Responsibility Matrix PCI DSS 4.0

Akamai Content Delivery & Security Services

June 2024

Purpose

Akamai provides below a detailed matrix of PCI DSS requirements, including the description of whether responsibility for each individual control lies with Akamai, our customers, or whether responsibility is shared between both parties.

While leveraging Akamai’s cloud computing services infrastructure and services, customers have the ability to create their own cardholder data environment.

Overview

The PCI DSS responsibility matrix is intended for use by Akamai customers and their Qualified Security Assessors (QSAs) for use in audits for PCI compliance. The responsibility matrix describes, in accordance with Requirement 12.8.5 and other requirements, the actions an Akamai customer must take to maintain its own PCI compliance when cardholder data (CHD) and other sensitive data is passing through or stored on Akamai's systems.

PCI DSS and Akamai Services

Akamai’s services that may be used in a PCI DSS compliant manner include the following:

- Secure CDN with Enhanced TLS (the “Secure CDN”);
- Content Delivery products such as Ion, Dynamic Site Accelerator, API Acceleration, and Adaptive Media Delivery, when running on the Secure CDN;
- EdgeWorkers, when running on the Secure CDN;
- mPulse digital performance management services;
- App and API security products such as App & API Protector (including the Malware Protection add-on), Account Protector, Kona Site Defender, API Gateway, Cloudlets, and Bot Manager (Standard and Premier), when running on the Secure CDN;
- API Security;
- Client-Side Protection & Compliance;
- Audience Hijacking Protector;
- Secure Internet Access Enterprise (f/k/a Enterprise Threat Protector);
- Akamai MFA;

- Akamai Guardicore Segmentation; and
- The following cloud computing solutions: Dedicated CPU, Shared CPU, and High Memory.

Secure CDN with Enhanced TLS

Akamai's Secure CDN is the core component of its PCI compliant content delivery services. The servers in this network are physically secured against intrusion while being widely distributed around the globe to ensure availability and maximize origin offload. The Secure CDN also provides customers with custom TLS certificates with the flexibility to configure them to satisfy various security and business requirements. The Secure CDN is not typically sold as an independent service but is instead a feature included with most of Akamai's web performance and cloud security products, as described below.

Content Delivery Solutions

Akamai's content delivery solutions, including Ion and such legacy CDN solutions as Terra Alta or Dynamic Site Delivery, typically have the option of having their content delivered securely, in which case that content is delivered via the Secure CDN, and may be used in a PCI DSS compliant manner. Additional products, such as mPulse digital performance management, Cloudlets, and dynamic content delivery options such as adaptive image compression and pre-fetching options, have all been designed to work on Akamai's Secure CDN servers, and may be configured to be fully compliant with PCI DSS.

Edge Computing Solutions

The Akamai EdgeWorkers solution, which enables customers (developers) to create their own services using JavaScript and deploy them across our Secure CDN, is included in Akamai's PCI DSS assessment and may be used in a manner fully-compliant with PCI DSS.

The Akamai EdgeKV distributed key value store is not PCI DSS compliant, however. Please see "Non-Compliant Services" below for more information.

App and API Security Solutions

As with the above content delivery solutions, Akamai's App & API Protector (including the Malware Protection add-on), Kona Site Defender, Account Protector, and Bot Manager application as well as API security products may be configured to operate over the Secure CDN in a PCI DSS compliant manner.

In addition, the web application firewall (WAF) components of App & API Protector, Kona Site Defender, and Web Application Protector may be used by customers to help satisfy their obligations under Requirements 6.4.1 and 6.4.2 of PCI DSS 4.0.0, all of which encourage the use of a WAF, provided that the WAF is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances.

Bot Manager provides advanced bot detections designed to detect and mitigate the most sophisticated bots, like those typically seen in use cases such as credential abuse, inventory hoarding, gift card balance checking, and other forms of web fraud. Bot Manager's unmatched detections and mitigation capabilities allow automated operations to run more effectively and safely.

Account Protector is designed to prevent account takeover and human fraudulent activity by detecting during the authentication process whether a human user is the legitimate account owner. It does this by generating risk and trust signals to calculate the likelihood of a malicious request, self-tuning as the number of logins increase for the same set of credentials.

API Security protects all APIs, alerts teams to API vulnerabilities, analyzes runtime API interactions for abnormal, suspicious, and malicious behavior, and enables real-time threat response and vulnerability remediation.

Client-Side Protection & Compliance (formerly known as Page Integrity Manager) is a behavioral detection technology for web apps that catalogs JavaScript resources and identifies suspicious and malicious script behaviors. It then notifies security teams with actionable insight, empowering them to rapidly understand, and act on the threats. Client-Side Protection & Compliance it itself PCI DSS compliant and it may also be used by customers to help satisfy their obligations under Requirements 6.4.3 and 11.6.1 of PCI DSS 4.0.0, including managing script inventory, ensuring authorization and integrity of scripts in web applications, and the detection of and response to unauthorized changes to payment pages, respectively, provided that Client-Side Protection & Compliance is configured appropriately in the customers' environment in a manner that their PCI DSS qualified security assessors agree is appropriate under the circumstances.

Audience Hijacking Protector is a key security product for client-side web application protection against unwanted activity from client side plug-ins, browser extensions, and malware. Detecting and mitigating these types of interactions empowers our customers to protect their user journey, preventing users from being redirected to competing and/or malicious websites, reducing shopping cart abandonment rates, curbing fraudulent affiliate activities, and mitigating additional security and privacy risks. As a result, Audience Hijacking Protector will not only improve end-user experiences, but also improve key customer metrics (e.g., conversions, bounce rate, AOV), all while making the web safer for end-users.

Cloud Computing Solutions

Akamai offers a variety of cloud computing solutions. The following virtual machine hosting services are included in Akamai's current PCI DSS assessment: Dedicated CPU, Shared CPU, and High Memory.

Network and Infrastructure Security Solutions

Secure Internet Access (f/k/a Enterprise Threat Protector) (SIA Enterprise) is Akamai's PCI DSS compliant, cloud-based security solution that enables an organization to defend against advanced threats such as phishing, malware, ransomware, and DNS-based data exfiltration. As part of its Secure Web Gateway offering, SIA lets customers set up a proxy that performs URL filtering and anti-malware scanning on user traffic. The proxy acts as a man-in-the-middle that intercepts SSH/TLS traffic. A certificate generated in SIA or signed by your organization's Certificate Authority (CA) establishes trust between the client and proxy, and further allows Akamai to create a short-lived, dynamically generated certificate that's used to communicate with the destination server.

SIA Proxy inspects the URL path of requests and checks if a URL is a known threat. If it is a threat, the threat is handled based on the policy action that's assigned in an SIA policy. SIA proxy also performs payload analysis to determine whether websites contain malicious content.

Akamai's Prolexic DDoS mitigation solutions are not included in Akamai's PCI DSS assessment but are designed to have no access to or impact on cardholder data, and are therefore readily available to protect customers and their PCI DSS compliant Internet properties from attacks.

Enterprise Security Solutions

Akamai Guardicore Segmentation (AGS) is a microsegmentation solution designed to limit user access to only applications that are authorized to communicate with each other, significantly reducing the threat surface and risk exposure to the spread of malware.

Akamai's Enterprise Application Access (EAA) provides the infrastructure for customers to operate a "Zero-Trust" model for remotely accessing their corporate IT resources that neither stores nor processes cardholder data and has no ability to access customer application data streams. While EAA is not included in Akamai's PCI DSS assessment, services have been reviewed by a Qualified Security Assessor (QSA) and have been determined to be acceptable to use in customers' cardholder data environments.

Non-Compliant Services

Other Akamai services, such as the Netstorage network for storing large files, the legacy FreeFlow CDN, which is intended for traffic containing less sensitive data, Identity Cloud, EdgeKV, and Standard TLS solutions, are not in scope for Akamai's PCI DSS assessment. Customers must configure their properties to avoid using these services in their cardholder data environments.

Responsibility Matrix

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
1.1	Processes and mechanisms for installing and maintaining network security controls are defined and understood.		Responsible		
1.1.1	All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.		Responsible		
1.1.2	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.		Responsible		
1.2	Network security controls (NSCs) are configured and maintained.		Responsible		
1.2.1	Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.		Responsible		
1.2.2	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.		Responsible		
1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.				Customers' network diagram should include any data flows to Akamai Products.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
1.2.4	An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.				Customers' network diagram should depict use of Akamai Products including all connections between Akamai's networks and the customer's CDE.
1.2.5	All services, protocols, and ports allowed are identified, approved, and have a defined business need.		Responsible		
1.2.6	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.		Responsible		
1.2.7	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.		Responsible		
1.2.8	Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.		Responsible		
1.3	Network access to and from the cardholder data environment is restricted.		Akamai SCDN, APR/BMP, Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for restricting access to and from their own CDE.	
1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.		Akamai SCDN, APR/BMP, Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for restricting access to and from their own CDE.	
1.3.2	Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.		Akamai SCDN, APR/BMP, Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for restricting access to and from their own CDE.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
1.3.3	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.		Akamai SCDN, APR/BMP, Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for restricting access to and from their own CDE.	
1.4	Network connections between trusted and untrusted networks are controlled.		Responsible		
1.4.1	NSCs are implemented between trusted and untrusted networks.		Responsible		
1.4.2	Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.		Responsible		
1.4.3	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.		Responsible		
1.4.4	System components that store cardholder data are not directly accessible from untrusted networks.		Responsible		
1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
1.5	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		Responsible		
1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.				Customer is responsible for ensuring that a personal firewall is installed on any device they use to connect to Akamai Control Center
2.1	Processes and mechanisms for applying secure configurations to all system components are defined and understood.		Responsible		
2.1.1	All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.		Responsible		
2.1.2	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.		Responsible		
2.2	System components are configured and managed securely.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
2.2.1	Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.		Responsible		
2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.		Responsible		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
2.2.3	Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, OR • Primary functions with differing security levels that exist on the same system component are isolated from each other, OR • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.		Responsible		
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.		Responsible		
2.2.5	If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.		Responsible		
2.2.6	System security parameters are configured to prevent misuse.		Responsible		
2.2.7	All non-console administrative access is encrypted using strong cryptography.		Responsible		
2.3	Wireless environments are configured and managed securely.		Akamai excludes wireless subsystems from the CDE by design.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
2.3.1	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.		Akamai excludes wireless subsystems from the CDE by design.		
2.3.2	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.		Akamai excludes wireless subsystems from the CDE by design.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.1	Processes and mechanisms for protecting stored account data are defined and understood.	SCDN: N/A because Akamai does not store cardholder data.	BMP/APr: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.		API Security: Joint Responsibility. Akamai, in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.1.1	All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	SCDN: Akamai does not store cardholder data.	BMP/APr: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.		API Security: Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.1.2	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	SCDN: Akamai does not store cardholder data.	BMP/APr: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.		API Security: Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.
3.2	Storage of account data is kept to a minimum.	API Security: Account data is not stored in the platform.	BMP/APR: The service provider is responsible for keeping CHD storage to a minimum. Malware Protection: The service provider is responsible for keeping CHD storage to a minimum.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines.	

3.2.1	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. **This bullet is a best practice until its effective date on 31st March 2025.** • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	API Security: API Security product does not store account data. Akamai API Security Cloud applies retention policies that purge data once it is no longer needed for the purpose for which it was collected: The API Security data lake short-term storage retains data for 30 days and aggregate data (such as statistics about entities) for 120 days. This data is used in the customer-facing user interface. The API Security data lake long-term storage retains data for up to 1 year for research purposes. Alert data, including the alerted calls (request-response pairs), are stored indefinitely, in order to enable retroactive investigation even past the 30-day data retention window. Upon expiration of the ShadowHunt managed threat hunting service, the service and access to the data by the Akamai threat hunters will be revoked within 7 days. Upon termination of the API Security service,	BMP/APR: The service provider is responsible for keeping CHD storage to a minimum. Malware Protection: The service provider is responsible for keeping CHD storage to a minimum.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines.	

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
		access to the user interface and collection of API activity data are disabled after 7 days. Afterward, data in active systems in Akamai API Security Cloud will be marked inactive and removed from the active systems. Permanent deletion of all data may take up to an additional 180 days.			

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.3	Sensitive authentication data (SAD) is not stored after authorization.	API Security: Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.	Malware Protection: Service Provider is responsible for rending all data unrecoverable if SAD is received.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines. BMP/APr: Customers are responsible for ensuring no SAD is sent to Akamai machines.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.3.1	SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	API Security: Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines. BMP/APr: Customers are responsible for ensuring no SAD is sent to Akamai machines.	Malware Protection: Service Provider is responsible for rending all data unrecoverable if SAD is received.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.3.1.1	The full contents of any track are not retained upon completion of the authorization process.	API Security: Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.	Malware Protection: Service Provider is responsible for rending all data unrecoverable if SAD is received.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines. BMP/APr: Customers are responsible for ensuring no SAD is sent to Akamai machines.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.3.1.2	The card verification code is not retained upon completion of the authorization process.	API Security: N/A. Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.	Malware Protection: Service Provider is responsible for rending all data unrecoverable if SAD is received.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines. BMP/APr: Customers are responsible for ensuring no SAD is sent to Akamai machines.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.3.1.3	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	API Security: N/A. Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.	Malware Protection: Service Provider is responsible for rending all data unrecoverable if SAD is received.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines. BMP/APr: Customers are responsible for ensuring no SAD is sent to Akamai machines.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography. **This requirement is a best practice until its effective date on 31st March 2025.**	API Security: N/A. Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.	Malware Protection: Service Provider is responsible for rending all data unrecoverable if SAD is received.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines. BMP/APr: Customers are responsible for ensuring no SAD is sent to Akamai machines.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.3.3	Additional requirement for issuers and companies that support issuing services and store sensitive authentication data: Any storage of sensitive authentication data is: • Limited to that which is needed for a legitimate issuing business need and is secured. • Encrypted using strong cryptography. **This bullet is a best practice until its effective date on 31st March, 2025.**	API Security: N/A. Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one-way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.	Malware Protection: Service Provider is responsible for rending all data unrecoverable if SAD is received.	Akamai SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause credit card data to be cached or otherwise stored on Akamai machines. BMP/APr: Customers are responsible for ensuring no SAD is sent to Akamai machines.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.4	Access to displays of full PAN and ability to copy PAN is restricted.	API Security: The API Security solution does not have the ability to display or copy PANs.	BMP/APR: The service provider is responsible for masking PAN data when displayed. Malware Protection: The service provider is responsible for masking PAN data if displayed.	Akamai SCDN: If customers are transmitting cardholder data for user viewing over the Akamai Secure CDN with Enhanced TLS, they are responsible for ensuring that PANs are appropriately masked.	
3.4.1	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	API Security: The API Security solution does not have the ability to display or copy PANs.	BMP/APR: The service provider is responsible for masking PAN data when displayed. Malware Protection: The service provider is responsible for masking PAN data if displayed.	Akamai SCDN: If customers are transmitting cardholder data for user viewing over the Akamai Secure CDN with Enhanced TLS, they are responsible for ensuring that PANs are appropriately masked.	
3.4.2	When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need. **This requirement is a best practice until its effective date on 31st March 2025.**	API Security: The API Security solution does not have the ability to display or copy PANs.	BMP/APR: The service provider is responsible for masking PAN data when displayed. Malware Protection: The service provider is responsible for masking PAN data if displayed.	Akamai SCDN: If customers are transmitting cardholder data for user viewing over the Akamai Secure CDN with Enhanced TLS, they are responsible for ensuring that PANs are appropriately masked.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.5	Primary account number (PAN) is secured wherever it is stored.		BMP/APR: The service provider is responsible for ensuring PAN is unreadable everywhere it is stored. Malware Protection: The service provider is responsible for ensuring PAN is unreadable everywhere it is stored.	SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause PAN to be cached or otherwise stored on Akamai machines.	API Security: Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one-way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
3.5.1	PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN. • Index tokens. • Strong cryptography with associated key management processes and procedures.		BMP/APR: The service provider is responsible for ensuring PAN is unreadable everywhere it is stored. Malware Protection: The service provider is responsible for ensuring PAN is unreadable everywhere it is stored.	SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause PAN to be cached or otherwise stored on Akamai machines.	API Security: Akamai in conjunction with customers should configure tokenization for all cardholder data entering the platform from on premise nodes. Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it. API activity data that is sourced from the Akamai CDN are protected with a one-way salted hash. Akamai personnel have no ability to reverse the hashed values to derive the original clear text values. Akamai is responsible for the continued successful operation of the hashing processes originating in the Akamai CDN.
3.5.1.1	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1) are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.		BMP/APR: The service provider is responsible for ensuring PAN is unreadable everywhere it is stored. Malware Protection: The service provider is responsible for ensuring PAN is unreadable everywhere it is stored.	SCDN: Customer is responsible for ensuring that their configurations for using Akamai services will not cause PAN to be cached or otherwise stored on Akamai machines.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.5.1.2	If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media OR • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1. **This requirement is a best practice until its effective date on 31st March 2025.**	Akamai SCDN: Not applicable as it doesn't store cardholder data. BMP/APR: Not applicable, does not use disk encryption. Malware Protection: Service provider is responsible for encrypting the data.	Responsible		
3.5.1.3	If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	Akamai SCDN: Not applicable as it doesn't store cardholder data. BMP/APR: Not applicable, does not use disk encryption. Malware Protection: Service provider is responsible for encrypting the data. API Security: Disk level encryption is not used in the API Security product to render PANs unreadable.	Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.6	Cryptographic keys used to protect stored account data are secured.	Akamai SCDN: Not applicable as it doesn't store cardholder data. BMP/APR: Not applicable, does not use disk encryption. Malware Protection: Service provider is responsible for encrypting the data. API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.6.1	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	SCDN: Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	Responsible	
3.6.1.1	Additional requirement for service providers only: A documented description of the cryptographic architecture is maintained that includes: • Details of all algorithms, protocols, and keys used for the protection of stored account data, including key strength and expiry date. • Preventing the use of the same cryptographic keys in production and test environments. **This bullet is a best practice until its effective date**; • Description of the key usage for each key. • Inventory of any hardware security modules (HSMs), key management systems (KMS), and other secure cryptographic devices (SCDs) used for key management, including type and location of devices, as outlined in Requirement 12.3.4.	SCDN: Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	Responsible	

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
3.6.1.2	Secret and private keys used to encrypt/decrypt stored account data are stored 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 (SCD), such as a hardware 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.	SCDN: Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	
3.6.1.3	Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	SCDN: Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	
3.6.1.4	Cryptographic keys are stored in the fewest possible locations.	SCDN: Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.7	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	
3.7.1	Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	
3.7.2	Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
3.7.3	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	
3.7.4	Key management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.7.5	Key management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	
3.7.6	Where manual cleartext cryptographic key management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	
3.7.7	Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
3.7.8	Key management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	SCDN: NA Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Customers are responsible for all key management activities associated with the tokenization process. Akamai personnel have no access to the keys which are used to tokenize the data and are not able to decrypt it.	
3.7.9	Additional requirement for service providers only: Where a service provider shares cryptographic keys with its customers for transmission or storage of account data, guidance on secure transmission, storage and updating of such keys is documented and distributed to the service provider's customers.	SCDN: N/A. Akamai SCDN does not store cardholder data.	BMP/APR: This is a service provider responsibility. Malware Protection: This is a service provider responsibility.	API Security: Akamai does not share cryptographic keys with API Security customers. Customers are responsible for all aspects of key management associated with the on premise node.	
4.1	Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.		API Security: Akamai protects all data traversing public networks to and from the solution using TLS 1.2 or higher.	SCDN: Customer must train their relevant personnel to ensure that Akamai services carrying customer PCI data are configured to use strong cryptography at all times.	BMP/APR: This is a shared responsibility to ensure all parties involved are trained in relevant policies and procedures for encrypting transmission of CHD. Malware Protection: This is a shared responsibility to ensure all parties involved are trained in relevant policies and procedures for encrypting transmission of CHD.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
4.1.1	All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.		API Security: Akamai protects all data traversing public networks to and from the solution using TLS 1.2 or higher.	SCDN: Customer must train their relevant personnel to ensure that Akamai services carrying customer PCI data are configured to use strong cryptography at all times.	BMP/APR: This is a shared responsibility to ensure all parties involved are trained in relevant policies and procedures for encrypting transmission of CHD. Malware Protection: This is a shared responsibility to ensure all parties involved are trained in relevant policies and procedures for encrypting transmission of CHD.
4.1.2	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.		API Security: Akamai protects all data traversing public networks to and from the solution using TLS 1.2 or higher.	SCDN: Customer must train their relevant personnel to ensure that Akamai services carrying customer PCI data are configured to use strong cryptography at all times.	BMP/APR: This is a shared responsibility to ensure all parties involved are trained in relevant policies and procedures for encrypting transmission of CHD. Malware Protection: This is a shared responsibility to ensure all parties involved are trained in relevant policies and procedures for encrypting transmission of CHD.
4.2	PAN is protected with strong cryptography during transmission.		API Security: Akamai protects all data traversing public networks to and from the solution using TLS 1.2 or higher.	It is the customer's responsibility to never send PANs using Akamai services without taking appropriate action to secure the contents.	BMP/APR: This is a joint responsibility to ensure neither customer nor service provider send PAN by end-user technologies. Malware Protection: This is a joint responsibility to ensure neither customer nor service provider send PAN by end-user technologies.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
4.2.1	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. **This bullet is a best practice until its effective date on 31st March, 2025.** • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	Akamai SCDN: NA. It does not store cardholder data.	API Security: Akamai protects all data traversing public networks to and from the solution using TLS 1.2 or higher.		BMP/APR: It is a shared responsibility between customer and BMP/APR product. Malware Protection: It is a shared responsibility between customer and Malware Protection.
4.2.1.1	An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained. **This requirement is a best practice until 31 March 2025.**		API Security: Akamai protects all data traversing public networks to and from the solution using TLS 1.2 or higher.	It is the customer's responsibility to never send PANs using Akamai services without taking appropriate action to secure the contents.	BMP/APR: This is a joint responsibility to ensure neither customer nor service provider send PAN by end-user technologies. Malware Protection: This is a joint responsibility to ensure neither customer nor service provider send PAN by end-user technologies.
4.2.1.2	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	Akamai excludes wireless subsystems from the CDE by design.			

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
4.2.2	PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.		API Security: Akamai protects all data traversing public networks to and from the solution using TLS 1.2 or higher.	It is the customer's responsibility to never send PANs using Akamai services without taking appropriate action to secure the contents.	BMP/APR: This is a joint responsibility to ensure neither customer nor service provider send PAN by end-user technologies. Malware Protection: This is a joint responsibility to ensure neither customer nor service provider send PAN by end-user technologies.
5.1	Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.1.1	All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
5.1.2	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.2	Malicious software (malware) is prevented, or detected and addressed.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
5.2.2	The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.2.3	Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.2.3.1	The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025.**				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
5.3	Anti-malware mechanisms and processes are active, maintained, and monitored.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.3.1	The anti-malware solution(s) is kept current via automatic updates.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.3.2	The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
5.3.2.1	If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025.**				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.3.3	For removable electronic media, the antimalware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, OR • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted. **This requirement is a best practice until 31 March 2025.**				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.4	Anti-phishing mechanisms protect users against phishing attacks.				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
5.4.1	Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks. **This requirement is a best practice until 31 March 2025.**				Customer is responsible for ensuring selecting appropriately capable anti-virus software is installed on their systems. The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
6.1	Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.				The scope of Akamai's responsibility is limited to processes and mechanisms identified within this requirement for the protection of the application and related system components under the control of Akamai.
6.1.1	All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.				Customers are responsible for security policies and operational procedures for all executable content they create which handles PCI data and is served by the Akamai Secure CDN with Enhanced TLS. BMP/APR: It is a joint responsibility as the customer is responsible for the secure development of the systems they use to share data with BMP/APR.
6.1.2	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.				Akamai and Customers are responsible for their own internal software development processes as applies to PCI DSS Requirement 6.
6.2	Bespoke and custom software are developed securely.				Akamai and Customers are responsible for their own internal software development processes as applies to PCI DSS Requirement 6.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
6.2.1	Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.				Akamai and Customers are responsible for their own internal software development processes as applies to PCI DSS Requirement 6.
6.2.2	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.				Customers are responsible for addressing common coding vulnerabilities described in this section for all executable content they create which handles PCI data and is served by the Akamai Secure CDN with Enhanced TLS. BMP/APR: It is a joint responsibility as the customer is responsible for the secure development of the systems they use to share data with BMP/APR.
6.2.3	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.				Akamai and Customers are responsible for their own internal software development processes as applies to PCI DSS Requirement 6.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
6.2.3.1	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. • Reviewed and approved by management prior to release.				Customers are responsible for addressing common coding vulnerabilities described in this section for all executable content they create which handles PCI data and is served by the Akamai Secure CDN with Enhanced TLS. BMP/APR: It is a joint responsibility as the customer is responsible for the secure development of the systems they use to share data with BMP/APR.

6.2.4	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following: • Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws. • Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data. • Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation. • Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). • Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms. • Attacks via any “high-risk” vulnerabilities identified in the				Akamai and customers are each responsible for software engineering techniques and other methods to prevent and mitigate common software attacks and related vulnerabilities in bespoke and customer software within their control.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
	vulnerability identification process, as defined in Requirement 6.3.1.				
6.3	Security vulnerabilities are identified and addressed.				Joint responsibility.
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.				Joint responsibility.
6.3.2	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management. **This requirement is a best practice until 31 March 2025.**				Joint responsibility.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).				Joint responsibility.
6.4	Public-facing web applications are protected against attacks.				Joint responsibility.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections OR • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web-based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated. **This requirement will be superseded by 6.4.2 after 31st March 2025.**				Joint responsibility.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated. **This requirement is a best practice until 31 March 2025.**				Joint responsibility.
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows: • A method is implemented to confirm that each script is authorized. • A method is implemented to assure the integrity of each script. • An inventory of all scripts is maintained with written justification as to why each is necessary. **This requirement is a best practice until 31 March 2025.**				Joint responsibility.
6.5	Changes to all system components are managed securely.				Joint responsibility.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
6.5.1	Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.				Joint responsibility.
6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.				Customers will are responsible for tracking and documenting PCI-relevant changes to their Akamai configurations.
6.5.3	Pre-production environments are separated from production environments and the separation is enforced with access controls.				Customers must review their own executable content transmitted over Akamai services prior to release to production or customers in order to identify any potential coding vulnerabilities. BMP/APR: It is a joint responsibility as the customer is responsible for the secure development of the systems they use to share data with BMP/APR.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.				Customers must review their own executable content transmitted over Akamai services prior to release to production or customers in order to identify any potential coding vulnerabilities. BMP/APR: It is a joint responsibility as the customer is responsible for the secure development of the systems they use to share data with BMP/APR.
6.5.5	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.				Customers must review their own executable content transmitted over Akamai services prior to release to production or customers in order to identify any potential coding vulnerabilities. BMP/APR: It is a joint responsibility as the customer is responsible for the secure development of the systems they use to share data with BMP/APR.
6.5.6	Test data and test accounts are removed from system components before the system goes into production.				Akamai and Customers are responsible for their own internal software development processes as applies to PCI DSS Requirement 6.
7.1	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.				Customers must limit access to API Security accounts to those whose job requires such access.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
7.1.1	All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.				Customer must ensure that security policies and operational procedures for restricting access to the Akamai Control Center and OPEN API credentials are documented, in use, and known to all affected parties. API Security: Customers must limit access to API Security accounts to those whose job requires such access.
7.1.2	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.				Customers must define and assign roles and responsibilities for managing access.
7.2	Access to system components and data is appropriately defined and assigned.				SCDN: Customers must configure the Akamai Control Center's access control system for their accounts to restrict access to all PCI-relevant Akamai services and configurations. API Security: Customers must manage access to the solution ensuring access is appropriately defined and assigned.

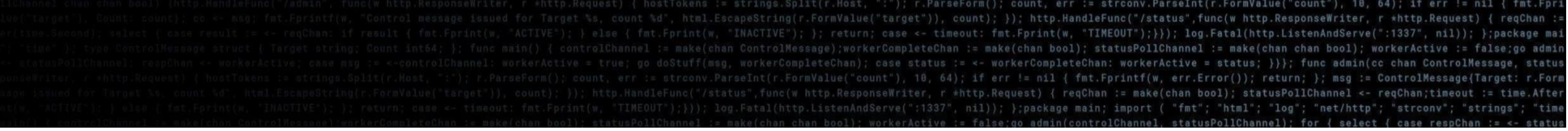
		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity’s business and access needs. • Access to system components and data resources that is based on users’ job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.				SCDN: Customers must configure the Akamai Control Center's access control system for their accounts to restrict access to all PCI-relevant Akamai services and configurations. API Security: Customers must manage access to the solution ensuring access is appropriately defined and assigned.
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.				SCDN: Customers must configure the Akamai Control Center's access control system for their accounts to restrict access to all PCI-relevant Akamai services and configurations. API Security: Customers must manage access to the solution ensuring access is appropriately defined and assigned.
7.2.3	Required privileges are approved by authorized personnel.				Customers are responsible for their own internal approval processes and documentation of approvals for access.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
7.2.4	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. **This requirement is a best practice until 31 March 2025.**				Customers are responsible for reviewing their user's access to the products at the interval required by PCI.
7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use. **This requirement is a best practice until 31 March 2025.**				The scope of Akamai's responsibility is limited to application and system accounts that Akamai manages.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
7.2.5.1	All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate. **This requirement is a best practice until 31 March 2025.**				The scope of Akamai's responsibility is limited to application and system accounts that Akamai manages.
7.2.6	All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.	N/A - Akamai does not store cardholder data.	BMP/APR: This is a service provider responsibility.		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
7.3	Access to system components and data is managed via an access control system(s).				SCDN: Customers must ensure that the Akamai Control Center's access control system restricts user access to only those privileges which are necessary for each user. API Security: Akamai is responsible for the access control system that is used for managed system components that deliver the application to customers. The customer is responsible for managing user access to the solution for their employees.
7.3.1	An access control system(s) is in place that restricts access based on a user’s need to know and covers all system components.				SCDN: Customers must ensure that the Akamai Control Center's access control system restricts user access to only those privileges which are necessary for each user. API Security: Akamai is responsible for the access control system that is used for managed system components that deliver the application to customers. The customer is responsible for managing user access to the solution for their employees.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
7.3.2	The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.				SCDN: Customers must ensure that the Akamai Control Center's access control system restricts user access to only those privileges which are necessary for each user. API Security: Akamai is responsible for the access control system that is used for managed system components that deliver the application to customers. The customer is responsible for managing user access to the solution for their employees.
7.3.3	The access control system(s) is set to “deny all” by default.				SCDN: Customers must ensure that the Akamai Control Center's access control system restricts user access to only those privileges which are necessary for each user. API Security: Akamai is responsible for the access control system that is used for managed system components that deliver the application to customers. The customer is responsible for managing user access to the solution for their employees.



		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.1	Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.		Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	SCDN: Customer must ensure that security policies and operational procedures for restricting access to the Akamai Control Center and OPEN API credentials are documented, in use, and known to all affected parties. API Security: Customers should maintain their own policies and procedures for identifying and authenticating users. Customers have the option to use SAML integration with their own identity provider or use the identity provider that is provided with the application.
8.1.1	All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.		Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	Customers should maintain their own policies and procedures for identifying and authenticating users. Customers have the option to use SAML integration with their own identity provider or use the identity provider that is provided with the application.
8.1.2	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.				Customers should maintain their own policies and procedures for identifying and authenticating users.
8.2	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.		Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.		Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	SCDN: Customer must assign all users a unique user ID before allowing them to access the Akamai Control Center. API Security: Customers are responsible for assigning unique user identifiers within their tenant.
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.		Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	SCDN: Customers are responsible for not using group, shared, or generic IDs, passwords, or other authentication methods when accessing the Akamai Control Center. API Security: Customers should have processes in place for the management of shared accounts if required.
8.2.3	Additional requirement for service providers only: Service providers with remote access to customer premises use unique authentication factors for each customer premises.	Akamai does not have remote access capabilities to customer environments.	Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.2.4	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.		Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	SCDN: Customer must control addition, deletion, and modification of Akamai Control Center user IDs, credentials, and other identifier objects. API Security: Customers are responsible for authorizing their own credentials within their tenant including the authorization of all lifecycle events identified in this requirement.
8.2.5	Access for terminated users is immediately revoked.		Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	SCDN: Customer must immediately revoke access to the Akamai Control Center for any terminated users. API Security: Customers are responsible for revoking access to its users of the application in compliance with this requirement.
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity.		Akamai is responsible to provide the capability for customers to manage user and administrative accounts for use with Akamai Services	Customers are responsible for configuration of user and administrative accounts for use with Akamai Services in accordance with PCI DSS Requirement 8.	SCDN: Customer must remove/disable inactive Akamai Control Center user accounts at least every 90 days, either manually or using the Akamai Control Center automated option. API Security: Customers are responsible for revoking access to its users of the application in compliance with this requirement.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.2.7	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.			If a customer grants a vendor access to their Akamai account, they are responsible for managing the vendor access. Akamai does not manage IDs for its resellers; customers purchasing accounts through Akamai resellers are responsible for working with the reseller to make sure that reseller access is PCI-compliant.	
8.2.8	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.				SCDN: Customer must set the Akamai Control Center configuration setting so that if a session has been idle for more than 15 minutes, the user must re-authenticate to re-activate the terminal or session. BMP/APR: BMP/APR has no public facing console. API Security: Customers utilizing SAML for authentication should ensure this configuration is in place.
8.3	Strong authentication for users and administrators is established and managed.				Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • 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 element.				Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.
8.3.2	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.				API Security: Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.
8.3.3	User identity is verified before modifying any authentication factor.				API Security: Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.
8.3.4	Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.				API Security: Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.
8.3.5	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.				Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.3.6	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters. **This requirement is a best practice until 31 March 2025.**				SCDN: Customers are responsible for setting Akamai Control Center password configurations to require a minimum length of at least seven characters and to contain both numeric and alphabetic characters. API Security: Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.
8.3.7	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.				SCDN: Customers are not allowed to submit a new password/passphrase that is the same as last 4 passwords/passphrases used. API Security: Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
8.3.8	Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.				SCDN: Customers must make sure that they have documented and have communicated authentication procedures and policies to all Akamai Control Center users including guidance on selecting strong authentication credentials, guidance for how users should protect their authentication credentials, instructions not to reuse previously used passwords and instructions to change passwords if there is any suspicion the password could be compromised. API Security: Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.
8.3.9	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.				SCDN: Customers are responsible for setting Akamai Control Center configurations so that user passwords/passphrases must be changed at least every 90 days. API Security: Customers utilizing SAML for authentication should ensure their SAML solution meets these requirements.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.3.10	Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single-factor authentication implementation), then guidance is provided to customer users including: • Guidance for customers to change their user passwords/passphrases periodically. • Guidance as to when, and under what circumstances, passwords/passphrases are to be changed.	Passwords are not the only authentication factor used.			
8.3.10.1	Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, OR • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. **This requirement is a best practice until 31 March 2025.**				Customers using two-factor authentication to access the Akamai Control Center must ensure that the second factor is always assigned to an individual account and not shared, and that controls are in place to ensure only the intended account can use the mechanism to gain access.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.3.11	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.				Customers may use a SAML identity provider to authenticate users with MFA. Customers are responsible for ensuring they do share authentication factors among multiple users.
8.4	Multi-factor authentication (MFA) is implemented to secure access into the CDE.	API Security: NA. The solution environment is not a CDE.	SCDN: This is a service provider responsibility.		
8.4.1	MFA is implemented for all non-console access into the CDE for personnel with administrative access.	API Security: The solution environment is not a CDE.	SCDN: This is a service provider responsibility.		
8.4.2	MFA is implemented for all access into the CDE. **This requirement is a best practice until 31 March 2025.**	API Security: The solution environment is not a CDE.	SCDN: This is a service provider responsibility.		
8.4.3	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.	API Security: The solution environment is not a CDE.	SCDN: This is a service provider responsibility.		
8.5	Multi-factor authentication (MFA) systems are configured to prevent misuse.	API Security: The solution environment is not a CDE.	SCDN: This is a service provider responsibility.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.5.1	MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted. **This requirement is a best practice until 31 March 2025.**	API Security: The solution environment is not a CDE.	SCDN: This is a service provider responsibility.		
8.6	Use of application and system accounts and associated authentication factors is strictly managed.				The scope of Akamai's responsibilities is limited to application and system accounts that it manages in the operstion of the product. Customers are responsible for application and system accounts that may be used in conjuction with the operation of the product such as accounts that used to integrate the solution with 3rd party products.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
8.6.1	If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user. **This requirement is a best practice until 31 March 2025.**				The scope of Akamai's responsibilities is limited to application and system accounts that it manages in the operstion of the product. Customers are responsible for application and system accounts that may be used in conjuction with the operation of the product such as accounts that used to integrate the solution with 3rd party products.
8.6.2	Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. **This requirement is a best practice until 31 March 2025.**				The scope of Akamai's responsibilities is limited to application and system accounts that it manages in the operstion of the product. Customers are responsible for application and system accounts that may be used in conjuction with the operation of the product such as accounts that used to integrate the solution with 3rd party products.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. **This requirement is a best practice until 31 March 2025.**				The scope of Akamai's responsibilities is limited to application and system accounts that it manages in the operstion of the product. Customers are responsible for application and system accounts that may be used in conjuction with the operation of the product such as accounts that used to integrate the solution with 3rd party products.
9.1	Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
9.1.1	All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.1.2	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.2	Physical access controls manage entry into facilities and systems containing cardholder data.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.2.1	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.2.1.1	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.2.2	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.2.3	Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.2.4	Access to consoles in sensitive areas is restricted via locking when not in use.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.3	Physical access for personnel and visitors is authorized and managed.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.3.1	Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.3.1.1	Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.3.2	Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.3.3	Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.3.4	A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
9.4	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.4.1	All media with cardholder data is physically secured.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.4.1.2	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.4.3	Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.4.5	Inventory logs of all electronic media with cardholder data are maintained.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.4.5.1	Inventories of electronic media with cardholder data are conducted at least once every 12 months.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
9.4.7	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.5	Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.5.1	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.5.1.1	An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.5.1.2	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
9.5.1.2.1	The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025.**	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
9.5.1.3	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	Akamai SCDN: NA. Akamai doesn't store any cardholder data, and thus control doesn't apply.	BMP/APr: This is a service provider responsibility. The BMP/APr offering uses third party storage services that have their own PCI AOC to meet this control. API Security: This is a service provider responsibility. The API security solution uses third party storage services that have their own PCI AOC to meet this control.		
10.1	Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.		Akamai has implemented processes and mechanisms for logging and monitoring all access to system components and cardholder data that are within Akamai's control.	Customers should implement processes and mechanisms for logging and monitoring all access to system components and cardholder data that are within their control.	

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.1.1	All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.		Akamai has implemented policies and operational procedures for logging and monitoring all access to system components and cardholder data that are within Akamai's control.	Customers should implement policies and operational procedures for logging and monitoring all access to system components and cardholder data that are within their control.	
10.1.2	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.		Akamai has defined roles and responsibilities for performing activities in Requirement 10 for logging and monitoring all access to system components and cardholder data that are within Akamai's control and such roles and responsibilities are documented, assigned, and understood.	Customers should define roles and responsibilities for performing activities in Requirement 10 for logging and monitoring all access to system components and cardholder data that are within their control and such roles and responsibilities are documented, assigned, and understood.	
10.2	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		Responsible		
10.2.1	Audit logs are enabled and active for all system components and cardholder data.		Responsible		
10.2.1.1	Audit logs capture all individual user access to cardholder data.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.2.1.2	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.		Responsible		
10.2.1.3	Audit logs capture all access to audit logs.		Responsible		
10.2.1.4	Audit logs capture all invalid logical access attempts.		Responsible		
10.2.1.5	Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.		Responsible		
10.2.1.6	Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.		Responsible		
10.2.1.7	Audit logs capture all creation and deletion of system-level objects.		Responsible		
10.2.2	Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).		Responsible		
10.3	Audit logs are protected from destruction and unauthorized modifications.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.3.1	Read access to audit logs files is limited to those with a job-related need.		Responsible		
10.3.2	Audit log files are protected to prevent modifications by individuals.		Responsible		
10.3.3	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.		Responsible		
10.3.4	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.		Responsible		
10.4	Audit logs are reviewed to identify anomalies or suspicious activity.			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.4.1	The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.
10.4.1.1	Automated mechanisms are used to perform audit log reviews. **This requirement is a best practice until 31 March 2025.**			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.
10.4.2.1	The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025.**			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.4.3	Exceptions and anomalies identified during the review process are addressed.			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for reviewing API Security solution detection alerts and responding appropriately.
10.5	Audit log history is retained and available for analysis.		Responsible		
10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.6	Time-synchronization mechanisms support consistent time settings across all systems.			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for ensuring on premise nodes are configured to comply with the requirements in this section. The on premise node should have it's time synchronized to an external time source as specified in the requirement.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for ensuring on premise nodes are configured to comply with the requirements in this section. The on premise node should have it's time synchronized to an external time source as specified in the requirement.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.6.1	System clocks and time are synchronized using time-synchronization technology.			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for ensuring on premise nodes are configured to comply with the requirements in this section. The on premise node should have it's time synchronized to an external time source as specified in the requirement.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for ensuring on premise nodes are configured to comply with the requirements in this section. The on premise node should have it's time synchronized to an external time source as specified in the requirement.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.6.2	Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for ensuring on premise nodes are configured to comply with the requirements in this section. The on premise node should have it's time synchronized to an external time source as specified in the requirement.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for ensuring on premise nodes are configured to comply with the requirements in this section. The on premise node should have it's time synchronized to an external time source as specified in the requirement.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.6.3	Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.			Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for ensuring on premise nodes are configured to comply with the requirements in this section. The on premise node should have it's time synchronized to an external time source as specified in the requirement.	Akamai SCDN: Customers must review Akamai Control Center logs and security events related to customer access at least daily to identify anomalies or suspicious activity. API Security: Customers are responsible for ensuring on premise nodes are configured to comply with the requirements in this section. The on premise node should have it's time synchronized to an external time source as specified in the requirement.
10.7	Failures of critical security control systems are detected, reported, and responded to promptly.				The scope of Akamai's responsibilities for this requirement is limited to Akamai products & system components that Akamai directly controls.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
10.7.1	Additional requirement for service providers only: Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • FIM. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). **This requirement will be superseded by Requirement 10.7.2 on 31 March 2025.**				The scope of Akamai's responsibilities for this requirement is limited to Akamai products & system components that Akamai directly controls.
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used). **This requirement is a best practice until 31 March 2025.**				The scope of Akamai's responsibilities for this requirement is limited to Akamai products & system components that Akamai directly controls.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
10.7.3	Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.				The scope of Akamai's responsibilities for this requirement is limited to Akamai products & system components that Akamai directly controls.
11.1	Processes and mechanisms for regularly testing security of systems and networks are defined and understood.		Responsible		
11.1.1	All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.		Responsible		
11.1.2	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.		Responsible		
11.2	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Not applicable.			

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
11.2.1	Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for, • All authorized and unauthorized wireless access points are detected and identified, • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.	Not applicable.			
11.2.2	An inventory of authorized wireless access points is maintained, including a documented business justification.	Not applicable.			
11.3	External and internal vulnerabilities are regularly identified, prioritized, and addressed.		Responsible		
11.3.1	Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
11.3.1.1	All other applicable vulnerabilities (those not ranked as high-risk or critical per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed. **This requirement is a best practice until 31 March 2025.**		Responsible		
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • Sufficient privileges are used for those systems that accept credentials for scanning. • If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2. **This requirement is a best practice until 31 March 2025.**		Responsible		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
11.3.1.3	Internal vulnerability scans are performed after any significant change as follows: • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).		Responsible		
11.3.2	External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV). • Vulnerabilities are resolved and ASV Program Guide requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the ASV Program Guide requirements for a passing scan.		Responsible		
11.3.2.1	External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).		Responsible		
11.4	External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		Responsible		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
11.4.1	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
11.4.2	Internal penetration testing is performed: • Per the entity’s defined methodology, • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).		Responsible		
11.4.3	External penetration testing is performed: • Per the entity’s defined methodology • At least once every 12 months • After any significant infrastructure or application upgrade or change • By a qualified internal resource or qualified external third party • Organizational independence of the tester exists (not required to be a QSA or ASV).		Responsible		
11.4.4	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity’s assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.		Responsible		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
11.4.5	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).		Responsible		

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
11.4.6	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every six months and after any changes to segmentation controls/methods. • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).		Responsible		
11.4.7	Additional requirement for multi-tenant service providers only: Multi-tenant service providers support their customers for external penetration testing per Requirement 11.4.3 and 11.4.4. **This requirement is a best practice until 31 March 2025.**	Not applicable.			
11.5	Network intrusions and unexpected file changes are detected and responded to.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
11.5.1	Intrusion-detection and/or intrusion prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.		Responsible		
11.5.1.1	Additional requirement for service providers only: Intrusion-detection and/or intrusion-prevention techniques detect, alert on/prevent, and address covert malware communication channels. **This requirement is a best practice until 31 March 2025.**		Responsible		
11.5.2	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.		Responsible		
11.6	Unauthorized changes on payment pages are detected and responded to.		Responsible		

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
11.6.1	A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser. • The mechanism is configured to evaluate the received HTTP header and payment page. The mechanism functions are performed as follows: – At least once every seven days OR – Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). **This requirement is a best practice until 31 March 2025.**		Responsible		
12.1	A comprehensive information security policy that governs and provides direction for protection of the entity’s information assets is known and current. 12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.				Customers must establish, publish, maintain, and disseminate a policy for securely using Akamai services. Customers are responsible for responding to incidents within their own CDE.
12.1.1	An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.				Customers must establish, publish, maintain, and disseminate a policy for securely using Akamai services.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.1.2	The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment.				Customers must review their policy for secure use of Akamai services at least annually and update the policy as the environment changes.
12.1.3	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.				Customers must define information security roles and responsibilities for their personnel.
12.1.4	Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.				Akamai and Customers must each maintain their own information security program led by a Chief Information Security Officer or other information security knowledgeable member of executive management.
12.2	Acceptable use policies for end-user technologies are defined and implemented.				Customers are responsible for developing usage policies for their use of Akamai services, directly or via critical technologies, covering at least the following responsibilities:
12.2.1	Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.				Customers are responsible for acquiring approval of their use of Akamai services by authorized parties.
12.3	Risks to the cardholder data environment are formally identified, evaluated, and managed.				Customers must implement risk-assessment processes for their own use of Akamai services.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.3.1	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review. **This requirement is a best practice until 31 March 2025.**				Customers must conduct their own targeted risk analysis in compliance with this requirement.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.3.2	A targeted risk analysis is performed for each PCI DSS requirement that the entity meets with the customized approach, to include: • Documented evidence detailing each element specified in Appendix D: Customized Approach (including, at a minimum, a controls matrix and risk analysis). • Approval of documented evidence by senior management. • Performance of the targeted analysis of risk at least once every 12 months.				Customers must conduct their own targeted risk analysis in compliance with this requirement.
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities. **This requirement is a best practice until 31 March 2025.**				Akamai is responsible for this requirement only for the system components which are under the control of Akamai.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.3.4	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans. **This requirement is a best practice until 31 March 2025.**				Akamai is responsible for this requirement only for the system components which are under the control of Akamai.
12.4	PCI DSS compliance is managed.				Management of PCI DSS Compliance relating to the product and customer's use of the product for their own PCI compliance is a shared responsibility between Akamai and the customer.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
12.4.1	Additional requirement for service providers only: Responsibility is established by executive management for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance. • Defining a charter for a PCI DSS compliance program and communication to executive management.				Customers acting as service providers must meet any requirements for executive management for their own program.
12.4.2	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance with all security policies and operational procedures. Reviews are performed by personnel other than those responsible for performing the given task and include, but are not limited to, the following tasks: • Daily log reviews. • Configuration reviews for network security controls. • Applying configuration standards to new systems. • Responding to security alerts. • Change-management processes.				Customers acting as service providers must meet any requirements to conduct reviews in compliance with this requirement.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
12.4.2.1	Additional requirement for service providers only: Reviews conducted in accordance with Requirement 12.4.2 are documented to include: • Results of the reviews. Documented remediation actions taken for any tasks that were found to not be performed at Requirement 12.4.2. • Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.				Customers acting as service providers must meet any requirements to conduct reviews in compliance with this requirement.
12.5	PCI DSS scope is documented and validated.				Customers must document and validate their own PCI scope.
12.5.1	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.				Customers must maintain an inventory of system components that are in scope for PCI.

12.5.2	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce). • Updating all data-flow diagrams per Requirement 1.2.4. • Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups. • Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE. • Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope. • Identifying all connections from third-party entities with access to the CDE. • Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.				Customers must revalidate PCI scope once every 12 months.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.5.2.1	Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2. **This requirement is a best practice until 31 March 2025.**				Customers who are also service providers must meet this requirement for their environment.
12.5.3	Additional requirement for service providers only: Significant changes to organizational structure result in a documented (internal) review of the impact to PCI DSS scope and applicability of controls, with results communicated to executive management. **This requirement is a best practice until 31 March 2025.**				Customers who are also service providers must meet this requirement for their environment.
12.6	Security awareness education is an ongoing activity.				Customer is responsible for implementing a formal security awareness program to make all personnel with access to the API security product aware of the importance of cardholder data security and how their use of Akamai services can impact security.
12.6.1	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.				Customer is responsible for implementing a formal security awareness program to make all personnel with access to the API security product aware of the importance of cardholder data security and how their use of Akamai services can impact security.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.6.2	The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data. **This requirement is a best practice until 31 March 2025.**				Customer is responsible for implementing a formal security awareness program to make all personnel with access to the API security product aware of the importance of cardholder data security and how their use of Akamai services can impact security.
12.6.3	Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.				Customer is responsible for implementing a formal security awareness program to make all personnel with access to the API security product aware of the importance of cardholder data security and how their use of Akamai services can impact security.
12.6.3.1	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering. This requirement is a best practice until 31 March 2025.				Customer is responsible for implementing a formal security awareness program to make all personnel with access to the API security product aware of the importance of cardholder data security and how their use of Akamai services can impact security.
12.6.3.2	Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1. **This requirement is a best practice until 31 March 2025.**				Customer is responsible for implementing a formal security awareness program to make all personnel with access to the API security product aware of the importance of cardholder data security and how their use of Akamai services can impact security.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.7	Personnel are screened to reduce risks from insider threats.				Customer must screen potential personnel with access to the API Security product prior to hire to minimize the risk of attacks from internal sources.
12.7.1	Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.				Customer must screen potential personnel with access to the API Security product prior to hire to minimize the risk of attacks from internal sources.
12.8	Risk to information assets associated with third-party service provider (TPSP) relationships is managed.			Customers are responsible to 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:	Customers are responsible to 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:
12.8.1	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.			Customers must maintain a list of service providers in compliance with this requirement.	Customers must maintain a list of service providers in compliance with this requirement.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
12.8.2	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scopereduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.			Customers must 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.	Customers must 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.
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.			Customers must ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	Customers must ensure there is an established process for engaging service providers including proper due diligence prior to engagement.

		Responsibility			
Requirement	Requirement Text	Not Applicable	Akamai	Customer	Joint
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.			Customers must maintain a program to monitor service providers' PCI DSS compliance status at least annually.	Customers must maintain a program to monitor service providers' PCI DSS compliance status at least annually.
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.				Customers must maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. Akamai publishes the responsibility matrix for customers to use about the services provides by Akamai.
12.9	Third-party service providers (TPSPs) support their customers' PCI DSS compliance.				Akamai acknowledges in writing to customers that Akamai is responsible for the security of cardholder data Akamai transmits on behalf of the customer, as long as the customer meets the customer responsibilities described in this matrix.
12.9.1	Additional requirement for service providers only: TPSPs acknowledge in writing to customers that they are responsible for the security of account data the TPSP 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 CDE.		Responsible		Akamai acknowledges in writing to customers that Akamai is responsible for the security of cardholder data Akamai transmits on behalf of the customer, as long as the customer meets the customer responsibilities described in this matrix.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.9.2	Additional requirement for service providers only: TPSPs support their customers' requests for information to meet Requirements 12.8.4 and 12.8.5 by providing the following upon customer request: • PCI DSS compliance status information for any service the TPSP performs on behalf of customers (Requirement 12.8.4). • Information about which PCI DSS requirements are the responsibility of the TPSP and which are the responsibility of the customer, including any shared responsibilities (Requirement 12.8.5).		Responsible		Akamai supports customer requests for information in compliance with this requirement.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • 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.				Customers must implement an incident response plan and be prepared to respond immediately to a system breach which may relate to the customer's use of Akamai services.
12.10.2	At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.				Customers are required to review their own incident response plans in compliance with this requirement. Customers are also required to test their incident response plans, including their response to an incident related to their use of Akamai services, annually.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.10.3	Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.				Customer must designate specific personnel to be available on a 24/7 basis in response to incidents related to the customer's use of Akamai PCI services, and maintain up-to-date contact information for at least those personnel on the Akamai Control Center.
12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.				Customer must designate specific personnel to be available on a 24/7 basis in response to incidents related to the customer's use of Akamai PCI services, and maintain up-to-date contact information for at least those personnel on the Akamai Control Center.
12.10.4.1	The frequency of periodic training for incident response personnel is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. **This requirement is a best practice until 31 March 2025.**				Customer must provide appropriate training to staff with security breach response responsibilities.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.10.5	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. This bullet is a best practice until its effective date. • Detection of unauthorized wireless access points. **This requirement is a best practice until 31 March 2025.**				Customers must include monitoring and responding to alerts in their incident response program in compliance with this requirement.
12.10.6	The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.				Customer must have a process to modify and evolve their incident response plan for incidents involving Akamai services according to lessons learned and industry developments.

		Responsibility			
Requirement	**Requirement Text**	**Not Applicable**	**Akamai**	**Customer**	**Joint**
12.10.7	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected. **This requirement is a best practice until 31 March 2025.**				Customer is responsible to respond to incidents involving the detection of PAN anywhere it is not expected in compliance with this requirement.