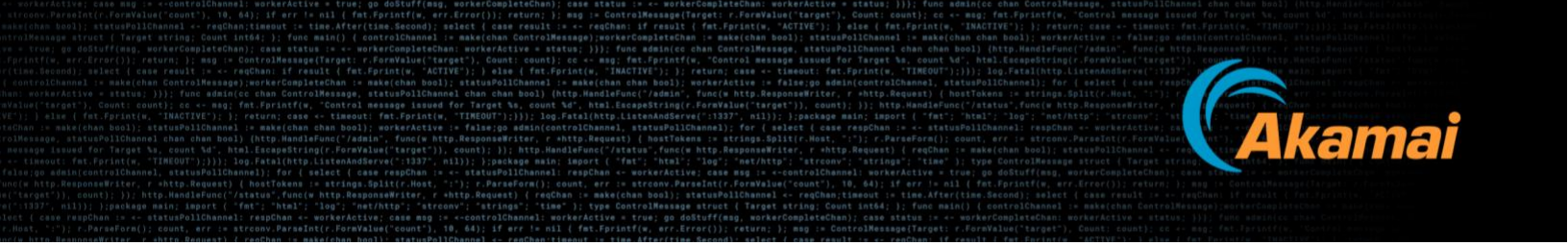


Responsibility Matrix
PCI DSS 4.0

Akamai Cloud Computing Services

June 2024

Executive Summary

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

The following document describes the PCI compliance responsibilities for Akamai and customers that use its cloud computing services. This document is intended to be used by Akamai customers and their compliance advisors to understand the scope of responsibility when using Akamai's cloud computing services as part of the customer's cardholder data environment. Customers and assessors should be familiar with Akamai security best practices and recommendations. As with any infrastructure, customers are responsible for using vendor provided security recommendations, features, and access controls.

Business Description

Akamai's cloud computing services accelerates innovation with scalable, simple, affordable, and accessible Linux cloud solutions and services. Our products, services, and people give developers and enterprises the flexibility, support, and trust they need to build, deploy, secure, and scale applications more easily and cost-effectively from cloud to edge on the world's most distributed network. Just as it did when pioneering cloud computing in 2003, we continue to play a significant role in the technological advancement of cloud computing.

Description of In-Scope Services

Below are descriptions of each service as described by Akamai and derived from its website at Public Cloud Products & Solutions (IaaS) | Akamai. The services within this list have been approved for customers to create their own cardholder data environment.

Compute

Shared CPU Instances

Shared CPU Compute Instances are our most affordable virtual machines that offer a significant price-to-performance ratio. They provide a well-balanced set of resources that are ideal for a wide range of applications. While most of our other Compute Instance types are equipped with dedicated CPUs, Shared Instances are not. This means that CPU resources are shared with other Compute Instances and a small amount of resource contention is possible.

Shared CPU Compute Instances are suitable for general workloads that value cost over maximum performance:

- Production applications with low to medium CPU requirements and are not affected by resource contention
- Applications that require a balanced set of resources
- Medium to low traffic websites, such as for marketing content and blogs
- Forums
- Development and staging servers
- Low traffic databases
- Worker nodes within a container orchestration cluster

In addition to the resources allocated to each available plan, Shared CPU Compute Instances have the following specifications:

- Shared vCPU cores
- 100% SSD (Solid State Disk) storage
- Free inbound network transfer
- Dedicated IPv4 and IPv6 addresses (additional addresses available on request)
- Deploy using the many available Linux Distributions, Marketplace Apps, or Community StackScripts
- Direct console access through Lish
- Provisioning and management through the Cloud Manager, or programmatically through the Linode API
- Multi-queue NIC support on plans with 2 or more vCPU cores.

More information about Shared CPU instances can be found at Shared CPU Compute Instances | Linode Docs.

Dedicated CPU Instances

Dedicated CPU Compute Instances are virtual machines that provide you with dedicated CPU resources. Their vCPU cores are guaranteed (and, thus, competition-free) so there are no surprises or CPU-related performance degradation. This enables you to run your production applications with confidence that your performance won't be impacted by others. These Compute Instances are CPU-optimized and can sustain CPU resource usage at 100% for as long as your workloads need. Dedicated CPU plans are ideal for nearly all production applications and CPU-intensive workloads, including high traffic websites, video encoding, machine learning, and data processing.

Dedicated CPU Compute Instances are suitable for almost any workload that requires consistently high-performance CPU resources. This includes:

- Production websites and e-commerce sites

- Applications that required 100% sustained CPU usage.
- Applications that might be impacted by resource contention.
- CI/CD toolchains and build servers
- Game servers (like Minecraft or Team Fortress)
- Audio and video transcoding
- Big data (and data analysis)
- Scientific computing
- Machine learning and AI
- High Traffic Databases (Galera, PostgreSQL with Replication Manager, MongoDB using Replication Sets)
- Replicated or Distributed File Systems (GlusterFS, DRBD)

In addition to the resources allocated to each available plan, Dedicated CPU Compute Instances have the following specifications:

- Dedicated vCPU cores
- 100% SSD (Solid State Disk) storage
- Free inbound network transfer
- Dedicated IPv4 and IPv6 addresses (additional addresses available on request)
- Deploy using the many available Linux Distributions, Marketplace Apps, or Community StackScripts
- Direct console access through Lish
- Provisioning and management through the Cloud Manager, CLI, or programmatically through the Linode API
- Multi-queue NIC support

More information about Dedicated CPU instances can be found at Dedicated CPU Compute Instances | Linode Docs.

High Memory

High Memory Compute Instances are virtual machines that offer a greater price-to-performance ratio for memory-intensive applications. When compared to Dedicated CPU Instances, High Memory Instances provide the same dedicated CPU resources but are equipped with more memory per CPU core. This tunes them specifically for memory-intensive applications that value larger amounts of memory over a larger number of CPU cores. High Memory plans are ideal for production applications and CPU-intensive workloads that value greater memory over CPU resources, including caching systems, high-performance databases, and in-memory data processing.

High Memory Compute Instances are suitable for workloads that value much larger amounts of memory than other plans of a similar price. This includes:

- Any production application that requires large amounts of memory

- In-memory database caching systems, such as Redis and Memcached
- In-memory databases, such as possible with NoSQL and other solutions
- Big data processing (and data analysis)

In addition to the resources allocated to each available plan, High Memory Compute Instances have the following specifications:

- Dedicated vCPU cores
- 100% SSD (Solid State Disk) storage
- Free inbound network transfer
- Dedicated IPv4 and IPv6 addresses (additional addresses available on request)
- Deploy using the many available Linux Distributions, Marketplace Apps, or Community StackScripts
- Direct console access through Lish
- Provisioning and management through the Cloud Manager, or programmatically through the Linode API
- Multi-queue NIC support

More information about High Memory instances can be found at High Memory Compute Instances | Linode Docs.

Cloud Manager

Cloud Manager is a user and mobile-friendly interface to deploy and manage virtual machines, configure networking, control user accounts, and access and configure the full range of Akamai cloud computing services. Cloud Manager supports you with self-serve migrations so you can conveniently move your infrastructure between data centers. Effortlessly create and configure your infrastructure with Cloud Manager. Assign SSH keys, deploy resources across the network, and add cloud storage volumes or buckets all from a single UI. Leverage Advanced Search to quickly find your cloud resources. Search using simple strings, Boolean operators, parenthesis, or custom groups with tags you create in Cloud Manager. Manage your account, update payment information, review credits remaining, and print invoices. Share access to your VMs with your team by adding multiple users and configure controls for each individual user. Manage your API Keys and add personal access tokens for more control over your cloud services.

More information about Cloud Manager can be found at Linode Cloud Manager Product Documentation.

Linode API

The Linode API provides the ability to programmatically manage the full range of Akamai's cloud computing services. Easily configure, manage, and deploy user management, billing, support tickets, and more with programmatic access to Akamai cloud computing services.

The full API documentation can be found at Linode API.

Service Architecture and Customer Considerations

There are several considerations for customers when implementing a cardholder environment. The information below provides some considerations and should be read in combination with the detailed control guidance provided later in this document.

Management Environment

The Management Environment consists of the following elements:

Hypervisor

Akamai currently utilizes a combination of the QEMU hardware emulator and the KVM hypervisor, taking advantage of paravirtualization (the default for guests). Because para-virtualized guests rely on the hypervisor to provide support for operations that normally require privileged access, the guest OS has no elevated access to the CPU.

Instance Isolation

Different instances running on the same physical machine are isolated from each other via the QEMU hypervisor. In addition, the QEMU process is restricted to a directory to which it has no write permissions.

API

The Linode API provides programmatic access to the Akamai cloud computing platform, allowing you to automate tasks through a fully documented REST API. Tasks include things such as calls to launch and terminate instances, adjust networking, change firewall parameters, and change account parameters. The full capability of the API can be found in our API Documentation. Access is controlled through a Personal Access Token. This token should only allow the level of access needed by the application. In addition, API calls can be encrypted with TLS to maintain confidentiality. Akamai recommends always using TLS-protected API endpoints.

Cloud Manager

The Cloud Manager application facilitates management for all aspects of an Akamai cloud computing account, including managing assets, monitoring monthly spending by service or managing security credentials. Cloud Manager requires user login credentials which are designated at the time of account creation, or added later on. Multi-Factor Authentication (MFA) can be configured to meet the requirement for MFA authentication for remote access. More information on managing users can be found at https://www.linode.com/docs/products/platform/accounts/guides/manage-users/.

More information on User Permissions can be found at https://www.linode.com/docs/products/platform/accounts/guides/user-permissions/.

Information on MFA configuration can be found here: https://www.linode.com/docs/products/platform/accounts/guides/2fa/.

Host Operating System

The host OS provides a platform for the Guest OS to run. These systems are specifically designed, built, configured, and hardened to protect the management plane. All such accesses are protected, logged, audited, and monitored. Customers are not permitted any access to the Host Operating System.

Data Isolation

Akamai maintains multiple controls to maintain and monitor isolation of customer data from any unauthorized user. In addition, controls are in place to ensure that deleted data and data remnants are also secured from unauthorized users. Physical storage devices are decommissioned using a controlled process that prevents customer data from being exposed to unauthorized individuals.

Customer Implementation Considerations

As customers leverage Akamai's cloud computing services to implement a compliant cardholder environment, the following section provides additional information to consider:

Firewall

Akamai provides solutions and guides for protecting your assets. Cloud Firewall is a robust cloud-based firewall solution available at no additional charge for our customers. More information about Cloud Firewalls can be found at Cloud Firewall Product Documentation | Linode Docs.

Akamai also provides extensive documentation on configuring Firewalls using open source solutions such as iptables, firewalld, nftables, and UFW. Customers have control of the firewall

rules; therefore, they are also responsible for creating the logical network segmentation, including DMZ's, where appropriate to meet PCI requirements.

Orchestration

Orchestration for a cloud service provider is the automated processes in place to deploy, configure, manage, retire, and migrate systems. This includes automated set up of management networks, IP Addresses, VLANs, and any other virtual machine, hypervisor, or physical device (switches, firewalls) configurations. Akamai manages and monitors the orchestration processes.

Guest Operating System

Virtual instances are controlled by the customer. Customers have full administrative access and control over accounts, services, and applications on these guest operating systems.

Introspection

Introspection introduces a set of APIs which expand the functionality of the hypervisor to allow a deeper analysis of the data being processed by the VM. Introspection functionality typically includes visibility into stored data files, as well as monitoring of network traffic, memory and program execution, and other elements of the VM. Akamai does not utilize any introspection utilities for monitoring customer virtual machines or guest operating systems.

Choosing an Operating System

While Akamai does provide images that can be used for deployment of host operating systems, customers need to develop and implement system configuration and hardening standards to align with all applicable PCI DSS requirements for operating systems. Customers own and manage their own instance operating system and the images provided are not intended to represent a PCI compliant platform.

Datacenter

Deploying your Compute instances to a geographically advantageous data center can make a big difference in connection speeds to your server. Ideally, your site or application should be served from multiple points around the world, with requests sent to the appropriate region based on client geolocation. On a smaller scale, deploying a virtual machine in the data center nearest to you will make it easier to work with than one in a different region or continent. There are many things that can affect network congestion, connection speeds, and throughput, so you should never interpret one reading as the sole data point. Always perform tests in multiples of three or five for an average, and on both weekends and weekdays for the most accurate information. For specific compliance certification requirements per datacenter, please refer to our security page.

Authorization and Authentication

There are several methods for handling authentication and authorization through Cloud Manager and the Linode API. Cloud Manager requires user login credentials which are designated at the time of account creation, or added later on. Multi-Factor Authentication (MFA) can be configured to meet the requirement for MFA authentication for remote access. Access permissions for these accounts can be configured by an administrator of the account. Along with the standard username authentication method, a user can login to Cloud Manager through Single Sign On using Google or GitHub. The Linode API provides the ability to authenticate through a personal access token or an OAuth 2.0 workflow. More information can be found at Linode API. Authorization for Personal Access Tokens can be controlled through the steps listed at Manage Personal Access Tokens | Linode Docs.

Storage

Akamai provides individual disks for PCI workloads. Customers should consider the technology and accessibility of the data to the Internet to meet PCI requirements for restricting direct inbound and outbound access to the systems that contain cardholder data.

Encryption

Customers retain the responsibility for transport and storage encryption of cardholder data for their environment.

Backup of Data

Backups is a managed service that automatically backs up your disks at regular intervals. **Use of Backups is not in scope for PCI DSS**. Any other backup options that customers may implement are at their sole discretion to configure and manage outside of the cloud computing services offered and validated. Akamai does not backup customer data to removable media.

Breach Notification Requirements

Akamai is a Shared Services Provider. As such, in the case of a breach of security, Akamai will, where applicable, cooperate with merchants as required by PCI DSS. Protection against attack vectors defined by Visa ("What to Do If Compromised," Feb 2010) in most scenarios is the responsibility of the customer. Akamai will assist with forensic investigations as required by law.

Forensics Investigations

Akamai will cooperate with forensic investigations as required by law. Akamai is classified as a shared hosting provider and has written policies that provide for a timely forensics investigation of related servers in the event of a compromise. Akamai will work with merchants or service providers and designated Qualified Incident Response Assessors (QIRA) or PCI Forensic Investigator (PFI) as required for forensic investigations.

Secondary Shared Hosting Providers

Akamai provides services as a Shared Hosting Provider. that host a PCI related service that is also classified as a “shared hosting provider” by PCI definition are referred to as a Secondary Shared Hosting Provider in this document. Applicable requirements such as 2.6 and Appendix A1 for both Akamai and Customer Responsibilities should be reviewed to understand the shared responsibilities.

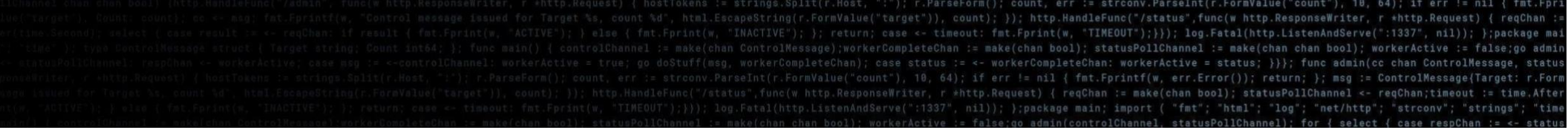
Load Balancing

It is recommended that customers maintain their own load balancing solution for ingress and egress. Nodebalancers are not in scope for PCI compliant workloads. To deploy an HAProxy instance for load balancing, please refer to the guide at How to Use HAProxy for Load Balancing | Linode Docs.

Out of Scope Services

The following cloud computing services are out of scope for PCI compliant workloads on Akamai Connected Cloud:

- Backups
- Block Storage
- Object Storage
- Databases
- Cloud Firewall
- Images
- Linode Kubernetes Engine
- Longview
- Marketplace Applications
- Nodebalancers



Responsibility Matrix

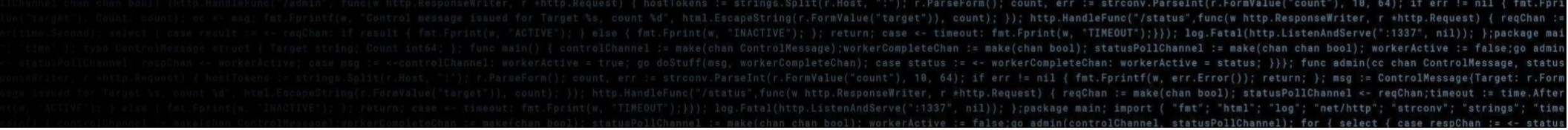
The section that follows provides more details related to demonstrating compliance for each of the 12 PCI DSS requirements.

Compute and compute customers operate in a shared responsibility model.

Compute controls the physical hosts up to the hypervisor and offers a high-level of physical and environmental security controls for our compute offerings.

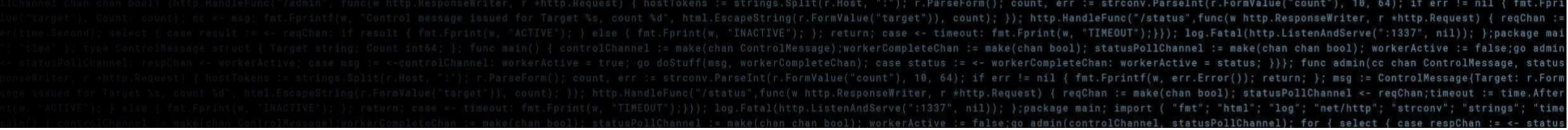
Customers are responsible for making sure installed applications and code are securely configured and patched.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
1.1	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Akamai is responsible for ensuring that documentation is kept for infrastructure up to the point of a customer instance that meets the requirements of Section 1 of the PCI DSS.	Akamai customers are responsible for ensuring that documentation is kept for any customer instances deployed on Akamai that meet the requirements of Section 1 of the PCI DSS.	Shared responsibility.
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.	Akamai is responsible for ensuring that documentation is kept for infrastructure up to the point of a customer instance that meets the requirements of Section 1 of the PCI DSS.	All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	Shared responsibility.

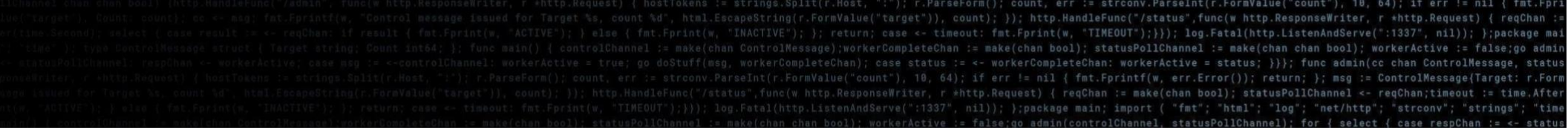


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
1.1.2	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	Akamai is responsible for ensuring that documentation is kept for infrastructure up to the point of a customer instance that meets the requirements of Section 1 of the PCI DSS.	All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	Shared responsibility.
1.2	Network security controls (NSCs) are configured and maintained.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	
1.2.1	Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	

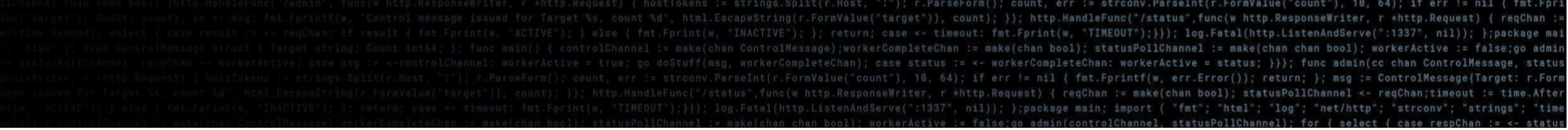
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
1.2.2	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	
1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.			Shared responsibility.
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.			Shared responsibility.
1.2.5	All services, protocols, and ports allowed are identified, approved, and have a defined business need.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	
1.2.7	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	
1.2.8	Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	

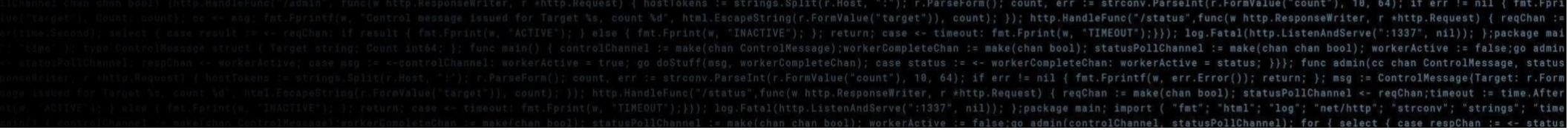


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
1.3	Network access to and from the cardholder data environment is restricted.	Akamai is responsible for network access controls with respect to its infrastructure	Customer are responsible for maintaining network access controls within their respective cardholder data environments.	Shared responsibility.
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 is responsible for network access controls with respect to its infrastructure	Customer are responsible for maintaining network access controls within their respective cardholder data environments.	Shared responsibility.
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 is responsible for network access controls with respect to its infrastructure	Customer are responsible for maintaining network access controls within their respective cardholder data environments.	Shared responsibility.
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 is responsible for network access controls with respect to its infrastructure	Customer are responsible for maintaining network access controls within their respective cardholder data environments.	Shared responsibility.
1.4	Network connections between trusted and untrusted networks are controlled.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	

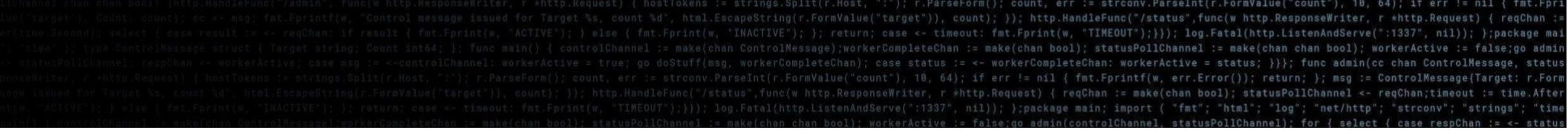


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
1.4.1	NSCs are implemented between trusted and untrusted networks.		Akamai is not responsible for meeting this requirement for customer workloads.	
1.4.2	Inbound traffic from untrusted 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.		Akamai is not responsible for meeting this requirement for customer workloads.	
1.4.3	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	
1.4.4	System components that store cardholder data are not directly accessible from untrusted networks.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	

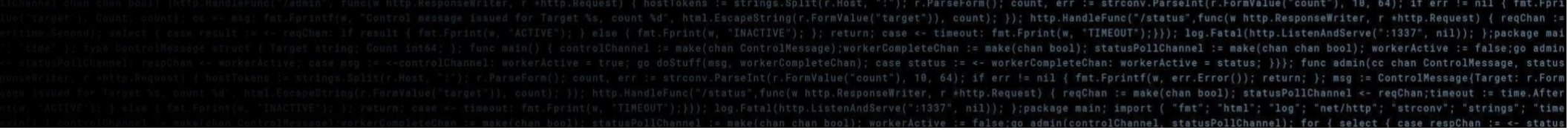
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	
1.5	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.		All In Scope Services: Akamai customers are responsible for implementing the processes and procedures necessary to ensure that all network connections, inbound and outbound traffic on any customer instances deployed on Akamai comply with the requirements of section 1 of the PCI DSS.	



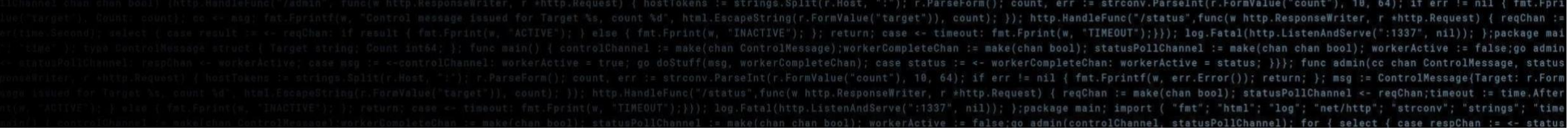
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and 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.		Akamai customers are responsible for ensuring that devices or systems owned by the customer that fall within the scope of this requirement are compliant.	Shared responsibility.
2.1	Processes and mechanisms for applying secure configurations to all system components are defined and understood.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	
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.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	
2.1.2	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	



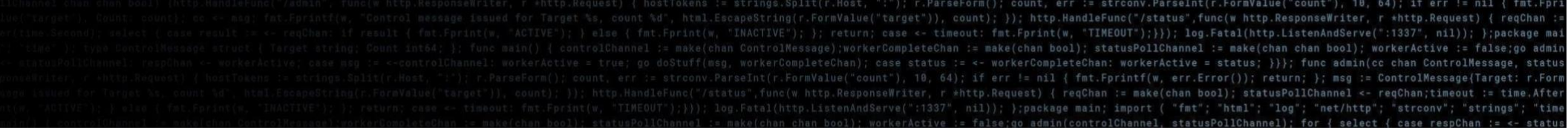
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
2.2	System components are configured and managed securely.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	
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.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	
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.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	
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.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	
2.2.6	System security parameters are configured to prevent misuse.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	

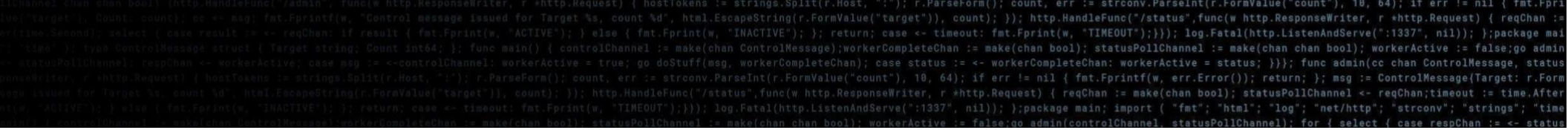


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
2.2.7	All non-console administrative access is encrypted using strong cryptography.		Akamai customers are responsible for complying with this requirement for any virtual machines, applications, services or databases deployed by them on Akamai.	
2.3	Wireless environments are configured and managed securely.		Akamai excludes wireless subsystems from the CDE by design.	
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.	



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
3.1	Processes and mechanisms for protecting stored account data are defined and understood.	Akamai is responsible for ensuring that documentation is kept for infrastructure up to the point of a customer instance that meets the requirements of Section 3 of the PCI DSS.	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
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.	Akamai is responsible for ensuring that documentation is kept for infrastructure up to the point of a customer instance that meets the requirements of Section 3 of the PCI DSS.	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
3.1.2	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	Akamai is responsible for ensuring that documentation is kept for infrastructure up to the point of a customer instance that meets the requirements of Section 3 of the PCI DSS.	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
3.2	Storage of account data is kept to a minimum.	Akamai is responsible for network access controls with respect to its infrastructure	Customers are responsible for maintaining network access controls within their respective cardholder data environments.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	Akamai is responsible for network access controls with respect to its infrastructure	Customers are responsible for maintaining network access controls within their respective cardholder data environments.	Shared responsibility.
3.3	Sensitive authentication data (SAD) is not stored after authorization.	Akamai is responsible for the security of SAD in its systems and applications.	Customers are responsible for the security of SAD in their applications and systems using the services.	Shared responsibility.
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.	Akamai is responsible for the security of SAD in its systems and applications.	Customers are responsible for the security of SAD in their applications and systems using the services.	Shared responsibility.

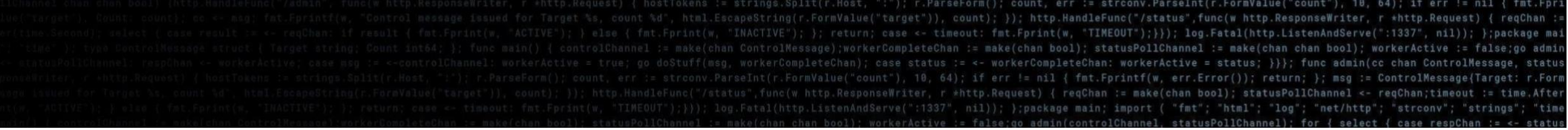


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
3.3.1.1	The full contents of any track are not retained upon completion of the authorization process.	Akamai is responsible for the security of SAD in its systems and applications.	Customers are responsible for the security of SAD in their applications and systems using the services.	Shared responsibility.
3.3.1.2	The card verification code is not retained upon completion of the authorization process.	Akamai is responsible for the security of SAD in its systems and applications.	Customers are responsible for the security of SAD in their applications and systems using the services.	Shared responsibility.
3.3.1.3	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	Akamai is responsible for the security of SAD in its systems and applications.	Customers are responsible for the security of SAD in their applications and systems using the services.	Shared responsibility.
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.**		Customers are responsible for the security of SAD in their applications and systems using the services.	
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.**	Akamai is responsible for the security of SAD in its systems and applications.	Customers are responsible for the security of SAD in their applications and systems using the services.	Shared responsibility.
3.4	Access to displays of full PAN and ability to copy PAN is restricted.		Customers are responsible for restricting access to displays of PAN in their systems and applications	Shared responsibility.
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.	Akamai is responsible for restricting access to displays of PAN in its systems and applications.	Customers are responsible for restricting access to displays of PAN in their systems and applications	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**	Akamai is responsible for restricting access to displays of PAN in its systems and applications.	Customers are responsible for restricting access to displays of PAN in their systems and applications	Shared responsibility.
3.5	Primary account number (PAN) is secured wherever it is stored.		Customers are responsible for securing PANs in their applications	
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.		Customers are responsible for securing PANs in their applications	
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.		Customers are responsible for securing PANs in their applications	

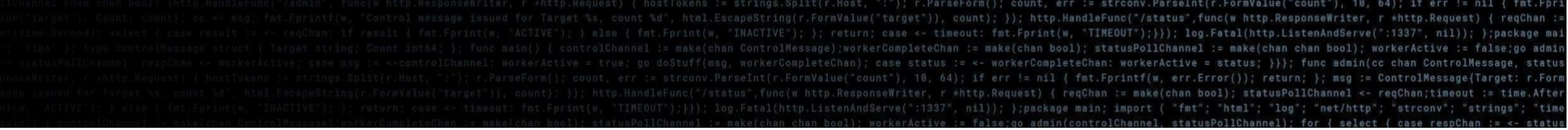
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
3.5.1.2	If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • 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 is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
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 is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
3.6	Cryptographic keys used to protect stored account data are secured.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.

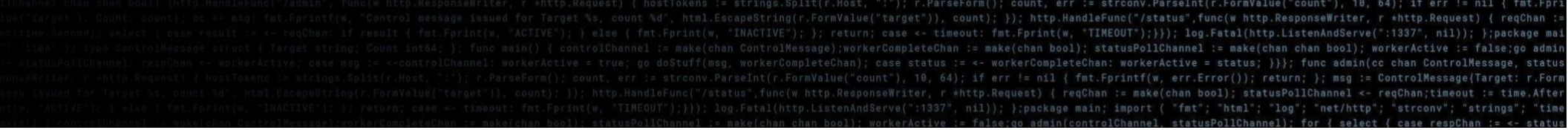


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
3.6.1.2	Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key 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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
3.6.1.3	Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
3.6.1.4	Cryptographic keys are stored in the fewest possible locations.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
3.7.1	Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
3.7.2	Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.



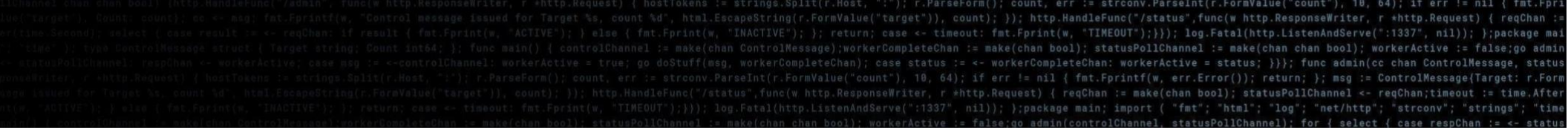
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
3.7.3	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.

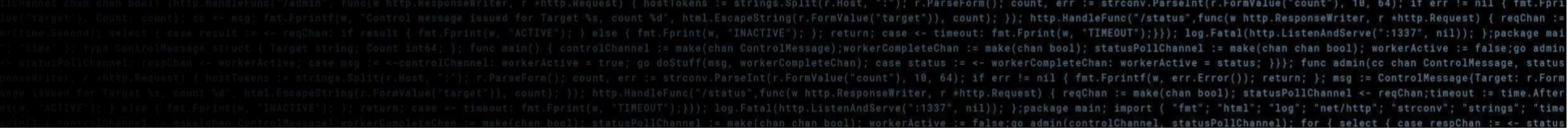
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
3.7.7	Key management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.
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.	*Akamai is not responsible for meeting this requirement for customer workloads.*	All In Scope Services: Akamai Customers are responsible for maintaining their own data storage, retention and disposal policies and procedures in accordance with PCI DSS. They are also responsible for ensuring data is stored securely in accordance with appropriate standards.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
4.1	Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.	Akamai is responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks on dedicated internal Akamai production and management network systems.	All In Scope Services: Akamai customers are responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks into their Akamai virtual instances. Customers are also responsible for any transmission of CHD over public networks that they initiate in their own software within the Akamai Platform.	Shared responsibility.
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.	Akamai is responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks on dedicated internal Akamai production and management network systems.	All In Scope Services: Akamai customers are responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks into their Akamai virtual instances. Customers are also responsible for any transmission of CHD over public networks that they initiate in their own software within the Akamai Platform.	Shared responsibility.

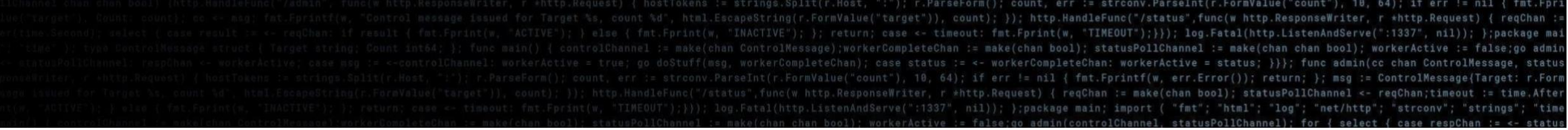


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
4.1.2	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	Akamai is responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks on dedicated internal Akamai production and management network systems.	All In Scope Services: Akamai customers are responsible for ensuring that appropriate security protocols, in compliance with section 4, are implemented for all transmissions of cardholder data over public networks into their Akamai virtual instances. Customers are also responsible for any transmission of CHD over public networks that they initiate in their own software within the Akamai Platform.	Shared responsibility.
4.2	PAN is protected with strong cryptography during transmission.		Customers are responsible for securing PANs in their applications	
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.		Customers are responsible for securing PANs in their applications	

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**		Customers are responsible for securing PANs in their applications	
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 is not responsible for meeting this requirement for customer workloads.*		
4.2.2	PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.		Customers are responsible for securing PANs in their applications	
5.1	Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.	Akamai is responsible for the implementation of malware protection in the underlying Akamai infrastructure in compliance with section 5 requirements. Akamai is NOT responsible for the implementation of malware protection within any customer deployed instances on Akamai.	Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	Shared responsibility.
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.	Akamai is responsible for the implementation of malware protection in the underlying Akamai infrastructure in compliance with section 5 requirements. Akamai is NOT responsible for the implementation of malware protection within any customer deployed instances on Akamai.	Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
5.1.2	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood.	Akamai is responsible for the implementation of malware protection in the underlying Akamai infrastructure in compliance with section 5 requirements. Akamai is NOT responsible for the implementation of malware protection within any customer deployed instances on Akamai.	Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	Shared responsibility.
5.2	Malicious software (malware) is prevented, or detected and addressed.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
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.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
5.2.2	The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	

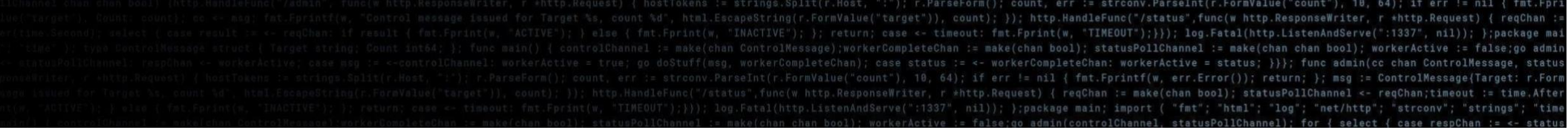


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
5.2.3	Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
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.**		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
5.3	Anti-malware mechanisms and processes are active, maintained, and monitored.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
5.3.1	The anti-malware solution(s) is kept current via automatic updates.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	

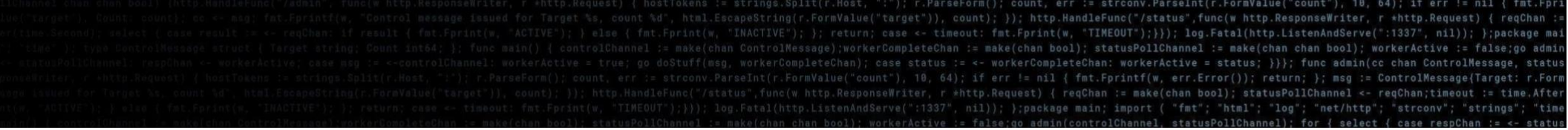
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
5.3.2	The anti-malware solution(s): • Performs periodic scans and active or real-time scans. OR • Performs continuous behavioral analysis of systems or processes.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
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.**		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
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.**		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.		Akamai customers are responsible for implementing malware protection on any customer deployed instances within Akamai in compliance with section 5 requirements.	
5.4	Anti-phishing mechanisms protect users against phishing attacks.	Akamai is responsible for implementing anti-phishing mechanisms for its staff.	Customers are responsible for implementing anti-phishing mechanisms for their staff	Shared responsibility.
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.**	Akamai is responsible for implementing anti-phishing mechanisms for its staff.	Customers are responsible for implementing anti-phishing mechanisms for their staff	Shared responsibility.
6.1	Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.	Akamai is responsible for protecting the systems and infrastructure underlying Akamai from vulnerabilities in compliance with the requirements in section 6.	Akamai customers are responsible for protecting customer deployed instances and software on Akamai from vulnerabilities in compliance with section 6 requirements.	Shared responsibility.
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.	Akamai is responsible for protecting the systems and infrastructure underlying Akamai from vulnerabilities in compliance with the requirements in section 6.	Akamai customers are responsible for protecting customer deployed instances and software on Akamai from vulnerabilities in compliance with section 6 requirements.	Shared responsibility.

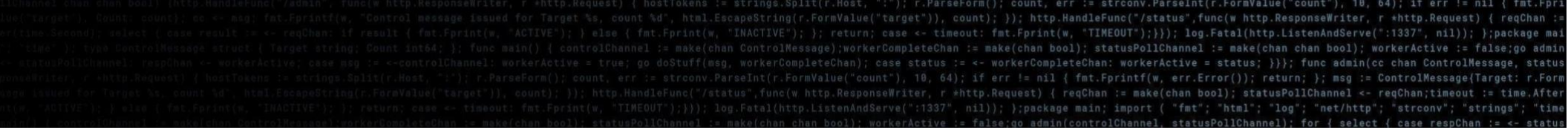
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
6.1.2	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	Akamai is responsible for protecting the systems and infrastructure underlying Akamai from vulnerabilities in compliance with the requirements in section 6.	Akamai customers are responsible for protecting customer deployed instances and software on Akamai from vulnerabilities in compliance with section 6 requirements.	Shared responsibility.
6.2	Bespoke and custom software are developed securely.	Akamai is responsible for secure software development for the software it develops	Customers are responsible for secure software development for software they develop.	Shared responsibility.
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 is responsible for secure software development for the software it develops	Customers are responsible for secure software development for software they develop.	Shared responsibility.
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.	Akamai is responsible for secure software development for the software it develops	Customers are responsible for secure software development for software they develop.	Shared responsibility.



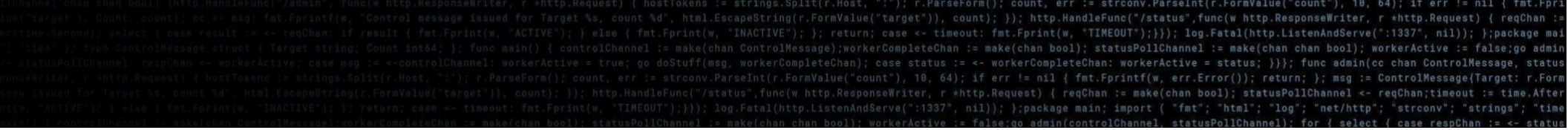
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
6.2.3	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code 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 is responsible for secure software development for the software it develops	Customers are responsible for secure software development for software they develop.	Shared responsibility.
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.	Akamai is responsible for secure software development for the software it develops	Customers are responsible for secure software development for software they develop.	Shared responsibility.



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 A PIs, 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 vulnerability identification process, as defined in Requirement 6.3.1.	Akamai is responsible for secure software development for the software it develops	Customers are responsible for secure software development for software they develop.	Shared responsibility.

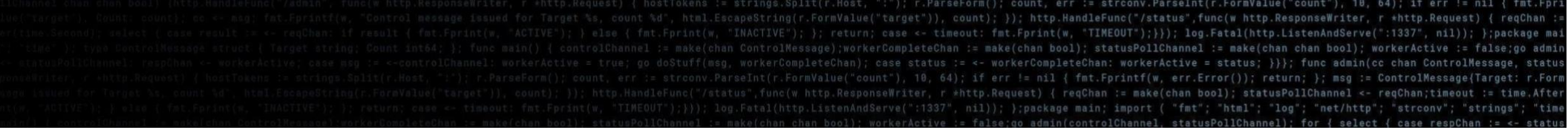


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
6.3	Security vulnerabilities are identified and addressed.	Akamai is responsible for vulnerability management with respect to systems and applications it controls	Customers are responsible for vulnerability management with respect to systems and applications they control.	Shared 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.	Akamai is responsible for vulnerability management with respect to systems and applications it controls	Customers are responsible for vulnerability management with respect to systems and applications they control.	Shared 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.**	Akamai is responsible for vulnerability management with respect to systems and applications it controls	Customers are responsible for vulnerability management with respect to systems and applications they control.	Shared responsibility.

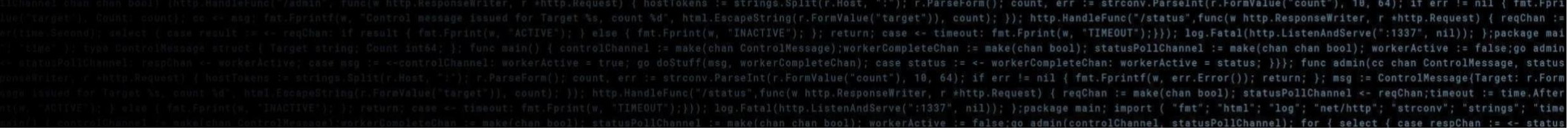


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified 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).	Akamai is responsible for vulnerability management with respect to systems and applications it controls	Customers are responsible for vulnerability management with respect to systems and applications they control.	Shared responsibility.
6.4	Public-facing web applications are protected against attacks.	Akamai is responsible for protecting public-facing web applications it controls.	Customers are responsible for protecting public-facing web applications they control	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**	Akamai is responsible for protecting public-facing web applications it controls.	Customers are responsible for protecting public-facing web applications they control	Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**	Akamai is responsible for protecting public-facing web applications it controls.	Customers are responsible for protecting public-facing web applications they control	Shared 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.**	Akamai is responsible for protecting public-facing web applications it controls.	Customers are responsible for protecting public-facing web applications they control	Shared responsibility.
6.5	Changes to all system components are managed securely.	Akamai is responsible for securely managing changes to system components it controls	Customers are responsible for security managing changes to system components they control	Shared responsibility.

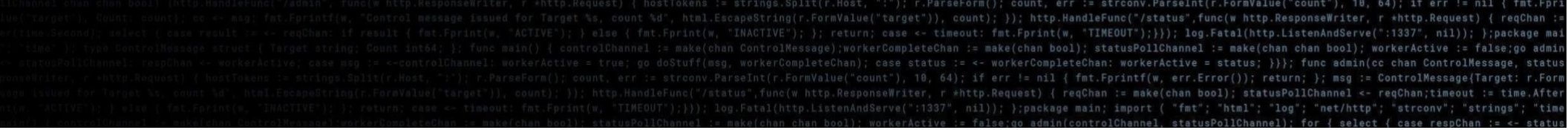


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
6.5.1	Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation 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.	Akamai is responsible for securely managing changes to system components it controls	Customers are responsible for security managing changes to system components they control	Shared 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.	Akamai is responsible for securely managing changes to system components it controls	Customers are responsible for security managing changes to system components they control	Shared responsibility.
6.5.3	Pre-production environments are separated from production environments and the separation is enforced with access controls.	Akamai is responsible for securely managing changes to system components it controls	Customers are responsible for security managing changes to system components they control	Shared responsibility.
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.	Akamai is responsible for securely managing changes to system components it controls	Customers are responsible for security managing changes to system components they control	Shared responsibility.

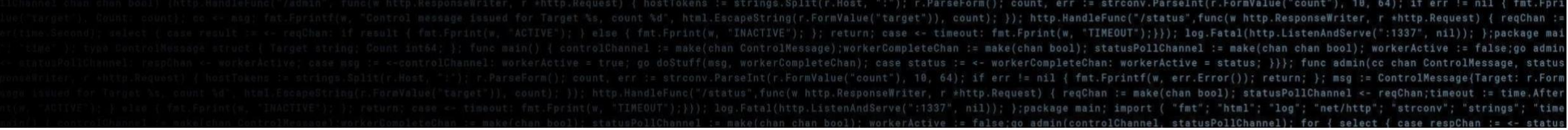
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
6.5.5	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	Akamai is responsible for securely managing changes to system components it controls	Customers are responsible for security managing changes to system components they control	Shared responsibility.
6.5.6	Test data and test accounts are removed from system components before the system goes into production.	Akamai is responsible for securely managing changes to system components it controls	Customers are responsible for security managing changes to system components they control	Shared responsibility.
7.1	Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.	Akamai is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying Akamai services.	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.	Akamai is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying Akamai services.	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
7.1.2	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	Akamai is responsible for implementing access controls in compliance with this requirement for the systems and infrastructure underlying Akamai services.	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
7.2	Access to system components and data is appropriately defined and assigned.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
7.2.3	Required privileges are approved by authorized personnel.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.

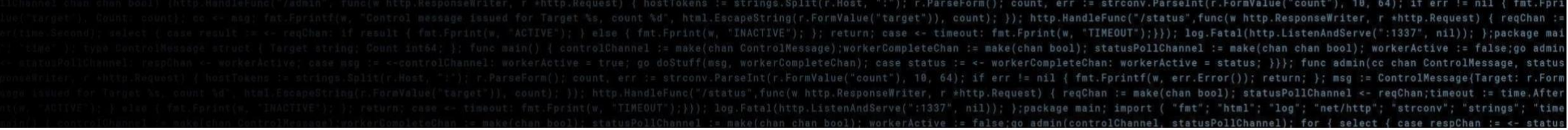
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
7.2.4	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts 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.**	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.**	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
7.3	Access to system components and data is managed via an access control system(s).	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
7.3.3	The access control system(s) is set to "deny all" by default.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
8.1	Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.	Akamai will manage the responsibility of ensuring any internal access to system components follow appropriate policies and guidelines set forth by PCI DSS.	All In-Scope Services: Akamai customers are responsible for managing the creation of user accounts, which includes access controls to any applications that customers may be hosting on Akamai services.	Shared responsibility.



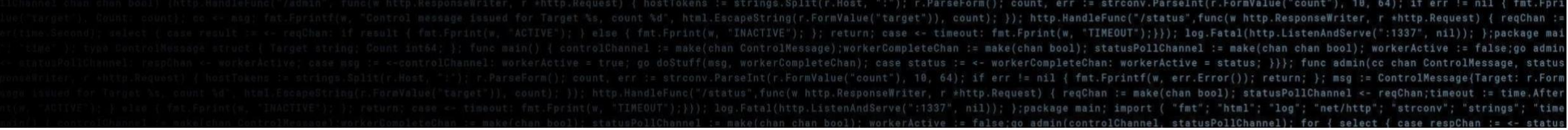
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.1.1	All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Akamai will manage the responsibility of ensuring any internal access to system components follow appropriate policies and guidelines set forth by PCI DSS.	All In-Scope Services: Akamai customers are responsible for managing the creation of user accounts, which includes access controls to any applications that customers may be hosting on Akamai services.	Shared responsibility.
8.1.2	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	Akamai will manage the responsibility of ensuring any internal access to system components follow appropriate policies and guidelines set forth by PCI DSS.	All In-Scope Services: Akamai customers are responsible for managing the creation of user accounts, which includes access controls to any applications that customers may be hosting on Akamai services.	Shared responsibility.
8.2	User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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 for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.		
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 for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.

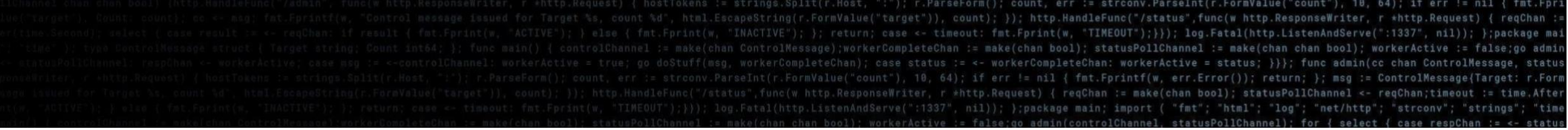
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.2.5	Access for terminated users is immediately revoked.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.			Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.3	Strong authentication for users and administrators is established and managed.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
8.3.2	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
8.3.3	User identity is verified before modifying any authentication factor.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.
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.**	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing access to all in-scope services that are included in their CDE. Akamai provides access controls to their services through the Cloud Manager Portal.	Shared responsibility.

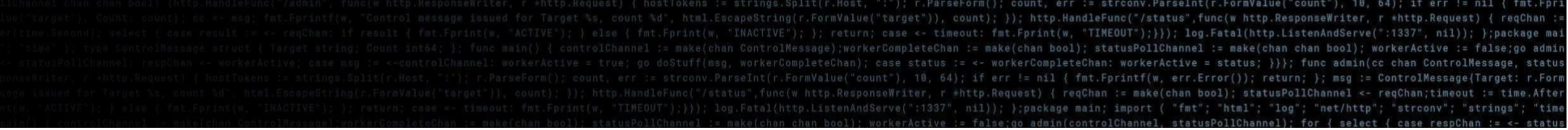


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.3.7	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing the creation of user accounts, which includes access controls to any applications that customers may be hosting on Akamai services.	Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing the creation of user accounts, which includes access controls to any applications that customers may be hosting on Akamai services.	Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing the creation of user accounts, which includes access controls to any applications that customers may be hosting on Akamai services.	Shared responsibility.



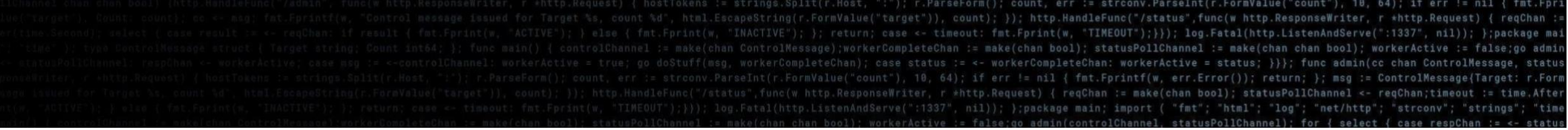
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.3.10	Additional requirement for service providers only: If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in 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.	Akamai will manage the responsibility of ensuring any internal access to system components follow appropriate policies and guidelines set forth by PCI DSS.		
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.**	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing the creation of user accounts, which includes access controls to any applications that customers may be hosting on Akamai services.	Shared responsibility.
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.	Akamai is responsible for access controls for systems and applications it controls	All In-Scope Services: Akamai customers are responsible for managing the creation of user accounts, which includes access controls to any applications that customers may be hosting on Akamai services.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.4	Multi-factor authentication (MFA) is implemented to secure access into the CDE.		All In-Scope Services: Akamai customers are responsible for enabling MFA to their Akamai services and accounts. Opt-in MFA is available to use on the customer's Cloud Manager portal. Customers are responsible for managing their own 2FA mechanisms for accessing their Akamai VMs and storage boxes.	
8.4.1	MFA is implemented for all non-console access into the CDE for personnel with administrative access.		All In-Scope Services: Akamai customers are responsible for enabling MFA to their Akamai services and accounts. Opt-in MFA is available to use on the customer's Cloud Manager portal. Customers are responsible for managing their own 2FA mechanisms for accessing their Akamai VMs and storage boxes.	
8.4.2	MFA is implemented for all access into the CDE. **This requirement is a best practice until 31 March 2025.**		All In-Scope Services: Akamai customers are responsible for enabling MFA to their Akamai services and accounts. Opt-in MFA is available to use on the customer's Cloud Manager portal. Customers are responsible for managing their own 2FA mechanisms for accessing their Akamai VMs and storage boxes.	



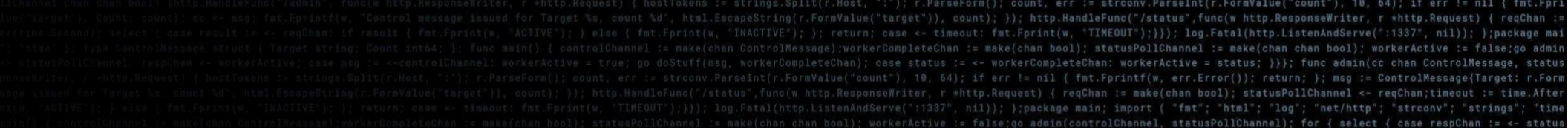
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.4.3	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.		All In-Scope Services: Akamai customers are responsible for enabling MFA to their Akamai services and accounts. Opt-in MFA is available to use on the customer's Cloud Manager portal. Customers are responsible for managing their own 2FA mechanisms for accessing their Akamai VMs and storage boxes.	
8.5	Multi-factor authentication (MFA) systems are configured to prevent misuse.		All In-Scope Services: Akamai customers are responsible for enabling MFA to their Akamai services and accounts. Opt-in MFA is available to use on the customer's Cloud Manager portal. Customers are responsible for managing their own 2FA mechanisms for accessing their Akamai VMs and storage boxes.	

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**		All In-Scope Services: Akamai customers are responsible for enabling MFA to their Akamai services and accounts. Opt-in MFA is available to use on the customer's Cloud Manager portal. Customers are responsible for managing their own 2FA mechanisms for accessing their Akamai VMs and storage boxes.	
8.6	Use of application and system accounts and associated authentication factors is strictly managed.	Akamai is responsible for managing the use of application and system accounts and associated authentication factors for systems and applications it controls.	Customers are responsible for managing the use of application and system accounts and associated authentication factors for systems and applications they controls.	Shared responsibility.

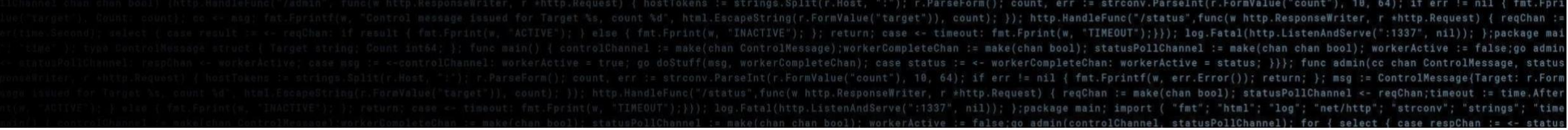


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.6.1	If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • 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.**	Akamai is responsible for managing the use of application and system accounts and associated authentication factors for systems and applications it controls.	Customers are responsible for managing the use of application and system accounts and associated authentication factors for systems and applications they controls.	Shared responsibility.
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.**	Akamai is responsible for managing the use of application and system accounts and associated authentication factors for systems and applications it controls.	Customers are responsible for managing the use of application and system accounts and associated authentication factors for systems and applications they controls.	Shared responsibility.

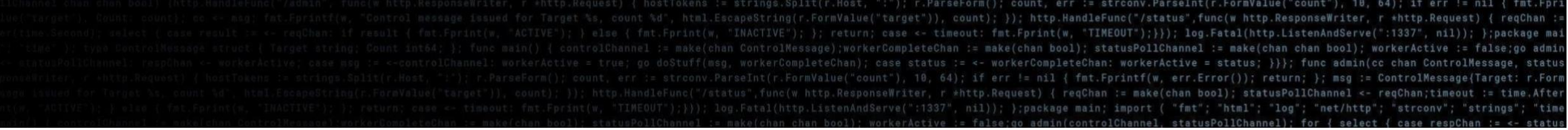
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined 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.**	Akamai is responsible for managing the use of application and system accounts and associated authentication factors for systems and applications it controls.	Customers are responsible for managing the use of application and system accounts and associated authentication factors for systems and applications they controls.	Shared responsibility.
9.1	Processes and mechanisms for restricting physical access to cardholder data are defined and understood.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.1.2	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
9.2	Physical access controls manage entry into facilities and systems containing cardholder data.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.2.1	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.2.2	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		

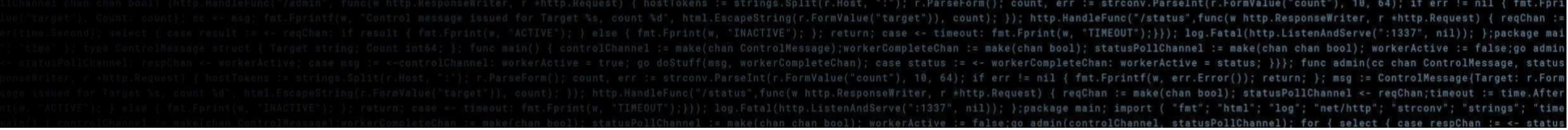


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
9.2.3	Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.2.4	Access to consoles in sensitive areas is restricted via locking when not in use.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.3	Physical access for personnel and visitors is authorized and managed.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		



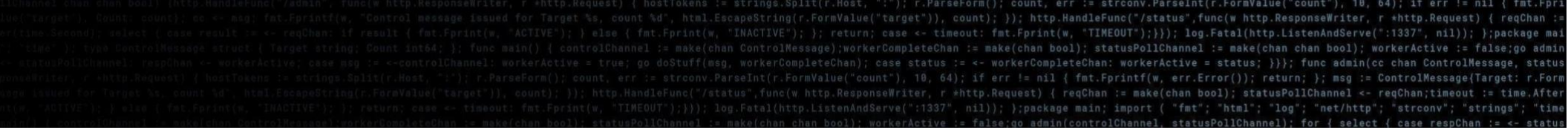
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
9.3.1.1	Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.3.3	Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.4	Media with cardholder data is securely stored, accessed, distributed, and destroyed.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.4.1	All media with cardholder data is physically secured.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		



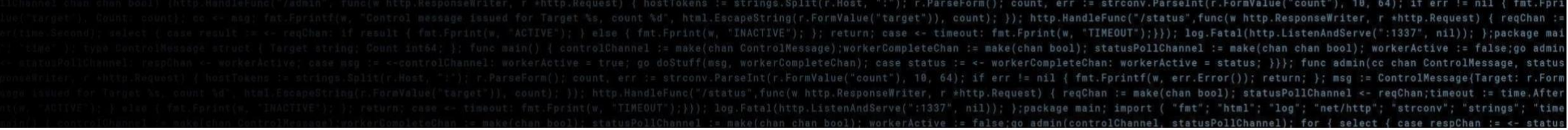
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.4.5	Inventory logs of all electronic media with cardholder data are maintained.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.4.5.1	Inventories of electronic media with cardholder data are conducted at least once every 12 months.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.5	Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		



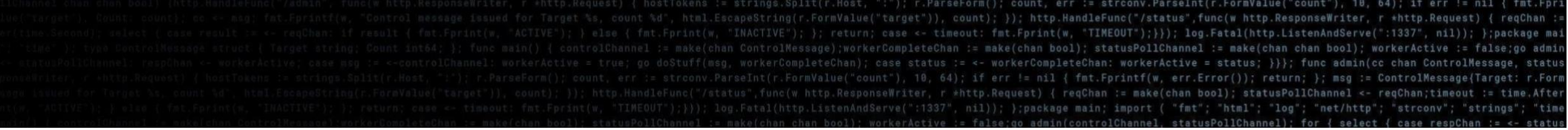
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
9.5.1.1	An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
9.5.1.2	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	Akamai is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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 is responsible for physical security controls provided by Akamai or its partners serving Akamai hardware assets.		
10.1	Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.	Akamai is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying Akamai in compliance with the requirements of section 10.	Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	Shared responsibility.

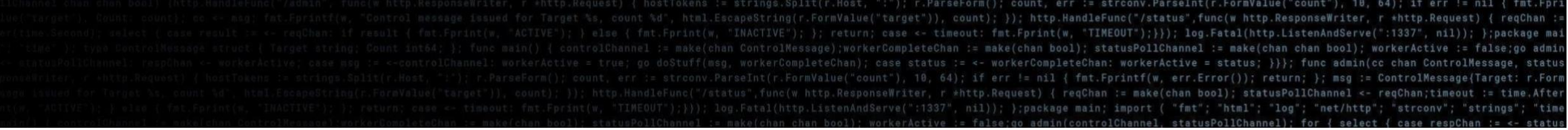


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.1.1	All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	Akamai is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying Akamai in compliance with the requirements of section 10.	Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	Shared responsibility.
10.1.2	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	Akamai is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying Akamai in compliance with the requirements of section 10.	Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	Shared responsibility.
10.2	Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	

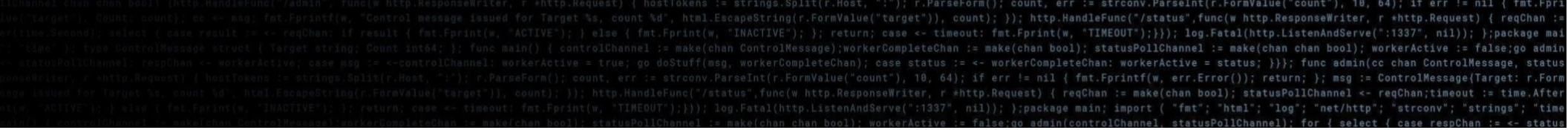
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.2.1	Audit logs are enabled and active for all system components and cardholder data.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
10.2.1.1	Audit logs capture all individual user access to cardholder data.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
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.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.2.1.3	Audit logs capture all access to audit logs.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
10.2.1.4	Audit logs capture all invalid logical access attempts.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
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.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	

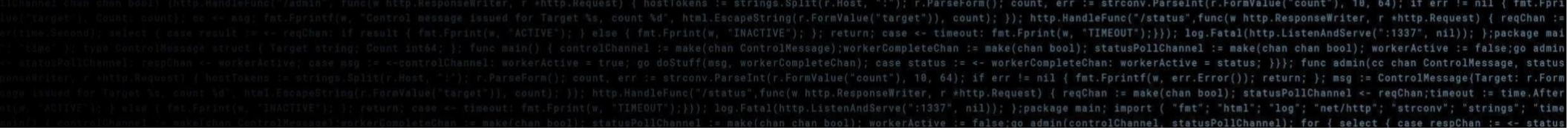


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.2.1.6	Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
10.2.1.7	Audit logs capture all creation and deletion of system-level objects.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
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).		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	

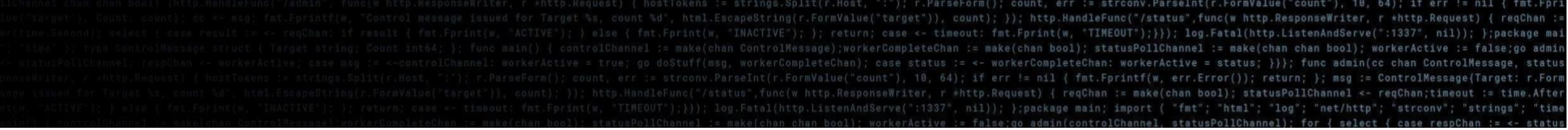


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.3	Audit logs are protected from destruction and unauthorized modifications.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
10.3.1	Read access to audit logs files is limited to those with a job-related need.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
10.3.2	Audit log files are protected to prevent modifications by individuals.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	

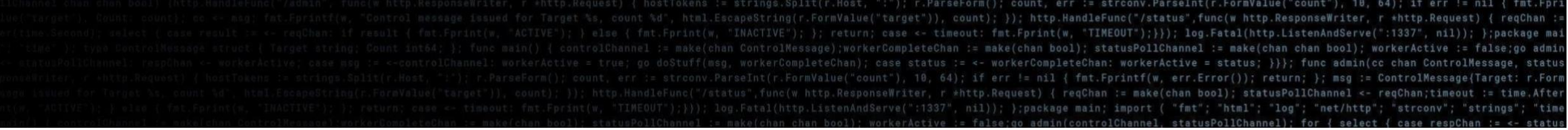
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.3.3	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
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.		Akamai customers are responsible for controlling access, logging and monitoring on all customer deployed instances on Akamai in compliance with the requirements of section 10. Akamai provides both access and event logging on the Cloud Manager platform for customers to utilize.	
10.4	Audit logs are reviewed to identify anomalies or suspicious activity.	Akamai is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying Akamai in compliance with the requirements of section 10.	Customers must 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.	Shared responsibility.



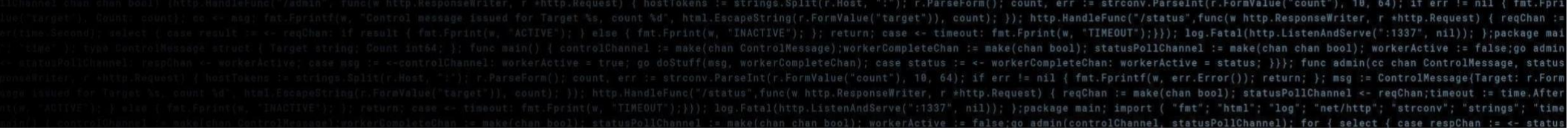
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.4.1	The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of 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).		Customers must review 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.**		Customers must review 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	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.		Customers must review 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.	



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**		Customers must review 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.	
10.4.3	Exceptions and anomalies identified during the review process are addressed.		Customers must review 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.		Customers must review 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.	

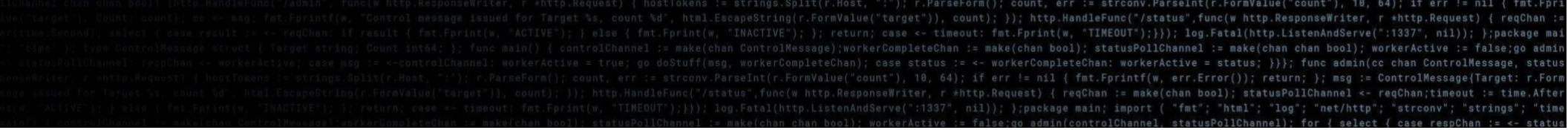


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.		Customers must review logs and security events 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.	
10.6	Time-synchronization mechanisms support consistent time settings across all systems.		Customers must review 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.	
10.6.1	System clocks and time are synchronized using time-synchronization technology.		Customers must review 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.	

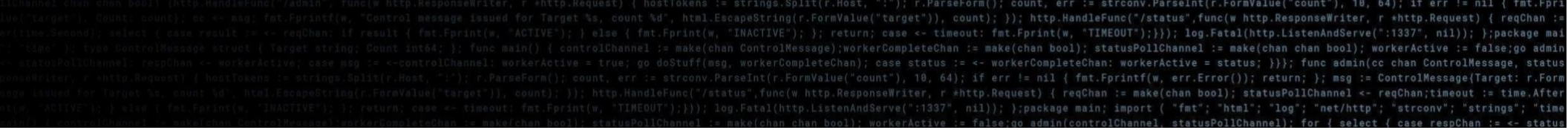


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.6.2	Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives 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).		Customers must review 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.	
10.6.3	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.		Customers must review 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.	
10.7	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.	

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**	Akamai is responsible for controlling access, logging and monitoring of the systems and infrastructure underlying Akamai in compliance with the requirements of section 10.		
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.	

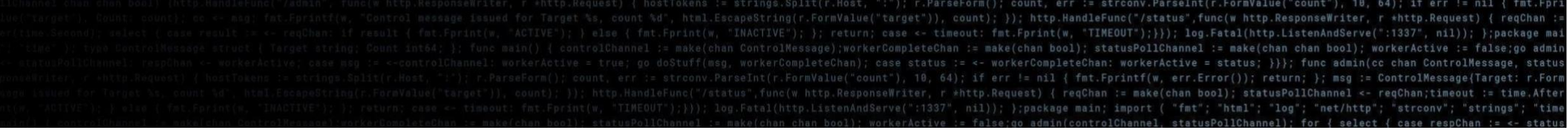


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
10.7.3	Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the 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.	Akamai is responsible for security policies and operational procedures for Akamai in compliance with the requirements of section 11.	Customers are responsible for the security of their wireless networks. Akamai infrastructure in scope for PCI does not use wireless.	Shared responsibility.
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.	Akamai is responsible for security policies and operational procedures for Akamai in compliance with the requirements of section 11.	Customers are responsible for the security of their wireless networks. Akamai infrastructure in scope for PCI does not use wireless.	Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
11.1.2	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	Akamai is responsible for security policies and operational procedures for Akamai in compliance with the requirements of section 11.	Customers are responsible for the security of their wireless networks. Akamai infrastructure in scope for PCI does not use wireless.	Shared responsibility.
11.2	Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.	Akamai is responsible for security policies and operational procedures for Akamai in compliance with the requirements of section 11.		
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.	Akamai is responsible for security policies and operational procedures for Akamai in compliance with the requirements of section 11.		
11.2.2	An inventory of authorized wireless access points is maintained, including a documented business justification.	Akamai is responsible for security policies and operational procedures for Akamai in compliance with the requirements of section 11.		
11.3	External and internal vulnerabilities are regularly identified, prioritized, and addressed.		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	

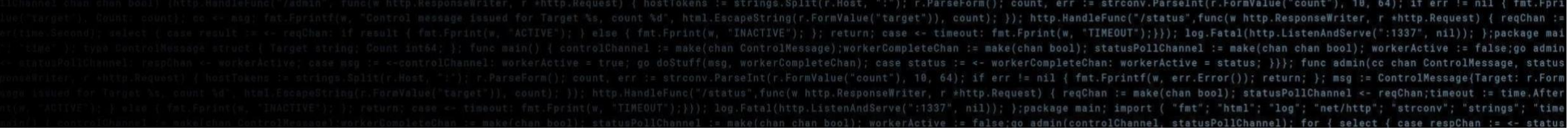
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
11.3.1	Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings 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.		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	
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.**		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	



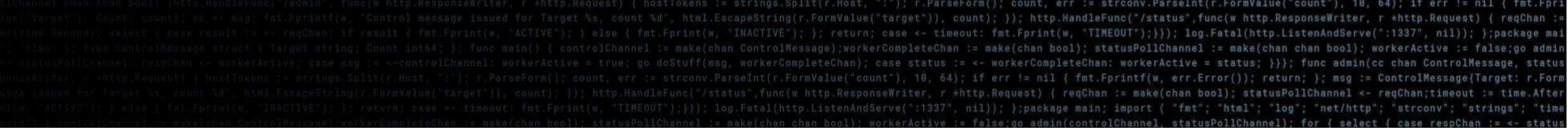
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning as follows: • Systems that are unable to accept credentials for authenticated scanning are documented. • 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.**		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	
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).		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	
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.		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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).		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	
11.4	External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	

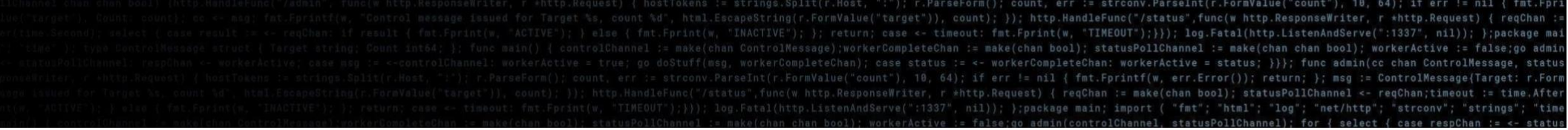
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
11.4.1	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the 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.		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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).		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	
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).		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	
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.		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	

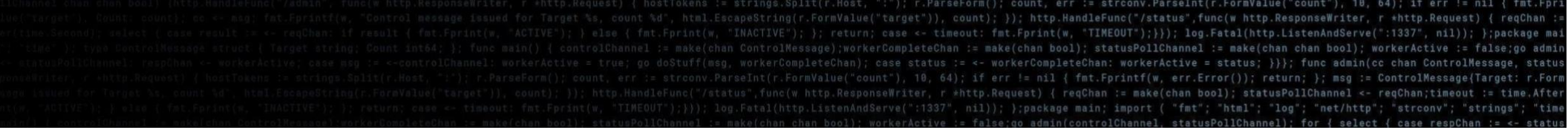


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
11.4.5	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after 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).		Akamai customers are responsible for performing vulnerability scans and penetration tests on customer deployed instances on Akamai in compliance with the requirements of section 11.	

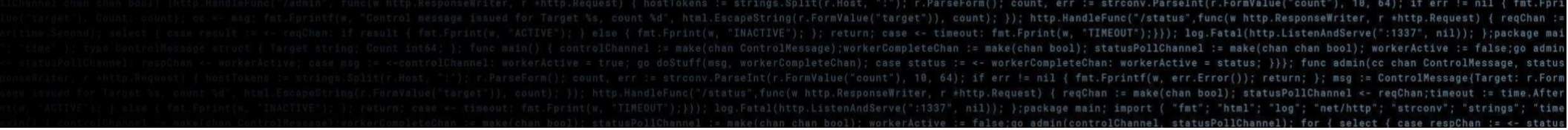


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
11.4.6	Additional requirement for service providers only: If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls 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).	Akamai is responsible for security policies and operational procedures for Akamai in compliance with the requirements of section 11.		
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.**	Akamai is responsible for security policies and operational procedures for Akamai in compliance with the requirements of section 11.		
11.5	Network intrusions and unexpected file changes are detected and responded to.		Customers are not responsible for meeting this requirement.	

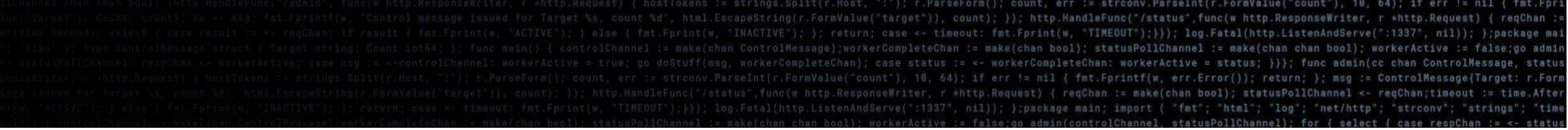
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
11.5.1	Intrusion-detection and/or intrusion prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter 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.		Customers are not responsible for meeting this requirement.	
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.**		Customers are not responsible for meeting this requirement.	
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.		Customers are not responsible for meeting this requirement.	
11.6	Unauthorized changes on payment pages are detected and responded to.		Customers are not responsible for meeting this requirement.	



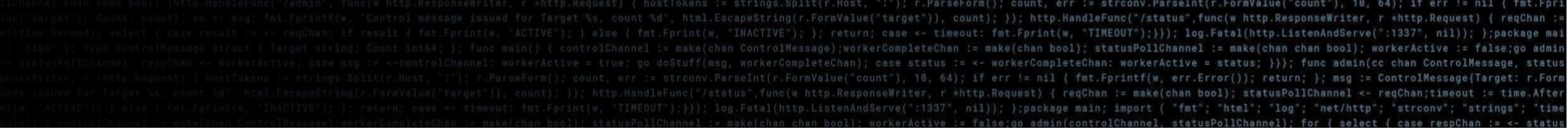
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
11.6.1	A change- and tamper-detection mechanism is deployed as follows: • To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, 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.**		Customers are not responsible for meeting this requirement.	
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.

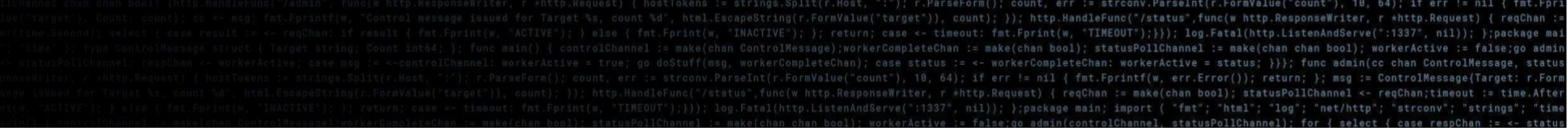


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
12.1.4	Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.
12.2	Acceptable use policies for end-user technologies are defined and implemented.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.

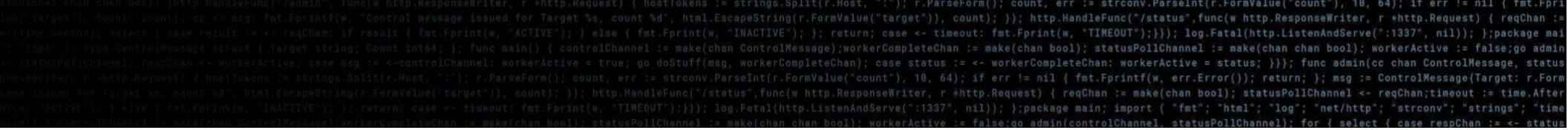


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
12.3	Risks to the cardholder data environment are formally identified, evaluated, and managed.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.
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.**	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.
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 establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.

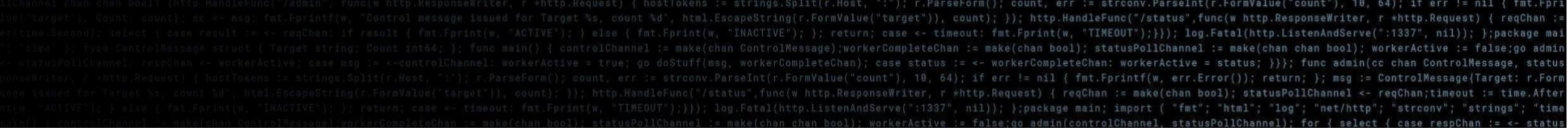


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
12.3.4	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive 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 establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.	Akamai customers are responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and instances deployed by customers on Akamai.	Shared responsibility.
12.4	PCI DSS compliance is managed.			
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.		

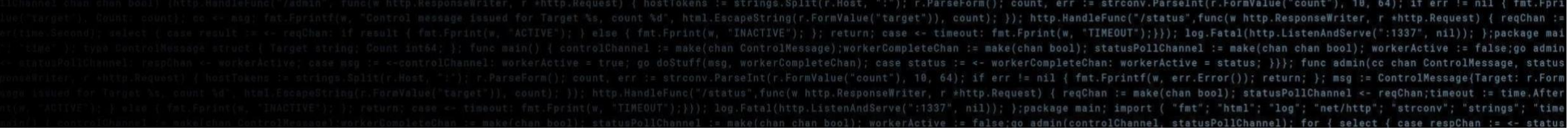


PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
12.4.2	Additional requirement for service providers only: Reviews are performed at least once every three months to confirm that personnel are performing their tasks in accordance 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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.		
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.		
12.5	PCI DSS scope is documented and validated.	Akamai is responsible for documenting and validating PCI DSS Scope with respect to systems and applications it controls	Customers are responsible for documenting and validating PCI DSS Scope with respect to systems and applications they control.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	Akamai is responsible for documenting and validating PCI DSS Scope with respect to systems and applications it controls	Customers are responsible for documenting and validating PCI DSS Scope with respect to systems and applications they control.	Shared responsibility.



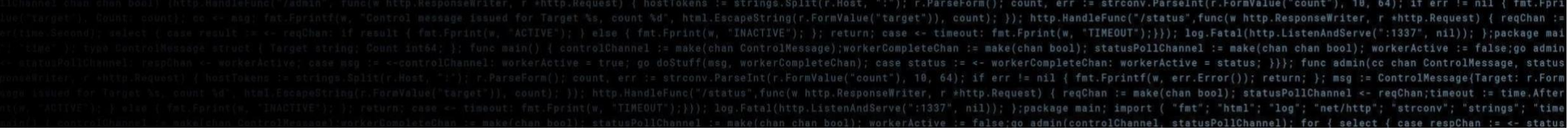
12.5.2	PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes: • Identifying all data flows for the various payment stages (for example, authorization, capture settlement, 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.	Akamai is responsible for documenting and validating PCI DSS Scope with respect to systems and applications it controls	Customers are responsible for documenting and validating PCI DSS Scope with respect to systems and applications they control.	Shared responsibility.
12.5.2.1	Additional requirement for service providers only: PCI DSS scope is documented and	Akamai is responsible for establishing, maintaining and		



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
	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.**	disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.		
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.**	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.		
12.6	Security awareness education is an ongoing activity.	Akamai is responsible for security awareness education of its staff.	Customers are responsible for security awareness education of their staff.	Shared responsibility.
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.	Akamai is responsible for security awareness education of its staff.	Customers are responsible for security awareness education of their staff.	Shared responsibility.

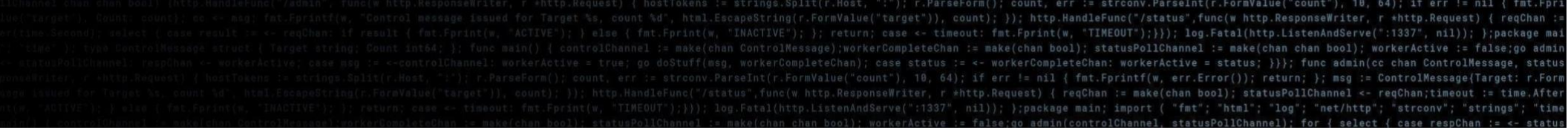
PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
12.6.2	The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security 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.**	Akamai is responsible for security awareness education of its staff.	Customers are responsible for security awareness education of their staff.	Shared responsibility.
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.	Akamai is responsible for security awareness education of its staff.	Customers are responsible for security awareness education of their staff.	Shared responsibility.
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.	Akamai is responsible for security awareness education of its staff.	Customers are responsible for security awareness education of their staff.	Shared responsibility.
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.**	Akamai is responsible for security awareness education of its staff.	Customers are responsible for security awareness education of their staff.	Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
12.7	Personnel are screened to reduce risks from insider threats.			Shared responsibility.
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.			Shared responsibility.
12.8	Risk to information assets associated with third-party service provider (TPSP) relationships is managed.			Shared responsibility.
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.			Shared responsibility.
12.8.2	Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.			Shared responsibility.
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.			Shared responsibility.
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.			Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.	Akamai maintains this information in this responsibility matrix		
12.9	Third-party service providers (TPSPs) support their customers' PCI DSS compliance.	Akamai is responsible for supporting customers' PCI DSS compliance.		
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.	Akamai is responsible for establishing, maintaining and disseminating security policies, usage policies and performing risk assessments for all systems and infrastructure underlying Akamai in compliance with the requirements in section 12.		
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).	**Akamai supports customer requests for information in compliance with this requirement.**		

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.			Shared responsibility.
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.			Shared responsibility.
12.10.3	Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.			Shared responsibility.



PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.			Shared responsibility.
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.**			Shared responsibility.
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.**			Shared responsibility.
12.10.6	The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.			Shared responsibility.

PCI Control Number	PCI DSS Requirement Responsibility	Akamai Responsibility	Customer Responsibility	Shared Responsibility
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.**			Shared responsibility.