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: MineSec Pte Ltd.

Date of Report as noted in the Report on Compliance: 2026-03-26

Date Assessment Ended: 2026-03-26

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:	MineSec Pte Ltd.
DBA (doing business as):	MineSec Pte Ltd.
Company mailing address:	10 Anson Road, #03-27 International Plaza, Singapore 079903
Company main website:	minesecsoftpos.com
Company contact name:	Stone ZHONG
Company contact title:	Chief Technical Officer
Contact phone number:	+86 18925114736
Contact e-mail address:	stone.zhong@minesecsoftpos.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):	Not Applicable
Qualified Security Assessor	
Company name:	Evolution Limited
Company mailing address:	1008, Tower B, 83 King Lam Street, Cheung Sha Wan, Hong Kong
Company website:	www.evolve-online.com
Lead Assessor name:	Stephen (Fu Hang) WONG
Assessor phone number:	+852 2151-2490
Assessor e-mail address:	stephenw@evolve-online.com
Assessor certificate number:	PCI DSS QSA 204-269, PCI 3DS QSA 1100-186

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:	SoftPOS Solution	
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):	**Payment Processing:** ☐ POI / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☒ Other processing (specify): SoftPOS Solution / card present
☐ 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.*

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:	Not Applicable	
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:		

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.	The assessed entity provides SoftPOS solution to merchants. Merchants can install the SoftPOS payment application on their smart phones to accept contactless payments. Cardholder data is provided by customers via the SoftPOS payment application with data encryption by using unique account key and TLS v1.2 to the assessed entity's payment server for card-present transaction. The assessed entity will transmit the received cardholder data to third party payment processors for authorization via the internet (HTTPS with TLS v1.2).

	Once authorization is received, the assessed entity will return the authorization result to merchants via the softPOS payment application. Only truncated PAN (i.e. first 6 and last 4 digits of PAN) and encrypted PAN are securely stored in the database with AES 256-bit. All other cardholder data and sensitive authentication data will be purged after authorization.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The assessed entity provides SoftPOS solution to merchants. Merchants can install the SoftPOS payment application on their smart phones to accept contactless payments. The development process and the security of the application may impact the security of its customers' account data.
Describe system components that could impact the security of account data.	The following system components related to the credit card managed services could impact the security of account data: ▪ SoftPOS payment application ▪ Databases ▪ Network security controls ▪ Intrusion Protection System

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 following items were covered by this assessment: People: ▪ Product Team ▪ Cybersecurity Team ▪ Network and Infrastructure Team ▪ System Operation Team ▪ Development Team ▪ Database Administrator ▪ Human Resources Processes: ▪ The whole development life cycle for in-scope applications Technologies: ▪ Network connection between CDE and other authorized networks ▪ Critical system components: - In-scope cloud platform - Database - Network security groups and rules - IPS/IDS - Log management system - KMS - WAF - Source code control tool ▪ Application systems: - SoftPOS payment application - MMS portal for payment service providers and merchants Documentation: ▪ Policy, Standard and procedure, etc.
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*
Corporate Office	1	Singapore

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
MineSec MineHades MPoC SDK	2.01.xx	MPoC v1.x	2024-01457.002	2027-05-16
MineSec MineZeus AM Service	-	MPoC v1.x	2024-01457.003	2027-07-08
MineSec MPoC White-Label SoftPOS Solution	2.00.xxx	MPoC v1.x	2024-01457.005	2028-01-22

* 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.

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:
Amazon Web Services, Inc.	Cloud Service Provider

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

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: SoftPOS Solution

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.	The following requirements are not applicable to the assessed entity in this assessment: Requirements 1.2.6 and 2.2.5: There is no insecure service, protocol or port enabled in the in-scope environment. Requirement 1.2.8: There is no configuration for NSC because all the in-scope system components are hosted on Cloud computing platform. Requirements 1.3.3, 2.3.1, 2.3.2, 4.2.1.2 and 11.2.2: There is no wireless network connected to CDE. Requirements 3.3.2 and 3.3.3: SAD is not stored before or after authorization. Requirement 3.5.1.1: The assessed entity does not use hash to render PAN unreadable. Requirements 3.5.1.2 and 3.5.1.3: Disk-level or partition-level encryption is not used to render PAN unreadable. Requirement 3.6.1.3 and 3.7.6: There is no manual cleartext cryptographic key-management operation. Requirement 3.7.9: The assessed entity does not share cryptographic keys with its customers for transmission or storage of account data. Requirements 2.2.3, 5.2.1, 5.2.2, 5.2.3, 5.2.3.1, 5.3.1, 5.3.2, 5.3.2.1, 5.3.3, 5.3.4, 5.3.5, 10.6.1, 10.6.2 and 11.5.2: The assessed entity is using serverless cloud service. There is no server in the assessment scope. Requirements 6.4.1 and 10.7.1 : These PCI DSS Requirements were superseded by other Requirements from March 31, 2025. Requirements 6.4.3 and 11.6.1: The assessed entity does not maintain any payment page in the assessment scope. Requirements 6.5.2, 11.3.1.3 and 11.3.2.1: There is no significant change occurred during the audit period. Requirements 7.2.5 and 7.2.5.1 : There is no application or system account in use. Requiremetn 8.2.2 : No shared or generic user account in use. Requirement 8.2.3: The assessed entity does not have any remote access to customer premises. Requirement 8.2.7 - No user account created for third party. Requirements 8.3.10 and 8.3.10.1: The assessed entity does not provide customer user to access to account data. Requirement 8.3.11 : There is no other authentication factor in use to gain access to cardholder data. Requirements 8.6.1, 8.6.2 and 8.6.3 : No interactive login functionalities available in AWS Requirements 9.1.1, 9.1.2, 9.2.1, 9.2.1.1, 9.2.2, 9.3.1, 9.2.3, 9.2.4, 9.3.1, 9.3.1.1, 9.3.2, 9.3.3, 9.3.4 and 11.2.1: All system components are hosted in cloud platform and the cloud service provider is complied with PCI DSS.

	Requirements 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.3, 9.4.4, 9.4.5, 9.4.5.1, 9.4.6 and 9.4.7: There is no media for cardholder data storage. Requirements 9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1 and 9.5.1.3: There is no payment card capturing device in the assessment scope. Requirement 10.6.3 : No internal NTP Server in use in AWS. Requirement 11.4.7 and Appendix A1: The assessed entity is not a multi-tenant service provider that allowing customer to access its own cardholder data and CDE. Requirement 12.3.2: The assessed entity does not use customized approach to meet any PCI DSS requirement. Appendix A2: No SSL/early TLS is identified in use on the assessed entity offering services.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	Not Applicable

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.*	2025-12-23
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2026-03-26
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 *(Date of Report as noted in the ROC 2026-03-26)*.

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 MineSec Pte Ltd. 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

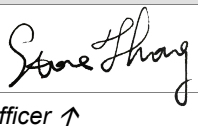
Part 3. PCI DSS Validation *(continued)*

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

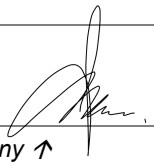


Signature of Service Provider Executive Officer ↑	Date: 2026-03-26
Service Provider Executive Officer Name: Stone Zhong	Title: CTO

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: 2026-03-26
Lead QSA Name: Stephen (Fu Hang) WONG	



Signature of Duly Authorized Officer of QSA Company ↑	Date: 2026-03-26
Duly Authorized Officer Name: Joseph Lee	QSA Company: Evolution Limited

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/