Technical and Organizational Measures

I. Adobe Security Certifications

Adobe Cloud Services meet the specific requirements of data protection as indicated at https://www.adobe.com/trust/compliance/compliance-list.html

At a minimum, Adobe has implemented for the Adobe Cloud Services, including applicable Support and Professional Services insofar as Adobe is in control of the environment, the following technical and organizational measures and maintains security practices within the production environments as outlined below. For Adobe Commerce (f/k/a Magento Commerce), which for the purposes of this document includes Business Intelligence and Order Management, some exceptions may apply as detailed in each section. For Adobe Commerce, Customer understands that the solution operates under a "Shared Responsibility Security Model", where Customer retains the primary responsibility for security monitoring of its production instance(s) while Adobe retains the primary responsibility for security monitoring of the Adobe Commerce infrastructure.

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) By policy, 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 services 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 devices 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://www.adobe.com/content/dam/cc/en/security/pdfs/Adobe-ZEN-WP.pdf

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

(2) Users are only required to change their passwords upon compromise indicator.

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

c) 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 sixteen (16) characters in length;

(2) May contain multiple words from the dictionary but the entirety of the password cannot be one word from the dictionary;

(3) Must not contain the first, last, or full name of the user or contain the users username;

(4) Must not contain all or part (three or more consecutive characters) of

the login ID; and,

(5) Must not contain Adobe in the password.

d) Remote connections to the corporate network are accessed via VPN through managed gateways or require a managed device enrolled in the Zen platform, and would still require multifactor authentication. However, many of the services Adobe employees' access are SaaS-based so they are not hosted on the Adobe network and therefore don't require VPN or Zen to access.

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.

c) Adobe personnel (including contract workers) may only access Customer Data while performing Support Services and Professional Services through Adobe's Cloud Services and are prohibited from making copies of any Customer Data outside Adobe's Cloud Services.

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.

(2) Emails initiated by Customer through the use of Adobe Sign Services, Adobe Campaign, and Adobe Marketo Engage utilize opportunistic TLS.

(3) 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, however for Adobe Commerce, Customer retains sole responsibility for monitoring.

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. Except for the Adobe Commerce code, Adobe installs security-relevant patches, including software or firmware updates in accordance with Adobe's patch management standard.

a) For Adobe Commerce patch management, Adobe releases patches to the Adobe Commerce core code as needed. Customer is solely responsible for installing and applying patches and updates to the Adobe Commerce application code.

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.

B. **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.

C. **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.