Google Apigee PCI-DSS 3.2.1 Responsibility Matrix

3/30/2020

Overview

Google Apigee adheres to the Payment Card Industry Data Security Standard (PCI DSS) requirements for level 1 Service Providers. Apigee delivers to its Customers, responsibility for the various requirements associated with PCI DSS varies. Some requirements are the sole responsibility of Apigee, some requirements are the sole responsibility of the Customer, and some requirements are a shared responsibility between the two.

Customers should reference the responsibility matrix within this document and share it with their PCI Qualified Security Assessor when conducting their own PCI audit.

Table of Contents – PCI DSS Responsibility Matrix

PCI DSS Responsibility Matrix

Requirement 1

Install and Maintain a Firewall Configuration to Protect Cardholder Data

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
1.1	Establish and implement firewall and router configuration standards that include the following:	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.1.2	Current diagram that identifies all networks, network devices, and system components, with all connections between the CDE and other networks, including any wireless networks	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.1.5	Description of groups, roles, and responsibilities for management of network components	Apigee and its production environment comply with this	Apigee clients are responsible for ensuring

		requirement internally	they are in compliance with this requirement
1.1.6	Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.1.7	Requirement to review firewall and router rule sets at least every six months	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.2	Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.2.2	Secure and synchronize router configuration files.	Apigee and its production environment comply with this requirement internally	Apigee is responsible for this requirement
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	Apigee and its production environment comply with this requirement internally	Apigee is responsible for this requirement
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance

			with this requirement
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.	Apigee and its production environment comply with this requirement internally	Apigee is responsible for this requirement
1.3.4	Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.3.5	Permit only "established" connections into the network.	Apigee and its production environment comply with this requirement internally	Apigee is responsible for this requirement
1.3.6	Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.3.7	Do not disclose private IP addresses and routing information to unauthorized parties. Note: Methods to obscure IP addressing may include, but are not limited to: ✔ Network Address Translation (NAT) ✔ Placing servers containing cardholder data behind proxy servers/firewalls ✔ Removal or filtering of route advertisements for private networks that employ registered addressing ✔ Internal use of RFC1918 address space instead of registered addresses	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
1.4	Install personal firewall software on any mobile and/or employee owned devices that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance

	access the network.		with this requirement
1.5	Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement

Requirement 2

Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
2.1	Always change vendor supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	N/A-Apigee does not have wireless networks in the environment	Apigee clients are responsible for ensuring they are in compliance with this requirement
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry- accepted system hardening standards.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
2.2.1	Implement only one primary function per server to prevent functions that require different security levels from coexisting on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure—for example, use secured technologies such as SSH, SFTP, TLS or IPSec VPN to protect insecure services such as NetBIOS, file sharing, Telnet, FTP, etc.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
2.2.4	Configure system security parameters to prevent misuse.	Apigee and its production	Apigee clients are

		environment comply with this requirement internally	responsible for ensuring they are in compliance with this requirement
2.2.5	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
2.3	Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or TLS for web-based management and other non-console administrative access.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for ensuring they are in compliance with this requirement
2.4	Maintain an inventory of system components that are in scope for PCI DSS	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
2.5	Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	N/A – Apigee is not a shared hosting provider	

Requirement 3

Protect Stored Cardholder Data

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
3.1	Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: ✔ Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements ✔ Processes for secure deletion of data when no longer needed ✔ Specific retention requirements for cardholder data ✔ A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.2	Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: There is a business justification and The data is stored securely.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.2.1	Do not store the full contents of any track (from the magnetic stripe	Apigee does not store or take	Apigee clients are

	located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic stripe data.	responsibility of the storage of cardholder data for the services offered	responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.2.2	Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card not present transactions.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking

			Storage
3.3	Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.4	Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: ✔ One way hashes based on strong cryptography, (hash must be of the entire PAN) ✔ Truncation (hashing cannot be used to replace the truncated segment of PAN) ✔ Index tokens and pads (pads must be securely stored) ✔ Strong cryptography with associated key management processes and procedures.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.4.1	If disk encryption is used (rather than file or column level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the

			links below for details on how to prevent the storage of cardholder data Masking Storage
3.5	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.5.1	**3.5.1** ***Additional Requirement for Service Providers Only:*** Maintain a documented description of the cryptographic architecture that includes: ✔ Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date ✔ Description of the key usage for each key. ✔ Inventory of any HSMs and other SCDs used for key management	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.5.2	Restrict access to cryptographic keys to the fewest number of custodians necessary.	Apigee does not store or take responsibility of the storage of	Apigee clients are responsible for

		cardholder data for the services offered	compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.5.3	Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: ✔ Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. ✔ Within a secure cryptographic device (such as a hardware/host security module (HSM) or PTS-approved point-of-interaction device). ✔ As at least two full-length key components or key shares, in accordance with an industry-accepted method.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.5.4	Store cryptographic keys in the fewest possible locations.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking

			Storage
3.6	Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.6.1	Generation of strong cryptographic keys	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.6.2	Secure cryptographic key distribution	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on

			how to prevent the storage of cardholder data Masking Storage
3.6.3	Secure cryptographic key storage	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.6.4	Cryptographic key changes for keys that have reached the end of their crypto-period (for example, after a defined period of time has passed and/or after a certain amount of cipher text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with	Apigee does not store or take responsibility of the storage of cardholder data for the	Apigee clients are responsible for compliance with this

	knowledge of a clear text key component), or keys are suspected of being compromised.	services offered	requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.6.6	If manual clear text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control. Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.6.7	Prevention of unauthorized substitution of cryptographic keys.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage

3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key custodian responsibilities.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage
3.7	Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	Apigee does not store or take responsibility of the storage of cardholder data for the services offered	Apigee clients are responsible for compliance with this requirement Customers should visit the links below for details on how to prevent the storage of cardholder data Masking Storage

Requirement 4

Encrypt Transmission of Cardholder Data Across Open, Public Networks

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
4.1	Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: ✔ Only trusted keys and certificates are accepted ✔ The protocol in use only supports secure versions or configurations ✔ The encryption strength is appropriate for the encryption methodology in use	Data encryption tools are not offered to customers for their use inside of Edge. However, customers are free to encrypt their PCI data prior to sending to Edge.	Data encryption tools are not offered to customers for their use inside of Edge. However, customers are free to encrypt their PCI data prior to sending to Edge. See links below for guidance on encryption in transmission. TLS Encryption
4.1.1	Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	N/A – Apigee does not have wireless networks in its environment	Apigee clients are responsible for compliance with this requirement
4.2	Never send unprotected PANs by end user messaging technologies (for example, email, instant messaging, chat, etc.).	Apigee and its production environment comply with this	Apigee clients are responsible for

		requirement internally	compliance with this requirement
4.3	Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

Requirement 5

Protect All Systems Against Malware and Regularly Update Anti-virus Software or Programs

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
5.1	Deploy antivirus software on all systems commonly affected by malicious software (particularly personal computers and servers).	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
5.1.1	Ensure that antivirus programs are capable of detecting, removing, and protecting against all known types of malicious software.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
5.1.2	For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
5.2	Ensure that all antivirus mechanisms are maintained as follows: ✔ Are kept current ✔ Perform periodic scans ✔ Generate audit logs which are retained per PCI DSS Requirement 10.7.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

5.3	Ensure that antivirus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
5.4	Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

Requirement 6

Develop and Maintain Secure Systems and Applications

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.3	Develop internal and external software applications (including web based administrative access to applications) securely, as follows: ✔ In accordance with PCI DSS (for example, secure authentication and logging) ✔ Based on industry standards and/or best practices ✔ Incorporating information security throughout the software-development life cycle	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.3.1	Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.3.2	Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes).	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.4	Follow change control processes and procedures for all changes to system components. The processes must include the following:	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

6.4.1	Separate development/test environments from production environments, and enforce the separation with access controls.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.4.2	Separation of duties between development/test and production environments	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.4.3	Production data (live PANs) are not used for testing or development	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.4.4	Removal of test data and accounts before production systems become active	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.4.5	Change control procedures for the implementation of security patches and software modifications must include the following:		
6.4.5.1	Documentation of impact.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.4.5.2	Documented change approval by authorized parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.4.5.3	Functionality testing to verify that the change does not adversely impact the security of the system.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.4.5.4	Back-out procedures.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

6.4.6	Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5	Address common coding vulnerabilities in software- development processes as follows: ✔ Train developers in secure coding techniques, including how to avoid common coding vulnerabilities, and understanding how sensitive data is handled in memory ✔ Develop applications based on secure coding guidelines	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.1	Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.2	Buffer overflows	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.3	Insecure cryptographic storage	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.4	Insecure communications	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.5	Improper error handling	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.6	All “high risk” vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

6.5.7	Cross-site scripting (XSS)	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.9	Cross-site request forgery (CSRF)	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.5.10	Broken authentication and session management Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.6	For public facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: ✔ Reviewing public facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes (Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2) ✔ Installing an automated technical solution that detects and prevents web based attacks (for example, a web application firewall) in front of public facing web applications, to continually check all traffic	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
6.7	Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

Requirement 7

Restrict Access to Cardholder Data by Business Need to Know

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance. Authorizations
7.1.1	Define access needs for each role, including: ✔ System components and data resources that each role needs to access for their job function ✔ Level of privilege required (for example, user, administrator, etc.) for accessing resources.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance. Authorizations
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance.

			Authorizations
7.1.3	Assign access based on individual personnel's job classification and function.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance. Authorizations
7.1.4	Require documented approval by authorized parties specifying required privileges.		Apigee clients are responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance. Authorizations
7.2	Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance. Authorizations
7.2.1	Coverage of all system components	Apigee and its production	Apigee clients are

		environment comply with this requirement internally	responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance. Authorizations
7.2.2	Assignment of privileges to individuals based on job classification and function.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance. Authorizations
7.2.3	Default “deny all” setting.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement when configuring user accounts within Edge. See link below for guidance. Authorizations
7.3	Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement when

			configuring user accounts within Edge. See link below for guidance. Authorizations

Requirement 8

Identify and Authenticate Access to System Components

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
8.1	Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:		
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Use link below for guidance Passwords
8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.1.3	Immediately revoke access for any terminated users.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.1.4	Remove/disable inactive user accounts at least every 90 days.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Use link below for guidance Passwords
8.1.5	Manage IDs used by vendors to access, support, or maintain system components via remote access as follows:	Apigee and its production environment comply with this	Apigee clients are responsible for

	✔ Enabled only during the time period needed and disabled when not in use ✔ Monitored when in use	requirement internally	compliance with this requirement
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Use link below for guidance Passwords
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.2	In addition to assigning a unique ID, ensure proper user authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: ✔ Something you know, such as a password or passphrase ✔ Something you have, such as a token device or smart card ✔ Something you are, such as a biometric	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Use link below for guidance Passwords
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	Apigee and its production environment comply with this requirement internally	Apigee is responsible for this requirement
8.2.2	Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.2.3	Passwords/phrases must meet the following:	Apigee and its production	Apigee clients are

	✔ Require a minimum length of at least seven characters ✔ Contain both numeric and alphabetic characters ✔ Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above	environment comply with this requirement internally	responsible for compliance with this requirement. Use link below for guidance Passwords
8.2.4	Change user passwords/passphrases at least every 90 days.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Use link below for guidance Passwords
8.2.5	Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Use link below for guidance Passwords
8.2.6	Set passwords/phrases for first time use and upon reset to a unique value for each user, and change immediately after the first use.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Use link below for guidance Passwords
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.3.1	Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access.	Apigee and its production environment comply with this	Apigee clients are responsible for compliance with this

		requirement internally	requirement. Use link below for guidance Passwords
8.3.2	Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Use link below for guidance Passwords
8.4	Document and communicate authentication procedures and policies to all users including: ✔ Guidance on selecting strong authentication credentials ✔ Guidance for how users should protect their authentication credentials ✔ Instructions not to reuse previously used passwords ✔ Instructions to change passwords if there is any suspicion the password could be compromised	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.5	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: ✔ Generic user IDs are disabled or removed ✔ Shared user IDs do not exist for system administration and other critical functions ✔ Shared and generic user IDs are not used to administer any system components	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

8.5.1	Additional requirement for service providers: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.6	Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: ✔ Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts ✔ Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.7	All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: ✔ All user access to, user queries of, and user actions on databases are through programmatic methods ✔ Only database administrators have the ability to directly access or query databases ✔ Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes)	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
8.8	Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

Requirement 9

Restrict Physical Access to Cardholder Data

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
9.1	Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.1.1	Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.1.2	Implement physical and/or logical controls to restrict access to publicly accessible network jacks.	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.1.3	Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.

		GCP.	
9.2	Develop procedures to easily distinguish between onsite personnel and visitors, to include: ✔ Identifying new onsite personnel or visitors (for example, assigning badges) ✔ Changes to access requirements ✔ Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.3	Control physical access for onsite personnel to the sensitive areas as follows: ✔ Access must be authorized and based on individual job function ✔ Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.4	Implement procedures to identify and authorize visitors. Procedures should include the following:	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.4.1	Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.4.2	Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	Apigee and its production environment comply with this requirement internally through the use of cloud service	Apigee is responsible for this requirement through the use of cloud service providers such as AWS

		providers such as AWS and GCP.	and GCP.
9.4.3	Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.4.4	A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	Apigee and its production environment comply with this requirement internally through the use of cloud service providers such as AWS and GCP.	Apigee is responsible for this requirement through the use of cloud service providers such as AWS and GCP.
9.5	Physically secure all media.	N/A	Apigee clients are responsible for compliance with this requirement
9.5.1	Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	N/A	Apigee clients are responsible for compliance with this requirement
9.6	Maintain strict control over the internal or external distribution of any kind of media, including the following:	N/A	Apigee clients are responsible for compliance with this requirement
9.6.1	Classify media so the sensitivity of the data can be determined.	N/A	Apigee clients are responsible for compliance with this requirement

9.6.2	Send the media by secured courier or other delivery method that can be accurately tracked.	N/A	Apigee clients are responsible for compliance with this requirement
9.6.3	Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	N/A	Apigee clients are responsible for compliance with this requirement
9.7	Maintain strict control over the storage and accessibility of media.	N/A	Apigee clients are responsible for compliance with this requirement
9.7.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	N/A	Apigee clients are responsible for compliance with this requirement
9.8	Destroy media when it is no longer needed for business or legal reasons as follows:		
9.8.1	Shred, incinerate, or pulp hard- copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	N/A	Apigee clients are responsible for compliance with this requirement
9.8.2	Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	N/A	Apigee clients are responsible for compliance with this requirement

9.9	Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	N/A	Apigee clients are responsible for compliance with this requirement
9.9.1	Maintain an up-to-date list of devices. The list should include the following: ✔ Make, model of device ✔ Location of device (for example, the address of the site or facility where the device is located) ✔ Device serial number or other method of unique identification	N/A	Apigee clients are responsible for compliance with this requirement
9.9.2	Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	N/A	Apigee clients are responsible for compliance with this requirement
9.9.3	Provide training for personnel to be aware of attempted tampering or replacement of devices.	N/A	Apigee clients are responsible for compliance with this requirement
9.10	Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

Requirement 10

Track and Monitor All Access to Network Resources and Cardholder Data

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
10.1	Implement audit trails to link all access to system components to each individual user.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.2	Implement automated audit trails for all system components to reconstruct the following events:		
10.2.1	All individual user accesses to cardholder data	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace

			Audit
10.2.2	All actions taken by any individual with root or administrative privileges	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.2.3	Access to all audit trails	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.2.4	Invalid logical access attempts	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative

			activities performed within the customer's org, including the use of Trace Audit
10.2.5	Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.2.6	Initialization, stopping, or pausing of the audit logs	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.2.7	Creation and deletion of system-level objects	Apigee and its production environment comply with this	Apigee clients are responsible for

		requirement internally	compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.3	Record at least the following audit trail entries for all system components for each event:		
10.3.1	User identification	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.3.2	Type of event	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed

			within the customer's org, including the use of Trace Audit
10.3.3	Date and time	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.3.4	Success or failure indication	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.3.5	Origination of event	Apigee and its production environment comply with this	Apigee clients are responsible for compliance with this

		requirement internally	requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace
10.3.6	Identity or name of affected data, system component, or resource.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.4	Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
10.4.1	Critical systems have the correct and consistent time.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
10.4.2	Time data is protected.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
10.4.3	Time settings are received from industry accepted time sources.	Apigee and its production environment comply with this	Apigee clients are responsible for

		requirement internally	compliance with this requirement
10.5	Secure audit trails so they cannot be altered.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
10.5.1	Limit viewing of audit trails to those with a job-related need.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.5.2	Protect audit trail files from unauthorized modifications.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	Apigee and its production environment comply with this	Apigee clients are responsible for

		requirement internally	compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.5.5	Use file integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace

			Audit
10.6	Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.6.1	Review the following at least daily: ✔ All security events ✔ Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD ✔ Logs of all critical system components ✔ Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS) authentication servers, e-commerce redirection servers, etc.)	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability

			to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.6.3	Follow up exceptions and anomalies identified during the review process.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit

10.8	***Additional Requirement for Service Providers Only*:** Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: ✔ Firewalls ✔ IDS/IPS ✔ FIM ✔ Anti-virus ✔ Physical access controls ✔ Logical access controls ✔ Audit logging mechanisms ✔ Segmentation controls (if used)	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement. Apigee customers have the ability to review the audit trail of all administrative activities performed within the customer's org, including the use of Trace Audit

10.8.1	**10.8.1** ***Additional Requirement for Service Providers Only*****:** Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: ✔ Restoring security functions ✔ Identifying and documenting the duration (date and time start to end) of the security failure ✔ Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause ✔ Identifying and addressing any security issues that arose during the failure ✔ Performing a risk assessment to determine whether further actions are required as a result of the security failure ✔ Implementing controls to prevent cause of failure from reoccurring ✔ Resuming monitoring of security controls	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement.
10.9	Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement.

Requirement 11

Regularly Test Security Systems and Processes

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
11.1	Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement.
11.1.1	Maintain an inventory of authorized wireless access points including a documented business justification.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
11.1.2	Implement incident response procedures in the event unauthorized wireless access points are detected.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter.

			Use link below for additional details Scanning
11.2.1	Perform quarterly internal vulnerability scans and rescans as needed, until all “high-risk” vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter. Use link below for additional details Scanning
11.2.2	Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual

			API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter. Use link below for additional details Scanning
11.2.3	Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter. Use link below for additional details Scanning
11.3	Implement a methodology for penetration testing that includes the	Apigee and its production	Edge Cloud, customers

	following: ✔ Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) ✔ Includes coverage for the entire CDE perimeter and critical systems ✔ Includes testing from both inside and outside the network ✔ Includes testing to validate any segmentation and scope-reduction controls ✔ Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 ✔ Defines network-layer penetration tests to include components that support network functions as well as operating systems ✔ Includes review and consideration of threats and vulnerabilities experienced in the last 12 months ✔ Specifies retention of penetration testing results and remediation activities results	environment comply with this requirement internally	are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter. Use link below for additional details Scanning
11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter.

			Use link below for additional details Scanning
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter. Use link below for additional details Scanning
11.3.3	Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing

			should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter. Use link below for additional details Scanning
11.3.4	If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of- scope systems from in-scope systems.	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter. Use link below for additional details Scanning

11.3.4.1	***Additional Requirement for Service Providers Only:*** If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods.	Apigee and its production environment comply with this requirement internally	Edge Cloud, customers are responsible for the scanning and testing of their API endpoints (sometimes called the "runtime components") in Edge. Customer testing should cover the actual API proxy services hosted on Edge where API traffic is sent into Edge prior to being processed and then delivered to the customer datacenter. Use link below for additional details Scanning
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
11.5	Deploy a change-detection mechanism (for example, file- integrity monitoring tools) to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Note: For change- detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

	detection mechanisms such as file- integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).		
11.5.1	Implement a process to respond to any alerts generated by the change-detection solution.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
11.6	Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement

Requirement 12

Maintain a Policy That Addresses Information Security for All Personnel

Req#	PCI DSS Requirement	Apigee Responsibility	Client Responsibility
12.1	Establish, publish, maintain, and disseminate a security policy.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.1.1	Review the security policy at least annually and update the policy when the environment changes.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.2	Implement a risk-assessment process that: ✔ Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.) ✔ Identifies critical assets, threats, and vulnerabilities, and ✔ Results in a formal risk assessment	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3	Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following:	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.1	Explicit approval by authorized parties	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.2	Authentication for use of the technology	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.3	A list of all such devices and personnel with access	Apigee and its production environment comply with this	Apigee clients are responsible for

		requirement internally	compliance with this requirement
12.3.4	A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.5	Acceptable uses of the technology	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.6	Acceptable network locations for the technologies	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.7	List of company-approved products	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.8	Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.9	Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.3.10	For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.4	Ensure that the security policy and procedures clearly define	Apigee and its production	Apigee clients are

	information security responsibilities for all personnel.	environment comply with this requirement internally	responsible for compliance with this requirement
12.5	Assign to an individual or team the following information security management responsibilities:	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.5.1	Establish, document, and distribute security policies and procedures.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.5.2	Monitor and analyze security alerts and information, and distribute to appropriate personnel.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.5.3	Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.5.4	Administer user accounts, including additions, deletions, and modifications.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.5.5	Monitor and control all access to data.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.6	Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.6.1	Educate personnel upon hire and at least annually.	Apigee and its production environment comply with this	Apigee clients are responsible for compliance with this

		requirement internally	requirement
12.6.2	Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.7	Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.)	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.8	Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.8.1	Maintain a list of service providers.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.8.2	Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.8.3	Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.8.4	Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.8.5	Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	Apigee and its production environment comply with this	Apigee clients are responsible for compliance with this

		requirement internally	requirement
12.9	Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.10	Implement an incident response plan. Be prepared to respond immediately to a system breach.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.10.1	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: ✔ Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum ✔ Specific incident response procedures ✔ Business recovery and continuity procedures ✔ Data backup processes ✔ Analysis of legal requirements for reporting compromises ✔ Coverage and responses of all critical system components ✔ Reference or inclusion of incident response procedures from the payment brands	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.10.2	Test the plan at least annually.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.10.3	Designate specific personnel to be available on a 24/7 basis to respond to alerts.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.10.4	Provide appropriate training to staff with security breach response responsibilities.	Apigee and its production environment comply with this	Apigee clients are responsible for compliance with this

		requirement internally	requirement
12.10.5	Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.10.6	Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.11	***Additional Requirement for Service Providers Only:*** Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: ✔ Daily log reviews ✔ Firewall rule-set reviews ✔ Applying configuration standards to new systems ✔ Responding to security alerts ✔ Change management processes	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement
12.11.1	***Additional Requirement for Service Providers Only:*** Maintain documentation of quarterly review process to include: ✔ Documenting results of the reviews ✔ Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program	Apigee and its production environment comply with this requirement internally	Apigee clients are responsible for compliance with this requirement