® Vendor Security Review Program

Overview

Managed by the Information Security team, vendor security review (VSR) program includes a set of requirements to which third-party vendors that collect, store, process, transmit, or dispose of Internal, Confidential, or Restricted data outside of physical offices or data center locations must adhere. Typical scenarios include vendors processing and storing data at their site, cloud services (e.g., SaaS, PaaS, IaaS, and XaaS), and data centers.

The VSR program evaluates each vendor's compliance to Adobe's Vendor Information Security Standard, providing a risk-based review of the vendor's security practices and enabling managers to make fact-based decisions concerning whether or not to enter into a relationship with that vendor.

The management of vendor relationships and their interactions with information and technologyresources is an essential element of information security. The VSR program is a logical extension of Adobe's belief that every action taken on or interaction with data should be conducted with a lens of security to help ensure the security, privacy, and availability of our customers' and employees' data, no matter where it is stored or processed, which is one of the key controls within the Common Controls Framework (CCF). With the VSR program, helps ensure that its culture of security extends to any vendor with whom the company does business.

Table of Contents

Vendor Security Review (VSR) Program Process

The VSR program evaluates a third-party vendor's compliance with the Vendor Information Security Standard (described above).

Business owners within that wish to enter into a relationship with a third-party vendor initiatethe process with a VSR request, which includes a description of the service provided by the vendor, whether the vendor will process data off-site, and the classification of the data the vendor intends to process.

Based on the information provided by the business owner, sends the main point of contactat the vendor a detailed questionnaire, including questions from each security control area (see VSR Security Controls section).

After the vendor completes and returns the questionnaire, information security analysts review the information and perform a gap assessment. A vendor is assigned a risk level score of "critical," "high," "medium," or "low" based upon a risk matrix used by our risk analysts. If finds any gaps in, or deviations from, security standards, a risk analyst holds discussions with the business owner to understand the details about the gap and to provide potential remediation suggestions. The analyst documents the recommended remediation and the actions to be performed by the vendor and/or the business owner. If necessary, risk analysts will meet directly with vendors to resolve more complex issues.

Data Classification

developed the Data Classification and Handling Standard to aid in ensuring the security and privacy of all data that collects, processes, stores, uses, or otherwise handles regardless of whether the data is owned by or a third party, where the data is located (e.g., data center,colocation), or the type of hardware or media on which the data resides, whether paper or electronic (e.g., server, desktop, laptop, mobile device, USB flash drive). The standard establishes that all data

collected, processed, transmitted, stored, or destroyed by or on behalf of must be classified and then protected in accordance with its designated classification. The specific classifications in the standard define with whom employees can share data and determine where and how toshare, protect, and secure this data.

The Data Classification and Handling Standard includes four (4) classifications:

- Restricted
- Confidential
- Internal
- Public

A VSR is required for all third-party vendors that store or process data classified as Restricted, Confidential, or Internal off-premise (not at Depending on the classification of the data handled by the vendor, a new VSR is required either annually or bi-annually (see Recertification section).

Each data classification includes specific protection and handling requirements, and if data falls into multiple classifications, it must be protected in accordance with the most restrictive classification.

Any business owner requesting an exception to the Data Classification and Handling Standard mustsubmit a request in writing to the appropriate management personnel for review and approval.

If finds that data that should be classified as Restricted or Confidential has been handled incorrectly, either due to incorrect classification or negligence in its handling, may take disciplinary action against the offender.

Restricted Data

Restricted data is the most restrictive classification and requires the most care; only very limited segments of the workforce need access to Restricted data to perform their jobs. Unauthorized disclosure of Restricted data could cause severe harm to its employees, customers, stockholders, or business partners. Restricted data includes the following:

- Cardholder data, as defined by the PCI DSS
- Bank account numbers
- Social Security and taxpayer identification numbers relating to an individual
- Driver's license numbers or identification card number used to verify an individual's identity(state, military, student, voter, tribal, operator's number, etc.)
- Passport information
- Credential stores used to authenticate users or employees, such as Active Directory (butnot including personal password managers, such as Splash ID)
- Credentials, secrets, tokens, or keys permitting access to systems storing Restricted data or permitting decryption of Restricted data (e.g., identity management systems, deployment systems, or secret stores)
- Digital certificates used for signing software
- Medical or health information, including electronically protected health information (ePHI)
- Federal classified or intelligence contracts
- Security question response (including mother's maiden name) or Personal IdentificationNumber (PIN)
- Private key digital signatures
- Biometric information

- Genetic information
- Racial origin
- Ethnic origin
- Political opinions
- Religious beliefs
- Philosophical beliefs
- Trade union membership
- Sex life information
- Sexual orientation
- Criminal offenses and convictions
- Birth certificate
- Marriage certificate
- Information or data collected through use or operation of an automated license platerecognition system

Classification	Examples	Impact of Unauthorized Disclosure
Restricted data has a High Business Impact	Regulatory protected data, material financial data, intellectual property, passwords and credential.	Likely to cause severe harm to its employees, customers, stockholders, or business partners.
Confidential data has a Medium Business Impact	People related data (salary, benefits), data with need-to-know restrictions like source code, Customer Files, product roadmaps, financial information.	Likely to cause significant harm to its employees, customers, stockholders, or business partners
Internal data has a Moderate Business Impact ***Note:*** The default type for unclassified data is Internal	Operational planning, collaboration and internal communications, IT Knowledge Center articles.	May cause minor embarrassment or operational inconvenience
Public data	Information that is openly available	No impact

Confidential Data

Only limited segments of the workforce need access to data classified as Confidential in order to perform their jobs. Unauthorized disclosure of Confidential data would likely cause significant harm (such as financial, contractual, or legal or reputational harm orservice disruptions) to its employees, customers, stockholders, and business partners.

Confidential data includes:

- Data that is contractually required to treat as confidential
- Personal information (PI) (unless the personal information meets the definition of Restricted data) about an individual (including free users, paid users, enterprise users, suppliers, or employees). This can include directly identifiable personal information, such as name, email address, phone number, home address, or precise geolocation information. Personal informationcan also include indirectly identifiable personal information, such as a user GUID, IP address, cookie ID, or device identifier.
- Content or data that customers, partners, or users provide to (unless the content or datameets the definition of Restricted data below)