Agreement Number: 4400831431

AMENDMENT TO THE ADOBE VALUE INCENTIVE PLAN
MEMBERSHIP TERMS AND CONDITIONS

AMENDMENT EFFECTIVE DATE: The date of last signature below

This Amendment (the "Amendment") to the standard Adobe Value Incentive Plan Membership Terms and Conditions (the "VIP Terms") amends the VIP Terms between Adobe and the VIP Member listed below.

WHEREAS, Adobe and VIP Member wish to modify the VIP Terms as provided below.

NOW THEREFORE, in consideration of the mutual promises and covenants contained in this Amendment, the parties agree as follows:

1. The parties agree that the version of Adobe's K-12 (Primary and Secondary) Education Additional Terms For Board of Cooperative Educational Services for the First Supervisory District, Erie County (attached hereto as Annex 1) (the "Additional Terms") shall apply for the Amendment Term (as defined below) and no modification to the Additional Terms shall be valid or binding during the Amendment Term, unless in a writing, signed by both parties hereto.

2. This Amendment is effective as of the Amendment Effective Date and will continue until 11:59 pm Eastern Time on June 30, 2023 (the "Initial Term"), unless earlier terminated pursuant to the Terms (as defined in the Additional Terms) (the "Amendment Term").

3. Adobe may change the VIP Terms from time to time to incorporate updates. VIP Member may reaccept the updated VIP Terms, and then this Amendment will apply to the then-current VIP Terms.

4. Unless otherwise expressly defined in this Amendment, capitalized terms used in this Amendment shall have the same meaning set forth in the VIP Terms. Except for the terms provided in this Amendment, all other terms and conditions of the VIP Terms will remain in full force and effect. Any inconsistency between this Amendment and the VIP Terms shall be resolved in favor of this Amendment.

IN WITNESS WHEREOF, the parties have executed this Amendment by their duly authorized representatives as of the Amendment Effective Date.

Adobe Inc.	**VIP Member: Board of Cooperative Educational Services for the First Supervisory District, Erie County**
Greg Simpson	James Fregelette James Fregelette (Oct 2, 2020 13:00 EDT)
Authorized Signature	Authorized Signature
Greg Simpson	James Fregelette
Print Name	Print Name
Director of Finance Asst Controller	Executive Director , Admin Services & Operations
Title	Title
Oct 2, 2020	Oct 2, 2020
Date	Date

Annex 1

Adobe K-12 (Primary and Secondary) Education Additional Terms
For Board of Cooperative Educational Services for the First Supervisory District, Erie County

These Additional Terms are entered into between Adobe Inc. ("Adobe") and Board of Cooperative Educational Services for the First Supervisory District, Erie County ("**You**" or "**you**" or "**Erie 1 BOCES**" or "**Customer**") effective as of the date of last signature below (the "**Effective Date**") and govern your use and deployment of Adobe products and services to students in the K-12 (primary and secondary) school environment (the **"Student Services"**).

Boards of Cooperative Educational Services ("**BOCES**"), including Customer, are municipal corporations organized and existing under Section 1950 of the New York Education Law, and are authorized to provide cooperative educational services to school districts in New York State pursuant to cooperative educational service agreements ("**CoSers**") approved by the New York State Education Department.

Regional Information Centers ("**RICs**"), organized and administratively aligned under a BOCES, provide shared technology and other educational support services on a regional basis to its BOCES's component school districts, and to other BOCES and school districts located within the RIC's respective region. Cooperative educational services provided by a BOCES (by the BOCES itself, or if applicable, its respective RIC) include shared computer services, software, and technical training and support that are provided to school districts that enter into applicable CoSers.

Customer is authorized to issue requests for proposals, award and enter into contracts for the purchase of instructional software applications that can be made available to school districts as part of applicable approved CoSers, on behalf of itself and other BOCES across New York State that participate in a statewide Instructional Technology Contract Consortium ("**NYSITCC**"). Through Customer's procurement process, Adobe has been identified and accepted by Customer as a provider of Student Services. As Customer and several other BOCES throughout New York State have expressed an interest in offering the Student Services to school districts as part of the applicable approved CoSers, Customer wishes to make the Student Services available through the NYSITCC.

The Adobe General Terms of Use ("**General Terms**") located at https://www.adobe.com/legal/terms.html and the Adobe Value Incentive Plan Terms and Conditions located at https://www.adobe.com/howtobuy/buying-programs/vip-terms.html (the "**VIP Terms**") are incorporated herein by reference (these Additional Terms, the VIP Terms and the General Terms are collectively referred to herein as **"Terms"**). Capitalized terms not defined herein have the same meaning as defined in the General Terms. By agreeing to these Additional Terms, you represent that you have the authority to bind any School to which the Student Services are deployed hereunder to the Terms.

1. Additional Definitions

1.1. "BOCES Member" means a School located within New York State which purchases certain shared instructional technology services and software through a CoSers with Customer, and as a result is authorized to use the Student Services pursuant to the terms and conditions of these Terms.

1.2. "School" means a qualified primary or secondary educational institution located within New York State, defined at: www.adobe.com/go/primary-secondary-institution-eligibility-guidelines, including Customer, a BOCES, and a BOCES Member, made up of one or more educational institutions meeting the aforementioned guidelines. For example, a K-12 educational institution in the United States is a School.

1.3. "Student" means an individual enrolled in classes at a School.

1.4. "**Student Assets"** means the files, data, and Student-generated content created by Students through the use of the Student Services.

1.5. "Student Data" means Student Personal Information and Student Assets.

1.6. "Student Personal Information" means any information, whether gathered by Adobe or provided by a Student, a School, or a parent or guardian during the provision of the Student Services pursuant to these Terms, that can be used to identify or contact a particular Student or that, alone or in combination, is linked or linkable to a specific Student so as to allow a reasonable person in the School community who does not have knowledge of the relevant circumstances, to identify the Student with reasonable certainty. To the extent U.S. law applies, Student Personal Information may include "education records" as defined in FERPA (20 U.S.C. § 1232(g)).

1.7. "You" or **"you,"** as used in these Additional Terms, means a School and its teachers, administrators, or other users authorized to access and use the Student Services on the School's behalf.

2. Deployment of the Offering: Enterprise IDs or Federated IDs Only

2.1 Deployment. You may only deploy the Student Services using Enterprise IDs or Federated IDs. Use of Enterprise IDs or Federated IDs is essential for us to meet our Student privacy commitments to you. Use of Enterprise IDs or Federated IDs also ensures you retain control over the Student Services and the Student Data provided to or generated through the Services. Any deployment of an individual Adobe ID to a Student nullifies any commitment we make regarding the use and protection of Student Data, and you must defend and indemnify us for any privacy or other claims related to your license deployment using an Adobe ID for the Student Services. More information about ID types is available at https://helpx.adobe.com/enterprise/using/edu-deployment-guide.html.

2.2 Use of Student Services. All users of the Student Services must comply with the applicable provisions of the General Terms, including but not limited to those governing acceptable use.

3. Data Ownership and Authorized Access

3.1. Student Data Consents and Authority. By using the Student Services and offering the Student Services to Students, you represent and warrant that (i) you have the authority to provide Student Data to Adobe, or to authorize Adobe to collect Student Data through the Student Services, and to allow Adobe to process Student Data for the purpose of providing the Student Services, and (ii) you have provided appropriate disclosures to, and obtained consents from, your School, the School's end users, the parents or guardians of Students, or any other required individual regarding the School's use of the Student Services, to the extent such disclosures or consents are required by applicable law or by School agreements or policies.

3.2. Ownership and Control. Adobe will access and process Student Data for the purposes of providing the Student Services as described in these Terms. As between Adobe and School, School owns all rights, title, and interest to all Student Data processed by Adobe pursuant to the Terms, and Adobe does not own, control, or license such Student Data, except so as to provide the Student Services and as otherwise described in the Terms.

4. Compliance with Law and Obligations

4.1. United States. Both parties agree to uphold their responsibilities under applicable federal laws governing Student Personal Information, including, but not limited to, the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232(g), the Protection of Pupil Rights Amendment ("PPRA"), 20 U.S.C. 1232, and the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. 6501-6502. You represent and warrant that you have reviewed the Terms, as well as the exhibits to these Additional Terms, and have determined that they comply with

your obligations under New York law, including New York State Education Law 2-d, Part 121, and any implementing Regulations of the Commissioner of Education (collectively, "Section 2-d").

(a) **FERPA Compliance.** If you are located in the United States, Adobe will collect and process Student Data as a "school official" with a legitimate educational interest as defined under FERPA and its implementing regulations, and we agree to abide by the applicable limitations and requirements imposed by 34 CFR §99.33(a) on school officials.

(b) **COPPA Compliance.** If you are located in the United States, to the extent you allow children under 13 to access the Student Services or any other Adobe application for the use and benefit of your School, you will obtain consent to allow Adobe to collect and process information from students under 13 for the purposes described in these Terms, and you represent and warrant that you have the authority to provide such consent in accordance with COPPA. Adobe will provide you with notices regarding its practices related to the collection, use and disclosure of personal information that you will, in turn, provide to parents as required under COPPA. You will ensure that your configuration of the Student Services and the features and functionality of the Student Services you permit children under 13 to access are appropriate for use in a manner consistent with COPPA.

4.2. Local Law Compliance. Schools and the use of Student Services may also be subject to laws and regulations in the jurisdiction in which you are located. You are responsible for ensuring that you can use the Student Services consistent with your local laws. In particular, it is the School's obligation to (a) determine whether legal obligations arising from such local laws and regulations apply with respect to the School's use and deployment of Student Services, (b) obtain any necessary consents from parents or legal guardians, to the extent such consents may be required, and (c) configure the Student Services such that they are deployed in the School and made available to Students in a manner consistent with these local laws.

5. Student Data Processing

5.1. Permitted Uses of Student Data. Adobe may use, transmit, distribute, modify, reproduce, display, process, and store Student Data solely: (i) for the purposes of providing the Student Services as contemplated by the Terms, and as otherwise described herein, (ii) for the purposes of maintaining, supporting, evaluating, analyzing, diagnosing, improving and developing Adobe's websites, services, and applications, as permitted by law, (iii) for the purpose of enforcing its rights under the Terms, (iv) as permitted with consent of the parent or guardian, eligible Student, or the School, and (v) as otherwise authorized by applicable law.

5.2. Use of De-Identified Data. Notwithstanding anything to the contrary herein, you agree that Adobe may use de-identified data, including (i) Student Data from which all direct and indirect identifiers have been removed such that there is no reasonable basis to believe the information can be used to identify an individual, and (ii) data relating to access and use of the Student Services, for any lawful purpose, including, but not limited to, the development, research, and improvement of educational sites, services, or applications, and to demonstrate the effectiveness of the Student Services. Unless permitted or required by law, Adobe agrees not to attempt to re-identify any such data and will not disclose it to any third party unless the recipient agrees not to attempt to re-identify the information.

5.3. Marketing and Advertising. Adobe is prohibited from using Student Data: (i) to inform or direct targeted online advertising to Students or to a parent or guardian unless with the consent of the parent or guardian, (ii) to amass a profile of a Student, other than for the purpose of providing Student Services or as authorized by School or the Student, and (iii) for any other commercial purpose unless authorized by School, the parent or guardian, or as otherwise permitted by the Terms or applicable law. Notwithstanding the foregoing, you agree that Adobe may (a) market or advertise products and services directly to parents, guardians, or School employees, so long as the marketing does not result from the use of Student Data, (b) direct online advertising to a Student or other individual based on that Student or individual's current visit to that online location, provided that the Student's online activities are not collected over time for the purpose of delivering targeted advertising; (c) use Student Data to recommend educational products or services to parents/guardians and School's employees so long as the recommendations are not based in whole or in part on payment or other consideration from a third party, (d) use aggregate or de-identified information to inform, influence, or enable marketing, advertising, or other commercial efforts by Adobe; (e) use Student Data for adaptive learning or customized student learning purposes, or (f) use

Student Data to send emails or other communications to Students relating to their account and use of the Student Services.

5.4. Student Data Retention and Deletion. Schools may access a Student account through the Adobe Admin Console at any time in order to modify or delete Student Data. It is your responsibility to delete or remove Student Data from the Student Services when it is no longer needed for an educational purpose. Upon termination of your agreement with Adobe, Adobe will retain Student Data for a reasonable period of time to permit Students to download to and store Student Assets in a personal account. It will be the responsibility of the School to delete any remaining Student Data upon termination of the agreement. If the School fails to delete Student Data, Adobe will dispose of or delete Student Data when it is no longer needed for the purpose for which it was obtained. Adobe has no obligation to delete de-identified data or Student Assets that have been transferred to a Student's personal account.

6. Restrictions on Access or Disclosure of Student Data

6.1. Permitted Disclosures. Adobe will not sell, disclose, transfer, share, or rent any data obtained under the agreement in a manner that could identify an individual Student to any entity other than the School except: (i) to the extent set forth in the agreement, or (ii) with the consent, or at the direction of, the School, a Student's parent or legal guardian, or a Student who is over the legal age of consent. Depending on the features and functionality utilized by the School, some features of the Student Services may permit Students to share information or post information in a public forum. School administrative users should use caution when adjusting permissions and features accessed through the Adobe Admin Console to ensure such permissions and features are configured appropriately for your and your Students' use.

6.2. Third-Party Service Providers. You acknowledge and agree that, provided that they have a legitimate need to access such information in connection with their responsibilities in providing services to Adobe and such access is subject to contractual data protection terms, Adobe may permit its subcontractors, service providers, and agents to access Student Data.

6.3. Third Party Access Requests. School will establish reasonable procedures by which a parent, legal guardian, or eligible Student may request access, correction, or deletion of Student Data generated through the Student Services. Upon request by the School, Adobe will work with the School as needed to facilitate such access. Should a third party, including law enforcement and government entities, contact Adobe with a request for Student Data, Adobe will redirect the third party to request the data directly from School, unless and to the extent that Adobe reasonably and in good faith believes that granting such access is necessary to comply with a legal obligation or legal process or to protect the rights, property, or personal safety of Adobe's users, employees, or others.

6.4. Change of Control. In the event Adobe sells, divests, or transfers all or a portion of its business assets to a third party, Adobe may transfer Student Data to such third party provided that (i) such third party intends to maintain and provide the Student Services subject to data privacy standards no less stringent than those provided herein, or (ii) Adobe gives notice to School and an opportunity to opt out of the transfer of Student Data.

7. Data Security

7.1. School Obligations. School and users of Student Services will take reasonable precautions to secure usernames, passwords and any other means of gaining access to the Student Services and to Student Data. School will notify Adobe promptly of any known or suspected unauthorized access to School's account and/or to Adobe's systems or services. School will assist Adobe in any efforts by Adobe to investigate and respond to any incident involving unauthorized access to the systems.

7.2. Adobe Obligations. Adobe has implemented reasonable administrative, technical, and physical security controls to protect Student Data and has provided data privacy and security training to its employees who have access to Student Data or who operate or have access to relevant system controls. However, despite our efforts, no security controls are 100% effective and Adobe cannot ensure or warrant the security of your information. In the event that we determine any Student Personal Information that we have collected or received through the

Student Services was acquired by an unauthorized party (a **"Security Event"**), we will promptly notify the School and shall reasonably cooperate with the School's investigation of the Security Event. To the extent the School determines that a Security Event affects Student Personal Information in a manner that triggers third party notice requirements under applicable laws, the School shall be responsible for sending such notices, unless otherwise agreed in writing between Adobe and the School. Except as otherwise required by law, Adobe will not provide notice of the Security Event directly to individuals whose personal information was affected, to regulatory agencies, or to other entities, without first providing written notice to School.

7.3. Exhibits. Further information regarding data security is available for Students' parents in Exhibit A (Parents' Bill of Rights For Data Security and Privacy), Exhibit B (Supplemental Information About the Additional Terms) and Exhibit C (Technical Organizational Measures) to these Additional Terms.

8. Governing Law

8.1. These Terms shall be governed by the laws of the State of New York, except that body of law concerning conflicts of law.

9. Term/Termination

9.1. These Additional Terms apply to the Student Services for twenty-four (24) months from the date of your first VIP order for Student Services, unless earlier terminated pursuant to the Terms.

10. Reserved.

11. Order of Precedence.

11.1 In the event of an inconsistency in the terms referenced herein, the terms shall take precedence in the following order: (i) these Additional Terms, (ii) the VIP Terms, and (iii) the General Terms.

Adobe Inc.	**You: Board of Cooperative Educational Services for the First Supervisory District, Erie County**
Greg Simpson Authorized Signature	James Fregelette James Fregelette (Oct 2, 2020 13:00 EDT) Authorized Signature
Greg Simpson Print Name	James Fregelette Print Name
Director of Finance Asst Controller Title	Executive Director , Admin Services & Operations Title
Oct 2, 2020 Date	Oct 2, 2020 Date

Exhibit A
ERIE 1 BOCES
PARENTS' BILL OF RIGHTS FOR DATA SECURITY AND PRIVACY

Erie 1 BOCES is committed to protecting the privacy and security of student, teacher, and principal data. In accordance with New York Education Law § 2-d, the BOCES wishes to inform the community of the following:

(1) A student's personally identifiable information cannot be sold or released for any commercial purposes.

(2) Parents have the right to inspect and review the complete contents of their child's education record.

(3) State and federal laws protect the confidentiality of personally identifiable information, and safeguards associated with industry standards and best practices, including but not limited to, encryption, firewalls, and password protection, must be in place when data is stored or transferred.

(4) A complete list of all student data elements collected by the State is available for public review at http://www.nysed.gov/data-privacy-security/student-data-inventory, or by writing to the Office of Information & Reporting Services, New York State Education Department, Room 863 EBA, 89 Washington Avenue, Albany, New York 12234.

(5) Parents have the right to have complaints about possible breaches of student data addressed. Complaints should be directed in writing to the Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, New York 12234. Complaints may also be submitted using the form available at the following website http://www.nysed.gov/data-privacy-security/report-improper-disclosure.

Board of Cooperative Educational Services for the First Supervisory District, Erie County

James Fregelette
James Fregelette (Oct 2, 2020 13:00 EDT)
Authorized Signature
James Fregelette
Print Name

Executive Director , Admin Services & Operations
Title
Oct 2, 2020
Date

Adobe acknowledges that Erie 1 BOCES has provided this Parents' Bill of Rights to the community:

Adobe Inc.

Greg Simpson
Authorized Signature

Greg Simpson
Print Name

Director of Finance Asst Controller
Title

Oct 2, 2020
Date

Exhibit B

SUPPLEMENTAL INFORMATION
ABOUT THE ADDITIONAL TERMS

Erie 1 BOCES has entered into the K-12 (Primary and Secondary) Education Additional Terms ("Additional Terms") with Adobe, which governs the deployment of Adobe products and services to students in the K-12 (primary and secondary) school environment. Such Additional Terms govern the Student Services which BOCES has licensed pursuant to the VIP Program (the "Product(s)"). Capitalized terms not defined herein have the same meaning as defined in the Additional Terms.

Pursuant to the Additional Terms, Erie 1 BOCES may provide to Adobe, and Adobe may receive, Student Personal Information and/or Teacher or Principal Data (as defined below), that is protected by Section 2-d ("Protected Data"). "Teacher or Principal Data" means Student Personal Information from the records of a School, school district, board of cooperative educational services (BOCES), or the New York Department of Education relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§3012-c and 3012-d.

Exclusive Purpose for which Protected Data will be Used: Adobe agrees that it will not use Protected Data for any purposes not authorized in the Additional Terms. Protected Data (other than de-identified data and usage data, which is collectively referred to herein as "Measurement Data") received by Adobe, or any of Adobe's subcontractors, assignees, or other authorized agents, through the provision or use of the Product(s) pursuant to the Additional Terms, will not be sold, released, or used for any commercial or marketing purposes other than for the purposes of providing the Student Services pursuant to the Additional Terms.

Oversight of Subcontractors: In the event that Adobe engages subcontractors to perform one or more of its obligations under the Additional Terms (including any hosting services), it will require those to whom it discloses Protected Data to be subject to contractual data protection terms at least as restrictive as those set forth in the Additional Terms. Adobe will oversee the performance of such subcontractors and determine that such subcontractors have a legitimate need to access the Protected Data in connection with their responsibilities in providing services to Adobe.

Duration of Additional Terms and Protected Data Upon Expiration: Upon expiration of the Additional Terms without renewal, or upon termination of the Additional Terms prior to expiration or termination of a Student, teacher or principal account, Adobe will securely delete or otherwise destroy any and all Protected Data (other than Measurement Data) remaining in the affected account(s) at the direction of Erie 1 BOCES , unless retention of such Protected Data is required by mandatory applicable law or necessary for Adobe to enforce its rights under the Terms. If requested by Erie 1 BOCES , prior to deletion, Adobe will reasonably assist Erie 1 BOCES in exporting all Protected Data (other than Measurement Data) previously received by Adobe back to Erie 1 BOCES for use by Erie 1 BOCES in accordance with applicable law.

Challenging Accuracy of Protected Data: Parents or eligible students can challenge the accuracy of any Protected Data provided by Erie 1 BOCES to Adobe, if any, by contacting the Student's district of residence regarding procedures for requesting amendment of educational records under FERPA. Teachers or principals may be able to challenge the accuracy of APPR data provided to Adobe by Erie 1 BOCES , if any, by following the appeals process in their employing school district's applicable APPR Plan.

Data Storage and Security Protections: Any Protected Data Adobe receives will be stored on systems maintained by Adobe, or by a subcontractor under the direction of Adobe, in a secure data center facility. The measures that Adobe will take to protect Protected Data include adoption of technologies, safeguards and practices that are consistent with industry standards. Additional information on Adobe's various security controls and processes for its products and services are located in Exhibit C (Technical Organizational Measures) to the Additional Terms. In

the event of a Security Event, Adobe will provide reasonable cooperation and support upon request from Erie 1 BOCES in order to assist Erie 1 BOCES 's investigation, analysis, and response obligations under relevant law, including reimbursing reasonable costs of providing legally required notice to the extent such Security Event occurred solely due to Adobe or its subcontractors.

Adobe Inc.

Greg Simpson
Authorized Signature

Greg Simpson
Print Name

Director of Finance Asst Controller
Title

Oct 2, 2020
Date

Exhibit C

Technical Organizational Measures

Exhibit Date: August 1, 2020

Adobe has implemented reasonable information security practices regarding the protection of Student Personal Information, including administrative, technical and physical security measures consistent with the information found at http://www.adobe.com/go/cloudcompliance and in the Technical and Organization Security Measures for the Adobe General Terms ("TOMS"), for the applicable Student Services. This information is current as of the Exhibit Date, but is subject to change as Adobe improves and modifies its products and services. Capitalized terms used herein but not defined herein shall have the meaning set forth in the Additional Terms.

Technical and Organizational Security Measures for the Adobe General Terms (2020FEB10)

I. Adobe Security Certifications.

Adobe Cloud Services meet the specific requirements of data protection, including, Article 28 of the General Data Protection Regulation and which are listed as SOC2, Type 2 (Security and Availability) and ISO 27001 compliant and others as indicated at http://www.adobe.com/go/cloudcompliance.

At a minimum, Adobe has implemented for the Adobe Cloud Services the technical and organizational measures and maintains security practices within the production environments as follows:

II. Confidentiality Measures

A. Site Operations

1. Physical Access Management

a) Employee physical access that is no longer required in the event of personnel termination or role change is promptly revoked. If applicable, temporary badges are returned prior to exiting facility.

b) Initial permission definitions, and changes to permissions, associated with physical access roles are approved by appropriate Adobe personnel.

2. Physical Access Reviews. Adobe performs physical access account reviews on a quarterly basis, corrective action is taken where applicable.

3. Physical Security

a) Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points and/or manned reception desks.

b) All facilities require badge and/or biometric access and have 24x7 security guards. Some facilities use additional measures to prevent unauthorized individuals from tailgating authorized individuals into the facility.

c) Intrusion detection and video surveillance are installed at all facilities. Adobe may review video logs when issues or concerns arise in order to determine

access.

d) Adobe power and telecommunication lines are protected from interference, interception and damage.

e) Granting physical access to an Adobe data center requires management approval and documented specification of:

(1) account type: (visitor, vendor, or regular);

(2) access privileges granted;

(3) intended business purpose;

(4) visitor identification method, if applicable;

(5) temporary badge issued, if applicable;

(6) access start date; and,

(7) access duration.

f) Visitors to a facility where allowed are required to be escorted at all times and are not allowed in caged areas.

g) Visitor Access Logs are retained for up to 12 months in accordance with Adobe's documentation retention policy.

B. Identity and Access Management of Adobe Personnel.

1. Logical access

a) Logical access provisioning to information systems requires approval from appropriate personnel.

b) Logical access that is no longer required in the event of a termination is documented, communicated to management, and revoked.

c) Adobe performs account and access reviews on a quarterly basis, and corrective action is taken where applicable.

2. Authentication.

a) Adobe creates unique identifiers for user accounts and prevents the reuse of identifiers. Account Login parameters follow these rules:

(1) Accounts are not shared;

(2) Inactive sessions are password protected after 15 minutes; and,

(3) All systems classified as confidential and restricted require multifactor authentication. Multifactor authentication must be used for access to environments that host production systems or systems and applications containing restricted or confidential data.

b) Adobe users are enrolled with Zen platform. Zen is a platform that uses multi-factor authentication plus device and security posture during authentication. For more information on Zen, see the Adobe white paper available here:
https://wwwimages2.adobe.com/content/dam/acom/en/security/pdfs/Adobe-

ZEN-WP.pdf

(1) Zen access proxy is encrypted with Transport Layer Security (TLS)

(2) Users enrolled in the Zen platform are only required to change their passwords upon compromise indicator.

(3) Privileged or high risk accounts require 90 day password rotation.

c) In case of circumstances where an Adobe user is not enrolled with Zen platform, user and device authentication to information systems is protected by passwords that meet Adobe's password complexity requirements. Strong password configurations adhere to the following rules:

(1) Must be at least twelve characters in length;

(2) Cannot be found in a dictionary or contain words from a dictionary (English);

(3) May not include any three (3) consecutive characters from the login username; and,

(4) Must be different than the previous 10 passwords.

d) Unless Zen enabled, remote connections to the corporate network are accessed via VPN through managed gateways and require multifactor authentication.

3. Role Based Access Control

a) Initial permission definitions, and changes to permissions associated with logical access roles are approved by appropriate personnel.

b) Access that allows modification to source code is restricted to authorized personnel.

c) Role based and context based access to data is modeled on the concept of least privilege.

d) Adobe restricts the use of shared service account authentication credentials via the use of a shared secret solution. Authentication credentials for shared service accounts are reset every 90 days.

4. Network Operations

a) Adobe maintains a dedicated Network Operations Center (NOC), which is staffed 24/7 with at least 2 dedicated personnel.

b) Network traffic to and from untrusted networks passes through a policy enforcement point; firewall rules are established in accordance to identified security requirements and business justifications.

c) Adobe uses IDSs, firewalls, bastion hosts and Access DMZs as layers of security. Antivirus is running on all employee desktops and laptops and all email traffic is scanned for malware. Additionally, real time antivirus scanning is enabled.

d) Production environments are logically segregated from non-production environments.

5. Key Management

a) Access to the cryptographic keystores is limited to authorized personnel.

6. Preservation and Review of Security Logs

a) Adobe shall keep logs used in connection with its security procedures for the protection of Personal Data related to the applicable product operations in a secure location. Adobe shall retain logs within the SIEM, or log aggregation service, for a minimum period of one year, with 90 days of data immediately available for analysis.

b) Security event logs are reviewed in accordance with the event context and severity, some of which require daily review.

C. Employee Management

1. Background Checks and Non-Disclosure Agreements

a) Adobe obtains pre-hire background check reports for employment purposes. The specific nature and scope of the report that Adobe typically seeks may include (as permitted by applicable law):

(1) Educational background;

(2) Work history;

(3) Court records (including criminal conviction records); and,

(4) References obtained from professional and personal associates.

b) Adobe hires employees based on a documented job description.

c) Employees are required to sign a Non-Disclosure Agreement upon employment. Adobe employees including contractors are required to sign an agreement that they will protect confidential information.

2. Training and Awareness

a) Adobe personnel (including contract workers) complete security awareness training, which includes annual updates about relevant policies, standards, and new or modified attack vectors and how to report security events to the appropriate response team. Records of annual training completion are documented and retained for tracking purposes. Any Adobe vendors with network access are required to complete their own equivalent security awareness training.

b) Annually, Adobe fulltime and temporary employees and interns complete a code of business conduct training. Anyone who is found to violate the Code of Business Conduct or other Adobe policies may be subject to disciplinary action including termination of employment or contract.

III. Integrity, availability and resilience of processing systems

A. Information Systems and Technology Management

1. Production Configuration Management

a) Adobe ensures security hardening and baseline configuration standards

have been established according to industry standards defined by the Center for Internet Security (CIS) and are reviewed and updated periodically.

b) Adobe uses mechanisms to detect deviations from baseline configurations on production environments.

c) Installation of software or programs in the production environment requires approval by appropriate personnel.

2. Change Management

a) Change scope, change type, and roles and responsibilities are pre-established and documented in a change control workflow. Notification and approval requirements are also pre-established based on risk associated with change scope and type. Change management uses an automated ticketing system.

b) Based on risk, prior to introducing changes into the production environment, approval from appropriate personnel is required based on the following:

(1) Change description is documented;

(2) Impact of change;

(3) Test results are documented; and,

(4) Back-out procedures are defined.

c) Changes to the production environment are implemented by authorized personnel only.

3. Data Transfer

a) Adobe deploys dedicated network connections from its corporate offices to Adobe data center facilities in order to enable secure management of the servers.

b) All management communications to the servers occur over encrypted tunnels and sessions. Some examples are: Secure Shell (SSH), Transport Layer Security (TLS); Internet Protocol Security (IPSec) or Virtual Private Network (VPN) channels. Remote access for VPN always requires multifactor authentication.

c) Unless the connection originates from a list of trusted IP addresses, Adobe does not allow management access from the internet.

d) Administrative data is encrypted in transit across the internet via TLS 1.2 or greater over HTTPS between the Customer and the user interface.

(1) Through Customer's enablement of TLS over HTTPS, where available, Customer may transmit data collected by the Distributed Code through the use of strong encryption (excluding any emails initiated by Customer through the use of Adobe Sign Services/Adobe Campaign,). In the event Customer transmits data to Adobe through any other means including but not limited to email or FTP, Customer acknowledges that such data will not be encrypted.

4. Security Governance

a) Corporate Documents. Adobe's key business functions and information

security capabilities are supported by documented procedures that are communicated to authorized personnel.

b) Information Security Management. Adobe has an established governance framework that supports relevant aspects of information security with policies and standards.

c) Security Leadership & Roles. Roles and responsibilities for the governance of Information Security within Adobe are formally documented and communicated by Management.

5. Cloud Services Systems Monitoring

a) Critical Information System Logs

(1) Adobe utilizes a centralized SIEM solution to aggregate and correlate logged events.

(2) In order to protect against unauthorized access and modification, Adobe captures network logs, operating system logs, application logs and security events.

(3) Application user activity is logged by the application.

b) Security Monitoring and Evaluation

(1) Adobe defines security monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts.

(2) Adobe defines availability monitoring alert criteria, how alert criteria will be flagged, and identifies authorized personnel for flagged system alerts. Customers can monitor a product's availability at: https://status.adobe.com.

c) System Design Documentation

(1) Documentation of system boundaries and key aspects of their functionality are published to authorized Adobe personnel.

(2) Adobe publishes public-facing whitepapers that describe the purpose, design, and boundaries of the system and system components which are available here: https://www.adobe.com/security/resources.html.

B. Service & Product Lifecycle

1. Source Code. Source code is checked for vulnerabilities prior to being released into production. For high risk services and products, manual security testing, and, where appropriate, manual and automated code review, is required to be performed for significant changes to ensure detection and prevention of common security issues

2. Major software releases are subject to the Service Life Cycle, which requires acceptance via Concept Accept and Project Plan Commit phases prior to implementation.

C. Vulnerability Management

1. Information Systems and Technology

a) For customer-facing products as defined in Adobe's Current List of Certifications, Standards, and Regulations listed at https://www.adobe.com/content/dam/acom/en/security/pdfs/MasterComplianceList.pdf, at least annually, Adobe will engage with a third party to perform application penetration testing, assign risk ratings to discovered vulnerabilities, and track vulnerabilities through resolution. At least annually, Adobe will also perform network penetration testing for all critical services defined in the above list. Network testing may be performed by Adobe's internal security teams.

b) The objective of penetration testing is to find security vulnerabilities following industry standards and best practices (such as those listed in the Open Web Application Security Project current ten most common web applicable security risks).

c) Upon receipt of the deliverable provided by a third party, Adobe will document these vulnerabilities, evaluate them in accordance with its internal processes as well as recommendations by the third party, and then create a mitigation strategy or remediation plan.

d) A remediation report which provides an overview of the testing methodologies, findings and remediations is either available on https://www.adobe.com/trust.html or can be requested from an Adobe sales representative.

2. If applicable, Adobe has managed enterprise antivirus deployments and ensures the following:

a) Signature definitions are updated daily;

b) Full scans are performed weekly and real-time scans are enabled; and,

c) Alerts are reviewed and resolved by appropriate personnel.

3. Vulnerability Scans. External and internal vulnerability scans are performed at least quarterly. Internal scans are also performed after major changes.

4. Vulnerability Reviews. Adobe reviews reasonable customer vulnerability-related inquiries for advisement only.

5. Patch Management. Adobe installs security-relevant patches, including software or firmware updates in accordance with Adobe's patch management standard.

IV. Measures for prompt recoverability and access to Customer Data

A. **Incident Response.** Adobe has implemented a comprehensive incident response program that includes at least the measures below and as described at the Adobe Trust Center website.

1. Adobe defines the types of incidents that need to be managed, tracked, and reported. Such management includes the following:

a) Procedures for the identification and management of incidents;

b) Procedures for the resolution of confirmed incidents;

c) Key incident response systems;

d) Incident coordination and communication strategy;

e) Contact method for internal parties to report potential incidents;

f) Support team contact information;

g) Notification to relevant Adobe management in the event of a security breach;

h) Provisions for updating and communicating the plan;

i) Provisions for training of support team;

j) Preservation of incident information; and,

k) Management review and approval (either annually or when major changes to internal organization occur).

2. Adobe responds to confirmed incidents and resolution is tracked with appropriate management channels. If applicable, Adobe coordinates the incident response with business contingency activities.

3. Adobe provides a contact method for external parties to report incidents here: https://helpx.adobe.com/security/alertus.html.

C. Environmental security

1. Temperature and humidity levels of data halls are monitored and maintained at appropriate levels.

2. Emergency responders are automatically contacted when fire detection systems are activated. The design and function of fire detection and suppression systems is certified at appropriate intervals.

3. Adobe employs uninterruptible power supplies (UPS) and generators to support critical systems in the event of a power disruption or failure. The design and function of relevant equipment is certified at appropriate intervals.

D. Disaster Recovery and Business Continuity Plans

1. Adobe maintains disaster recovery and business continuity plans and processes to allow for continuation of the services and to provide an effective and accurate recovery. Such plans are tested on an annual basis. [Example: backup copies of the data stock are generated by means of the following procedures: description of the intervals, media, retention period and storage location of backup copies.]

V. Processes for regular testing, assessing and evaluating the effectiveness of security measures

A. Risk Management

1. Adobe management performs an annual risk assessment in alignment with National Institute of Standards and Technology (NIST) 800/30 rev1. Results from risk assessment activities are reviewed to prioritize mitigation of identified risks.

2. Management assesses the design and operating effectiveness of internal controls

against the established controls framework. Corrective actions related to identified deficiencies are tracked to resolution.

3. Adobe establishes internal audit requirements and executes audits on information systems and processes at planned intervals.

4. Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.

B. Third Party Management

1. On a periodic basis, management reviews controls within third party assurance reports to ensure that they meet organizational requirements. If control gaps are identified in the assurance reports, management addresses the impact that disclosed gaps have on the organization.

2. Adobe performs a risk assessment to determine the data types that can be shared with a managed service provider.

VI. Technical Progress

A. Adobe´s Technical and Organizational Measures are subject to technical progress and further development. Accordingly, Adobe reserves the right to modify the Technical and Organizational Measures provided that the functionality and security of the Adobe Cloud Services are not degraded.

VII. Notification to Adobe.

A. To notify Adobe of a security issue, please see https://helpx.adobe.com/security/alertus.html.