Adobe Security

The availability, integrity and confidentiality of client data are of paramount importance to Adobe. To ensure the security of client data, Adobe has identified the organizational, network, hosting facility, corporate office, and employee processes as the areas in which to focus security efforts. This white paper describes the proactive approach and procedures followed to maximize the security of each area.

Organization

Security Organization

Adobe has the following organization in place to handle Security needs:

• Information Security Manager
• Information Security Team
• Physical Security Team
• Chief Information Security Officer
• Chief Privacy Officer
• Privacy Committee

The Information Security Manager is responsible for overseeing the security organizational needs of Adobe. This includes defining policy, creating controls, implementing procedures, handling incidents, conducting audits and reporting to management. At the executive level, the Information Security Manager reports under the CIO.

The Security Teams reports to the Information Security Manager and is staffed with qualified Security Engineers to carry out the needs of the organization. Members of the Security Team are expected to earn and maintain Certified Information Systems Security Professional (CISSP) certification, and receive specific training in the areas and on the security products they are responsible for.

The Chief Privacy Officer (CPO) oversees all ongoing activities related to the development, implementation, maintenance of, and adherence to the organization's policies and procedures covering the privacy of, and access to, employee and customer information in compliance with federal and state laws and the organization's information privacy practices.

The Privacy Committee is comprised of representatives from Legal, Client Services, Network Operations and Engineering to discuss matters involving privacy laws, regulations and customer data.

Information Security Policies

Adobe has developed company-wide Information Security policies using the ISO/IEC 17799/27002 standards as a framework. These policies are approved by management and accepted by all Adobe Employees.

The following policies and standards are defined:

• General Information Security Policy
• Network Security Policy
• Remote Access and Telecommunications Usage Policy
• Electronic Communications Policy
• Restricted Access Authorization Policy
• Login ID and Password Standard
• Code of Business Conduct

Additional Standards and Procedures are defined within the Adobe Marketing Cloud:

• Data Protection Standards
• Data Overwrite Procedures
• Live Network Access Procedures
• InfoSec Incident Response Procedures
• Vulnerability Management Procedures

Portions of these policies may be available for review by clients under NDA through a web session. Adobe policy prevents the sharing of these policies otherwise.

Vulnerability Management
Adobe follows major vulnerability announcement lists (e.g. US-CERT, Bugtraq, SANS, etc.) and vendor lists for the latest security alerts. If a vulnerability is announced that affects Adobe, the threat level and priority to address the vulnerability are determined and the mitigation effort is coordinated with the appropriate teams.

Audits
Adobe performs internal audits and works with third parties to perform security audits as an additional check against the policies, procedures and controls implemented by Adobe. These audits are performed at the corporate level, product level or against specific threats as identified. The results of third party audits performed for Adobe may be available to clients under NDA. Adobe also works with clients when additional audits are required.

Product Development
Adobe has an established development process that includes security standards, security code reviews, quality assurance testing and release controls. Security standards are developed using industry best practices and are updated to include current trends and threats. We strive to conform to OWASP standards for our Web Applications. Architecture security reviews are performed when needed by the Security Team to ensure proper controls are in place and security standards are followed.

Training
Adobe provides Security Awareness training to all employees, as well as more specific security training at a departmental level (e.g. Network Operations, Engineering, Client Services) when necessary.

Network
The security of the Adobe Marketing Cloud is highly important to Adobe because of the data collection, data content serving, and reporting activities taking place. Network security is ensured based upon the following approaches:
• Password protected user access
• Segregated client data
• Secure management
• Firewalls and load balancers
• Intrusion Detection
• Non-routable, private addressing
Password Protected User Access

In order for a client to access their data, he or she must authenticate with a username and password. All users are required to transmit this information over SSL-encrypted channels to prevent it from being intercepted. The Adobe Online Marketing Suite can restrict the types of passwords users can create to access the site. Passwords are created and administered by designated client administrators. When enabled, all system user passwords must meet all of the following criteria:

• Must be at least eight characters in length
• Has at least one symbol/number character between the first and last characters
• Has at least one alpha character
• Cannot be found in a dictionary or contain words from a dictionary (English)
• May not include any three (3) consecutive characters from the login username
• Must be different than the previous 10 passwords

Segregating Client Data

Data is placed into separate databases (report suites), and a single client’s site reports are grouped together on one or more servers. In some cases, more than one client may share a server, but the data is segmented into separate databases. The only access to these servers and databases is via secure access by the application. All other access to the application and data servers is made only by authorized Adobe personnel, and is conducted via encrypted channels over secure management connections. We separate our testing environments from our production environments, and we do not use customer data in testing environments unless specifically granted permissions by the customer.

Secure Management

All management connections to the servers occur over encrypted SSH, SSL, or VPN channels. Adobe has deployed dedicated network connections from our corporate offices to our data center facilities to allow secure management of our servers. Management access from the Internet is denied by default unless the connection originates from a list of trusted IP addresses.

Firewalls and Load Balancers

All Internet connections are filtered out by the firewalls, passing only those going to allowed ports (e.g. 80 and 443 for HTTP and HTTPS respectively). The firewalls also perform Network Address Translation (“NAT”, RFC 1631). NAT is a process that masks the true IP address of a server from the client connecting to it. The load balancers proxy incoming HTTP/HTTPS connections and also distributes requests to ensure that momentary load spikes can be handled. Both the firewalls and load balancers are fully redundant, greatly reducing the possibility that a single device failure can disrupt the flow of traffic.

Intrusion Detection

Network Intrusion Detection System (IDS) sensors are placed at critical points in the network to detect and alert on attempts to break into our network. The IDS is monitored and configured to automatically provide real-time notification to the Security Team. Sensors are regularly updated and monitored for proper operation.

Non-routable, Private Addressing

Adobe maintains all servers containing client data on servers with IP addresses that are not routable across the Internet (RFC 1918). In combination with the firewall and NAT, servers are not directly addressable from the Internet which greatly reduces the vectors of attack that can be tried against them.
Service Monitoring
All servers, routers, switches, load balancers, and other critical network equipment are monitored 24 hours a day. The software responsible for monitoring this system performs around one million health checks per hour probing for data integrity and service interruptions. Temperature probes and power monitoring equipment watch for temperature rises and power spikes to ensure the servers run in an optimal environment without local power interruption. Notifications are monitored by our 24x7 Network Operations Center, who will escalate to the appropriate on-call staff or management until the issue is resolved. Additionally, Adobe employs multiple independent monitoring services to provide several layers of monitoring redundancy.

Data Backups
Data backups are performed on a nightly basis to locally and remotely. This solution provides quick recovery from backup when required, as well as off-site protection of data.

Notifications
Notifications are sent to clients for the following types of situations.
• Scheduled maintenance requiring down time
• Outage conditions causing down time
• Security incidents affecting client data
Notifications will come from the ClientServices organization, to the designated client contacts.

Hosting Facility
Adobe takes our choice of co-location facilities seriously and requires all facilities to meet the requirements described in the following sections.

Physical Facility Security
All facilities include dedicated 24-hour on-site security personnel who require credentials to gain admittance to the facility. Adobe uses PIN or badge (or both) to authorize data center access. Remotely monitored and recorded video cameras provide continuous surveillance. Some facilities include the use of man-traps prevents unauthorized individuals from tailgating into the facility. Access to a facility is only granted if the individual is on the approved list and all access to the facility is logged.

Fire Suppression
The facilities employ air-sampling smoke detector systems (such as VESDA) that alert facility personnel at the first sign of a fire, and pre-action, dry-pipe sprinkler systems with double interlock to ensure no water is released into a server area without the activation of a smoke detector and the presence of heat.

Controlled Environment
The facilities are environmentally controlled for temperature, humidity, and fluid detection. The HVAC system is completely redundant and facility teams are available 24 hours a day, every day, to deal with any problems. Environmental monitors alerts the NOC if the environment moves outside of desired parameters.

Backup Power
All facilities provide 100% of the power necessary to run independently of any other power supply. Multiple power feeds from independent power distribution units ensures continuous power delivery. Transition from primary power to backup power is fully automatic and occurs without interruption of service. Redundancy exists at every level, including generators and diesel fuel contracts. Regular testing of the generators under load ensures equipment is ready when needed.

Video Surveillance
All Adobe contracted hosting facilities have video surveillance in place to monitor at least entry and exit point access, and wherever possible, physical access to equipment. Adobe may review video logs when issues or concerns arise to determine access.

Offices
Adobe maintains office around the world. The following procedures represent the processes Adobe has implemented to protect against security threats:

Onsite Guards
Adobe has onsite guards to protect the premises 24x7.

Virus Protection
All desktops/laptops run real-time virus scanning software which is automatically updated with the latest signatures, with no intervention required from the end user. Additionally, all in-bound and out-bound email is scanned for known malware threats.

Building Access
All employees are issued a key card ID badge for building access. Visitors must enter through the front entrance, sign in and out with the receptionist, have a temporary Visitor ID badge, and be accompanied by an employee at all times. Server equipment, development machines, phone systems, file and mail servers and other sensitive systems are further kept locked at all times in an environment-controlled server room accessible only to the appropriate staff.

Video Surveillance
Video cameras are placed in entry and exits points for review by security staff.

Adobe Employees

Background Checks
Adobe obtains consumer 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 record; and references obtained from professional and personal associates, each as permitted by applicable law.
Adobe currently uses HireRight, Inc., 2100 Main Street, Suite 400, Irvine, CA 92614, to provide its U.S. background check reports.
Adobe also uses e-verify, a web-based system operated by US Citizenship and Immigration Services (USCIS) and the Social Security Administration (SSA) which enables Adobe to verify employment eligibility of job applicants and their Social Security numbers.
These background check requirements apply to regular US 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.

Employee Termination
In the event Adobe must terminate an employee, the employee is notified and removed from the building with their things. Any Adobe property is returned to Adobe. The Human Resources Department immediately contacts the IT Department, which makes the following changes.

- The employee’s Blackberry is wiped clean (if applicable)
• The employee’s email and VPN access is terminated
• IT makes an image of the employee’s computer, which is retained for two years. The computer is reformatted.
• Their access to Adobe Offices and Datacenters is terminated
• If the employee had Live Network Access, all administrative passwords are changed and any access to Datacenters and Internal Databases is removed.

Employee Access to Client Data
Access to data is important because it is key to the success of Adobe clients. Adobe has taken measures to ensure that only access to both live data and reporting data is given to the appropriate employees.
Access to the Adobe Live Network environment is granted only after sufficient business justification for such access has been provided, successful passing of a background check, and appropriate written approval has been obtained.
Access privileges are reviewed periodically and with any change of job responsibility.

Client Data Confidentiality
Adobe does not share collected data with any competitors, organizations, or individuals without express written consent of the data owner. Adobe places a high value on the security of data, which will always be treated as confidential.

For more information
Product details: www.adobe.com
Licensing inquiries: 877-722-7088
Contact information: 877-722-7088