, Adobe Photoshop Sketch and Adobe Lightroom Mobile


From the endpoint, a user will validate their identity using one of the methods of named user entitlements as described above and access their content through Creative Cloud for enterprise.

The services available are dependent on which endpoint the customer is using to access Adobe Creative Cloud. For example, the mobile apps can access the Creative Cloud to validate the user, to synchronize settings, and to share content such as mobile creations. Similarly, the Creative Cloud desktop application allows user to download and update their creative desktop applications, such as Photoshop, download fonts through Adobe Typekit, and upload or download files to their local system from the Creative Cloud storage.
Regardless of the customer endpoint, all Creative Cloud access is controlled through a public set of services access via HTTPS/SSL. Content is encrypted in-transit with AES 128-bit GCM symmetric key cryptographic block ciphers and at rest with AES 256-bit symmetric security keys utilizing FIPS 140-2 approved cryptographic algorithms consistent with NIST 800-57 recommendations. Once a user has validated themselves to Adobe Creative Cloud for enterprise, they will access the services and apps to which their IT administrators have entitled them through the Adobe Admin Console. They can then perform whichever actions are allowed by their endpoint for which they have been entitled. For example, a user in Photoshop will be able to collaborate using Creative Cloud Libraries and share colors, graphics and type styles with other members of their team.

**Creative Cloud for enterprise content storage**

Creative Cloud for enterprise leverages multi-tenant storage. Customer content is processed by an Amazon Elastic Compute Cloud (EC2) instance and stored on a combination of Amazon Simple Storage Services (S3) buckets and through a MongoDB instance on an Amazon Elastic Block Store (EBS).

The content itself is stored in S3 buckets and the metadata about the content is stored in MongoDB, all protected by Identity and Access Management (IAM) roles within that AWS Region.

The content and assets stored in S3 are encrypted with AES 256-bit symmetric security keys that are unique to each customer and each customer’s claimed domain. The dedicated keys are managed by the Amazon Key Management Service (KMS) which provides additional layers of control and security for key management and Adobe will automatically rotate the key on an annual basis. If necessary, IT administrators can revoke their key via the Admin Console, which will render all data encrypted with that key inaccessible to the end users. Please see Dedicated Encryption Key below for more details.

Metadata and support assets which are stored in EBS have AES 256-bit encryption utilizing 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 with the loss of data in two locations.

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

- MongoDB: [http://www.mongodb.org](http://www.mongodb.org)
- Amazon S3 service: [https://aws.amazon.com/s3/faqs](https://aws.amazon.com/s3/faqs)

**Dedicated Encryption Key**

Content stored in the Creative Cloud for enterprise is encrypted as noted above. IT administrators can add an additional layer of control and security by having Adobe generate a dedicated encryption key for some or all of the domains in your organization. Content is then encrypted using that dedicated encryption key, and, if required, you can revoke the encryption key from the Admin Console. Revoking the key will render all content encrypted with that key inaccessible to the end user.

For more information on managing encryption using a dedicated key, please see:

**Creative Cloud services types**
Creative Cloud services included SaaS-based services, some of which can store user generated content and may be utilized by all Creative Cloud for enterprise services and endpoints if so entitled. End user access and entitlement to these services can be managed by an IT administrator via the Adobe Admin Console. For more information on the Creative Cloud services please see:

- Adobe Portfolio: [https://www.myportfolio.com/](https://www.myportfolio.com/)
- Behance: [https://www.behance.net/](https://www.behance.net/)
- Phonegap Build: [https://build.phonegap.com/](https://build.phonegap.com/)
- Share Online: [http://adobe.ly/2bYysLs](http://adobe.ly/2bYysLs)
- Typekit: [https://typekit.com/](https://typekit.com/)

**Amazon Web Services**
As previously covered, components of Creative Cloud for enterprise are hosted on AWS, including Amazon EC2 and Amazon S3, in the United States, the European Union (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.

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 security site](https://aws.amazon.com/security/).

**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 Creative Cloud for enterprise operates. 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 (e.g., host OS, virtualization software, etc.) 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 AWS Network**
The following information is from the AWS: Overview of Security Processes White paper. For more detailed information about AWS security, please consult the [AWS white paper](https://aws.amazon.com/security/).

Adobe stores all Adobe Creative Cloud customer data in Amazon Web Services’ US East Region. For customers within the United States, Adobe stores analytic data in AWS’s San Jose, California or Dallas, Texas facilities. For customers outside the U.S., Adobe stores analytic data in the London, U.K. facility of AWS.

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.
Isolation of Customer Data/Segregation of Customers
AWS uses 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 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 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: Overview of Security Processes white paper on the Amazon website.

Intrusion Detection
Adobe actively monitors Adobe Creative Cloud using industry-standard Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS).

Logging
Adobe conducts server-side logging of Adobe Creative Cloud 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 Creative Cloud 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. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper.

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 Console when service use is likely to be adversely affected. Adobe also maintains a Status Health Console for Adobe 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.

AWS 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 AWS data centers around the world. For more detailed information about AWS security, please consult the AWS: Overview of Security Processes white paper or the Amazon security website.

Physical Facility Security
AWS data centers utilize 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, 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 they continue 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 Common Controls Framework

To protect from the software layer down, Adobe uses the Adobe Secure Product Lifecycle, which is described in a following section. To protect from the physical layer up, Adobe implements a foundational framework of security processes and controls to protect the company’s infrastructure, applications, and services and help Adobe comply with a number of industry accepted best practices, standards, and certifications.

In creating the Adobe Common Controls Framework (CCF), Adobe analyzed the criteria for the most common security certifications and found a number of overlaps. After analyzing more than 1000 requirements from relevant cloud security frameworks and standards, Adobe rationalized these down to approximately 200 Adobe-specific controls. The CCF control owners know exactly what is required to address the expectations of Adobe stakeholders and customers when it comes to implementing controls.

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 specialists who serve as consultants to key Adobe product and operations teams, including the 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 secure product development
As with other key Adobe product and service organizations, the Creative Cloud organization employs the 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 some or all of the following recommended practices, processes, and tools, depending on the specific Creative Cloud service:

- 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.

<table>
<thead>
<tr>
<th>Belt</th>
<th>Certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black</td>
<td>The highest level of hands-on security expertise within Adobe</td>
</tr>
<tr>
<td>Brown</td>
<td>Focused on the development of security components in Adobe product code (e.g. sandboxing)</td>
</tr>
<tr>
<td>Green</td>
<td>Builds on basic security topics through real-world case studies</td>
</tr>
<tr>
<td>White</td>
<td>Introduces basic security concepts</td>
</tr>
</tbody>
</table>

Adobe Secure Software Engineering Certification Levels

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

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

Adobe risk and vulnerability management

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 severity and priority, and then creates a mitigation strategy or remediation plan.

Internally, the Adobe Creative Cloud security team performs a risk assessment of the Creative Cloud prior to every release. Conducted by highly trained security staff trusted with securing the network topology and infrastructure; the security reviews look for insecure network setup issues across firewalls, load balancers, and server hardware and also application level vulnerabilities. The security touchpoints include exercises like threat modeling coupled with vulnerability scanning, static and dynamic analysis of the application. The Creative Cloud security team partners with the technical operations and development leads to help ensure all high risk vulnerabilities are mitigated prior to each release. Penetrations tests are conducted at least annually or after every major release. Vulnerability scans are performed monthly while web and database scans are performed quarterly.

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 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 Adobe cloud-based services, including Creative Cloud, Adobe centralizes 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, the Creative 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.

**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. Adobe keeps all server equipment, development machines, phone systems, file and mail servers, and other sensitive systems locked at all times in environmentally controlled server rooms accessible only by appropriate, authorized staff members.

**Virus protection**

Adobe scans all inbound and outbound corporate email for known malware threats. Anti-malware protection mechanisms are implemented for all systems and employee assets (e.g., laptops) commonly affected by malware (e.g., Windows servers but not Linux servers). Anti-malware protection requires the following:

- Scanning signatures are updated daily
- Scan engine version is updated to stay current with vendor releases
- Full system scans are run weekly
- Event logs and alerts are generated
- Issues identified from scanning results are available to authorized parties or groups
- Real time scanning is enabled
- Antivirus mechanisms cannot be disabled
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, and employees with no legitimate business purpose are restricted from accessing these systems. Access is given to employees using least privilege and access rights are reviewed quarterly.

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 access, use, or share the information collected from a customer except as set forth in the Adobe General Terms of Use and in the Adobe Privacy Policy. For more information on Adobe’s privacy practices, please visit the Adobe Privacy Center.

Security compliance
AWS maintains their own compliance and assertions with an ISO 27001, SOC 1, SOC 2, PCI DSS and other industry security frameworks.

All Adobe services are governed by a comprehensive set of documented security processes and have been subject to numerous security audits to maintain and improve quality. Adobe services are under continuing self review to ISO 27001 standards and the underlying services infrastructure has a SOC 2 - Security certification.
Adobe is 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 SOC 2 Trust Services Principles, and the ISO 27001 security standard. Adobe Creative Cloud for enterprise is currently “FERPA-ready” which means that under FERPA guidelines, Adobe can contractually agree to act as a “school official” when it comes to handling regulated student data and therefore to enable our education customers to comply with FERPA requirements.

Please visit http://www.adobe.com/security/resources.html to view a list of security white papers including the Adobe Cloud Services Compliance Overview whitepaper for more information on Adobe’s overall security and compliance strategy.

Conclusion
At Adobe, we take the security of your digital experience seriously. The proactive approach to security and stringent procedures described in this paper help protect the security of your Creative Cloud data. If you have additional security questions beyond what is covered here, please contact your account representative, or visit http://www.adobe.com/security.