PCI DSS letter to the customer

version – v2.0 EN

15. Jan. 2024

plusserver gmbh
Venloer Straße 47
50672 Cologne

Contact
Phone: +49 2203 1045 3500
Email: info@plusserver .com

Trade Register
County Court Cologne
HRB 84977

Sales tax ID
DE815289260

Management
Alexander Wallner (CEO)
Claudia Berchtold

plusserver

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. 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

plusserver gmbh
Venloer Straße 47
50672 Cologne

Contact
Phone: +49 2203 1045 3500
Email: info@plusserver .com

Trade Register
County Court Cologne
HRB 84977

Sales tax ID
DE815289260

Management
Alexander Wallner (CEO)
Claudia Berchtold

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 Develop procedures to easily distinguish between onsite personnel and visitors	
	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.
	9.2.2 Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.
	9.2.3 Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.
	9.2.4 Access to consoles in sensitive areas is restricted via locking when not in use.
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 documented.	
	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 - Regularly test security systems and processes

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 - Maintain a policy that addresses information security for all personnel

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.	
	12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.
	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.