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: MWS Cloud, LLC

Date of Report as noted in the Report on Compliance: 2026-08-31

Date Assessment Ended: 2026-08-31

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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:	MWS Cloud, LLC
DBA (doing business as):	MWS Cloud, MWS Cloud Platform
Company mailing address:	18 Andropova ave., bldg. 9, Moscow, 115432, Russian Federation
Company main website:	https://mws.ru
Company contact name:	Victor Bobylkov
Company contact title:	Head of ISD MWS Cloud, LLC
Contact phone number:	+7 (495) 800-18-00
Contact e-mail address:	vmbobylkov@mts.ru
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):	Not Applicable
Qualified Security Assessor	
Company name:	Compliance Control Ltd.
Company mailing address:	3 Revolutsionnaya st., office 306, Volokolamsk,143600, Russian Federation
Company website:	https://compliance-control.ru
Lead Assessor name:	Aleksei Osipov
Assessor phone number:	+7 (499) 136-27-66
Assessor e-mail address:	info@compliance-control.ru
Assessor certificate number:	206-632

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	MWS Cloud Platform	
Type of service(s) assessed:		
Hosting Provider: ☒ Applications / software ☒ Hardware ☒ Infrastructure / Network ☒ Physical space (co-location) ☒ Storage ☒ Web-hosting services ☒ Security services ☐ 3-D Secure Hosting Provider ☒ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☒ Systems security services ☒ IT support ☒ Physical security ☐ Terminal Management System ☒ Other services (specify): SOC, DDoS Protection, IDS/IPS; 2FA; Firewall administration; WAF; NTP; Antivirus, Access management; log monitoring; vulnerability management, mDB, mK8s, MCripto, Object Storage, CDN.	**Payment Processing:** ☐ POI / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (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):		

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.*

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

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

Name of service(s) not assessed:	All other services not specifically listed above	
Type of service(s) not assessed:		
Hosting Provider: ☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	**Managed Services:** ☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	**Payment Processing:** ☐ POI / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (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 MWS Cloud Platform provides IaaS and managed services for the clients with partial responsibility for the clients' PCI DSS compliance by providing them security services according to PCI DSS requirements. Customers are responsible for the security and compliance of their private environments on their own, and those environments are out of the scope of the assessment, but the MWS Cloud Platform guarantees that its cloud platform is PCI DSS compliant as it is set out in an entity's standard agreement.

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.	MWS Cloud Platform does not directly transmit, process or store account data.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	MWS Cloud Platform is a managed service provider that offers a variety of IaaS services. Customers can create a PCI DSS-compliant environment that transmits, processes, and/or stores cardholder data using MWS Cloud Platform services and third-party solutions. As additional services, the MWS Cloud Platform provides managed services (SOC, DDoS Protection, IDS/IPS, 2FA, Firewall administration, WAF, NTP, Antivirus, Access management, log monitoring, vulnerability management, mDB, mK8s, MCripto, Object Storage, CDN). MWS Cloud Platform does not directly transmit, process, or store account data while providing these services. MWS Cloud Platform provides customers with controls and information needed to comply with PCI DSS.
Describe system components that could impact the security of account data.	MWS Cloud Platform does not directly transmit, process or store any cardholder data. System components that could impact the security of cardholder data: - Hypervisors, - Network security controls, - Servers, - Storages, - Information security services.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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.*	The MWS Cloud Platform provides an environment where customers may deploy their virtual servers and networks. MWS Cloud Platform does not directly transmit, process, or store any cardholder data. MWS Cloud Platform customers can create a PCI DSS-compliant environment based on a responsibility matrix using MWS Cloud Platform services and third-party solutions. MWS Cloud Platform does not access customer data, except for troubleshooting, on a per-incident basis, with customer permission. MWS Cloud Platform uses security tools for monitoring and testing its networks and system components. All communications from an out-of-scope environment and from web application interfaces are performed through the secure protocols. This assessment covered MWS Cloud Platform personnel responsible for the following: physical security, incident response, IS management, security awareness program implementation, administration of virtual infrastructure, administration of network infrastructure, and administration and maintenance of information security tools.
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*
Head office	1	Moscow, Russian Federation
Data center	2	Moscow, Russian Federation
Data center	1	Novosibirsk, Russian Federation

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD
				YYYY-MM-DD

* 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.

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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:
GreenBushDC	Datacenter (Co-location)
DC Avantage	Datacenter (Co-location)
MTS PJSC	Datacenter (Co-location)

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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: MWS Cloud Platform

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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	1.2.4, 1.4.4, 3.x, 4.x, 6.4.3, 6.5.5, 7.2.6, 9.4, 10.2.1.1, 11.6.1, 12.10.7 - The entity does not store, process and/or transmit cardholder data. 1.2.6 - No insecure protocols, ports or services are in use. 1.5.1 - Computing devices that connect to both untrusted networks, and the CDE, are not used. 2.2.5 - Insecure protocols, services or daemons are not used. 2.3 - There are no wireless networks and devices within the scope of the assessment. 6.2 - The entity does not develop any software in scope of PCI DSS. 6.4.1 - This requirement has been superseded by Requirement 6.4.2. 8.2.2 - Group, shared or generic IDs are not used. 8.2.3 - The entity does not have remote access to the customer premises. 8.2.7 - No remote access for third parties is allowed in the entity's infrastructure. 8.3.10 - This requirement has been superseded by Requirement 8.3.10.1. 8.6.1, 8.6.2 - The system accounts cannot be used for interactive login. 9.5 - The entity does not use POI-devices. 10.7.1 - This requirement has been superseded by Requirement 10.7.2. 11.2.2 - Wireless networks are not used. 12.3.2 - Customized Approach was not used. Appendix A2 - The entity does not use POS POI devices.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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.*	2026-07-31
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-08-31
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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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 *(Date of Report as noted in the ROC 2026-08-31)*.

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 MWS Cloud Platform 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

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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

Signature of Service Provider Executive Officer ↑	Date: 2026-08-31
Service Provider Executive Officer Name: Victor Bobylkov	Title: Head of ISD MWS Cloud, LLC

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:

Signature of Lead QSA ↑	Date: 2026-08-31
Lead QSA Name: Aleksei Osipov	
Signature of Duly Authorized Officer of QSA Company ↑	Date: 2026-08-31
Duly Authorized Officer Name: Ivan Tverdokhlebov	QSA Company: Compliance Control Ltd.

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:

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.

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/

© 2006–2024 PCI Security Standards Council, LLC. All rights reserved.