Certificate
Payment Card Industry Data Security Standard

more security. **usd**

We hereby confirm

PlusServer GmbH
Venloer Str. 47
50672 Cologne
Germany

successfully provided evidence of compliance according to the Payment Card Industry Data Security Standard (PCI DSS) version 4.0.1.

The company successfully passed the following PCI DSS assessment measures:

Assessment Measure	Assessment Date	Expiration Date
Onsite Assessment	15-Jan-2025	14-Jan-2026

This confirmation shall be valid only for the assessment objects tested on the date of the test. The company obligates itself to use the certificate it received and the assessment logo only during the validity period shown above.

more security.usd
JAN-2025
PCI DSS compliant

Neu-Isenburg, 22/01/2025

Place, Date

usd AG
Manfred Tubach, CEO

usd AG
Approved Scanning Vendor
Qualified Security Assessor
P2PE Qualified Security Assessor
3DS Assessor
Qualified PIN Assessor
Software Security Framework Assessor

Neu-Isenburg, Germany

Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: PlusServer GmbH

Date of Report as noted in the Report on Compliance: 15 Jan 2025

Date Assessment Ended: 15 Jan 2025

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures ("*Assessment*")*. Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information	
Part 1a. Assessed Entity **(ROC Section 1.1)**	
Company name:	PlusServer GmbH
DBA (doing business as):	-
Company mailing address:	Venloer Str. 47, 50672 Cologne, Germany
Company main website:	www.plusserver.com
Company contact name:	Falko Stetter
Company contact title:	Director IT-Security & Processes
Contact phone number:	+49 2203 1045-7804
Contact e-mail address:	falko.stetter@plusserver.com
Part 1b. Assessor **(ROC Section 1.1)**	
Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.	
PCI SSC Internal Security Assessor(s)	
ISA name(s):	**-**
Qualified Security Assessor	
Company name:	usd AG
Company mailing address:	Frankfurter Str. 233, Haus C1, 63263 Neu-Isenburg, Germany
Company website:	https://www.usd.de
Lead Assessor name:	Nur Ahmad
Assessor phone number:	+49 6102 8631 342
Assessor e-mail address:	nur.ahmad@usd.de
Assessor certificate number:	205-588

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were <u>INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	Housing / Co-location

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☐ Systems security services	☐ POI / card present
☒ Hardware	☐ IT support	☐ Internet / e-commerce
☒ Infrastructure / Network	☒ Physical security	☐ MOTO / Call Center
☒ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		

☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments

☐ Network Provider

☒ Others (specify):   Media handling and destruction, WLAN scanning

Note: These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.

PCI Security Standards Council ®

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were <u>NOT INCLUDED</u> in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Managed Services, Cloud Services

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software	☒ Systems security services	☐ POI / card present
☐ Hardware	☒ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		

☐ Others (specify):

Provide a brief explanation why any checked services were not included in the Assessment:	The entity offers various services. Nevertheless, this assessment only covers the housing / co-location services, media handling and destruction, and WLAN scanning

Part 2b. Description of Role with Payment Cards
(ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	PlusServer GmbH (PlusServer) is a housing / co-location provider.
	PlusServer offers their customers data center services including single racks up to whole cages which can only be entered by their customers.
	Those services include physical security as well as media handling and destruction, and WLAN scanning.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	PlusServer provides housing / co-location services and is therefore responsible for physical security and relating processes. PlusServer has no logical access to the networks, systems, or data of their customers. PlusServer is only responsible for providing physical security to their customers as well as media handling and destruction, and WLAN scanning.
Describe system components that could impact the security of account data.	None

Security Standards Council ®

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	There is no cardholder data environment at PlusServer since the assessed entity does not store, process, or transmit cardholder data itself or has any logical access to their customer's networks that have a cardholder data environment. Therefore, no critical systems exist in the scope of this assessment. PlusServer is only responsible for providing physical security to their customers as well as media handling and destruction and WLAN scanning.

Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities
(ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Datacenter CGN 3.1, CGN 3.2	2	Welserstr. 14, 51149 Cologne, Germany
Datacenter DUS 6.1, DUS 6.2	2	In der Steele 33a-41, 40599 Dusseldorf, Germany
Datacenter HAM5	1	Heidbergstrasse 101-111, 22846 Norderstedt, Germany
Datacenter HAM6	1	Koenig-Georg-Deich 2, 21107 Hamburg Wilhelmsburg, Germany

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions
(ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions.*?

☐ Yes   ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
-	-	-	-	-

*   For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

![PCI Security Standards Council logo]

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers
*(*ROC Section 4.4*)*

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☐ Yes ☒ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☐ Yes ☒ No

If Yes:

Name of Service Provider:	Description of Services Provided:
Stadtwerke Norderstedt	Data Center housing provider: Owner of the Data Center in Norderstedt, Germany (HAM 5). Responsible for the local administration (for Stadtwerke Norderstedt) and the physical environment and security mechanisms.
EPC Global Solutions Deutschland GmbH	Media disposal and destruction in Cologne, Dusseldorf and Hamburg
Gesellschaft für Wachschutz (GfW)	Object Monitoring and Access Control

Note: Requirement 12.8 applies to all entities in this list.

![PCI Security Standards Council logo]

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

Note: One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.

Name of Service Assessed: Housing / Co-location

PCI DSS Requirement	Requirement Finding — More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	**Not Applicable**	**Not Tested**	**Not in Place**	
Requirement 1:	☐	☐	☒	☐	☐
Requirement 2:	☐	☐	☒	☐	☐
Requirement 3:	☐	☐	☒	☐	☐
Requirement 4:	☐	☐	☒	☐	☐
Requirement 5:	☐	☐	☒	☐	☐
Requirement 6:	☐	☐	☒	☐	☐
Requirement 7:	☐	☐	☒	☐	☐
Requirement 8:	☐	☐	☒	☐	☐
Requirement 9:	☒	☒	☒	☐	☐
Requirement 10:	☒	☐	☒	☐	☐
Requirement 11:	☒	☐	☒	☐	☐
Requirement 12:	☒	☒	☐	☐	☐
Appendix A1:	☐	☐	☒	☐	☐
Appendix A2:	☐	☐	☒	☐	☐
Justification for Approach					

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	**9.2.2:** PlusServer does not have access to any customer's network. **9.2.4:** No systems with cardholder data are in scope of this assessment. **9.4.1.1 – 9.4.1.2:** No backups are part of this assessment. **9.4.3:** No sending of media is part of this assessment. **9.4.6:** There is no hard-copy material with cardholder data on it in scope of this assessment. **12.3.2:** The customized approach is not used in this assessment. **12.3.3:** PlusServer is only providing housing / co-location services. Cryptographic cipher suites and protocols are not used by PlusServer in the defined PCI DSS scope. **12.3.4:** PlusServer is only providing housing / co-location services. Hardware and software technologies are not part of the data center services assessed. **12.5.1:** PlusServer is only providing housing / co-location services. PlusServer has no system components in scope of this assessment. **12.10.7:** PlusServer is only providing co-location services and cardholder data is not stored by PlusServer.

For any Not Tested responses, identify which sub-requirements were not tested and the reason.	**1.1.1 – 1.5.1:** Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment. **2.1.1 – 2.3.2:** Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment. **3.1.1 – 3.7.9:** Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment. **4.1.1 – 4.2.2:** Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment. **5.1.1 – 5.4.1:** Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment. **6.1.1 – 6.5.6:** Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment. **7.1.1 – 7.3.3:** Not tested. This requirement is not part of the data center services assessed. The assessed entity does

not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment.

8.1.1 – 8.6.3:

Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment.

9.5.1 - 9.5.1.3:

Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data and does not have any devices that capture payment card data.

10.2.1 – 10.6.3:

Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment.

11.3.1 – 11.6.1:

Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment.

A1.1.1 – A1.2.3:

Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment.

A2.1.1 – A2.1.3:

Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that

	process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment. PlusServer does not have any devices that capture payment card data.
	A3:
	Not tested. This requirement is not part of the data center services assessed. The assessed entity does not store, process or transmit cardholder data in any way. The assessed entity has no access to the production environment of their customers that process cardholder data. Therefore, this requirement is not deemed to be in scope of this assessment.
	PlusServer is not a designated entity.

Section 2 Report on Compliance

(ROC Sections 1.2 and 1.3)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	19 Sep 2024
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	15 Jan 2025
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated 15 Jan 2025.

Indicate below whether a full or partial PCI DSS assessment was completed:

☐ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☒ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one):*

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby PlusServer GmbH has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

PCI Security Standards Council ®

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement
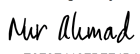
Signatory(s) confirms:

(Select all that apply)

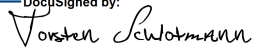| ☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Signiert von: *Falko Stetter* —01C89A30E64944B...	
Signature of Service Provider Executive Officer ↑	Date: 15 January 2025 | 10:50 MEZ
Service Provider Executive Officer Name: **Falko Stetter**	Title: **Director IT-Security & Processes**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

DocuSigned by: *Nur Ahmad* —E2F2E412FBFF4B4...	
Signature of Lead QSA ↑	Date: 15 January 2025 | 10:51 MEZ
Lead QSA Name: **Nur Ahmad**	

DocuSigned by: *Torsten Schlotmann* —9366AA034EE04CE...	
Signature of Duly Authorized Officer of QSA Company ↑	Date 15 January 2025 | 11:07 MEZ
Duly Authorized Officer Name: **Torsten Schlotmann**	QSA Company: **usd AG**

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	**NO**	
1	Install and maintain network security controls	☐	☐	
2	Apply secure configurations to all system components	☐	☐	
3	Protect stored account data	☐	☐	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	
5	Protect all systems and networks from malicious software	☐	☐	
6	Develop and maintain secure systems and software	☐	☐	
7	Restrict access to system components and cardholder data by business need to know	☐	☐	
8	Identify users and authenticate access to system components	☐	☐	
9	Restrict physical access to cardholder data	☐	☐	
10	Log and monitor all access to system components and cardholder data	☐	☐	
11	Test security systems and networks regularly	☐	☐	
12	Support information security with organizational policies and programs	☐	☐	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit: https://www.pcisecuritystandards.org/about_us/

PCI DSS letter to the customer

version – v2.4 EN

11. Dec 2024

Dear Customer,

To provide transparency over our continuous PCI DSS compliance effort, we have listed below all applicable clauses to plusserver sites from PCI DSS version 4.0.1. Please consider that other requirements, which are not mentioned in this paper, are not implemented at plusserver data centers or are the sole responsibility of you as our customer.

plusserver is responsible for the security of cardholder data to the extent of the services that are being provided, as specified in the list of security controls below. The responsibilities are based on housing services which are the basis to every customer data environment (CDE).

Please note that all requirements that we as plusserver fulfil must be checked by you, as the scope of your CDE may extend beyond the services booked with us.

If you have any questions regarding status information for any service provided by us or our subcontractors with the PCI DSS scope, please do not hesitate to contact our Support Team or your Service Manager.

Kind regards

Falko Stetter

Information Security Officer

Req. 9 - Restrict physical access to cardholder data

9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.

> 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

> 9.1.2 Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.

9.2 Physical access controls manage entry into facilities and systems containing cardholder data.

> 9.2.1 Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.

> 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.

> 9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.

9.3 Control physical access for onsite personnel to sensitive areas

> 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.

> 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.

> 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.

	9.3.3 Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.
	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.
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.	
	9.4.1 All media with cardholder data is physically secured.
	9.4.2 All media with cardholder data is classified in accordance with the sensitivity of the data.
	9.4.4 Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).
	9.4.5 Inventory logs of all electronic media with cardholder data are maintained.
	9.4.5.1 Inventories of electronic media with cardholder data are conducted at least once every 12 months.
	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.

Req.10 - Regularly Monitor and Test Networks

	10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and understood.
	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.
	10.1.2 Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.	
	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: • Physical access controls.

10.7.2 Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems:

- Physical access controls.

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.

Req.11 – Test Security of Systems and Networks Regularly

11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.

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.

11.1.2 Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.

11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.

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.

11.2.2 An inventory of authorized wireless access points is maintained, including a documented business justification.

Req.12 – Support Information Security with Organizational Policies and Programs

12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.

12.1.1 An overall information security policy is:

- Established.
- Published.
- Maintained.
- Disseminated to all relevant personnel, as well as to relevant vendors and business partners.

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.

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.

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.

12.2 Acceptable use policies for end-user technologies are defined and implemented.

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

12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.

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.

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.

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:

- Responding to security alerts.
- Change-management processes.

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.

12.5 PCI DSS scope is documented and validated.

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 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.

12.5.2.1 Additional requirement for service providers only: PCI DSS scope is documented and confirmed by the entity at least once every six months and upon significant change to the in-scope environment. At a minimum, the scoping validation includes all the elements specified in Requirement 12.5.2.

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.

12.6 Security awareness education is an ongoing activity.

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.

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.

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.

	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.
	12.6.3.2 Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.
12.7 Personnel are screened to reduce risks from insider threats.	
	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.
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.	
	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.
	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.
	12.8.3 An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.
	12.8.4 A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.
	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.
12.9 Third-party service providers (TPSPs) support their 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.
	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).

12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.	
	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.
	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.
	12.10.3 Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.
	12.10.4 Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.
	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.
	12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Detection of unauthorized wireless access points.
	12.10.6 The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.