Payment Card Industry
Data Security Standard

ASTROHMS
Hospitality Management Software

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: Mallorca Software Hotelero, S.L.

Date of Report as noted in the Report on Compliance: 16 Jan 2026

Date Assessment Ended: 16 Jan 2026

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:	Mallorca Software Hotelero, S.L.
DBA (doing business as):	Astro Hotel (AstroHMS)
Company mailing address:	Carrer Galileo Galilei, 2, Oficina 16, Parc Bit, 07121. Palma, Spain
Company main website:	https://astrohms.com/
Company contact name:	Fernando Romera
Company contact title:	CEO
Contact phone number:	+34 971439943
Contact e-mail address:	fromera@astrohotel.es
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):	N/A
Qualified Security Assessor	
Company name:	A2Secure Technologias Informatica, Sociedad Ltd.
Company mailing address:	Avda. Francesc Cambó 21, 10. Barcelona.
Company website:	www.a2secure.com
Lead Assessor name:	Miquel Casasayas
Assessor phone number:	+34 933945601
Assessor e-mail address:	miquel.casasayas@a2secure.com
Assessor certificate number:	PCI DSS QSA (206-455)

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:	AstroHMS demo 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):
☐ 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): N/A		

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:	All Astro Hotel 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:	All Astro Hotel services not specifically listed above have been excluded as they are not within the present PCI DSS scope. Other developments and services offered by Astro Hotel other than the AstroHMS demo solution have not been evaluated, as they are not included in the scope of this PCI DSS 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.	Astro Hotel is a service provider that creates customized solutions for its clients, with a particular focus on the hotel sector. Among these developments, Astro Hotel has developed **AstroHMS**, an all-in-one platform for managing hotel establishments via web, which includes PMS, booking engine, Channel Manager, and other key modules for managing these establishments.

	AstroHMS processes, transmits and stores cardholder data to provide the services to customers of the solution. It should be noted that the assessment covers the AstroHMS platform and its online payment channels (e-commerce solution). Other payment methods, such as point-of-sale terminals managed directly by hotel customers, are not included in this assessment. The evaluation performed under this scope **applies exclusively to the AstroHMS demo environment** (https://demo.astrohms.com/). AstroHMS has indicated that this demo environment is aligned with the standardized processes and security controls intended for the Production environment.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	The PCI DSS environment is hosted in a dedicated account in Amazon Web Services (AWS) and covers three different payment methods/flows: **1. Reservations or payments via Virtual POS:** • The final guest accesses the booking engine (website managed by AstroHMS) of the hotel/apartment where they wish to stay and proceeds to make a reservation. • Once the guest selects the dates and proceeds to make the payment, there is a redirect to the Redsys payment provider, so that the guest enters their card details and travel directly from their browser to Redsys. • Under this channel, card details are not received, transmitted, or stored by the AstroHMS infrastructure**.** **2. Reservations through OTAs:** • The guests make reservations on OTAs (such as Booking or Expedia) and make a reservation at the hotel/apartment where they want to stay. • OTAs send booking information along with customer card details via HTTPS on port 443 through associated web services so that card details can then be stored in encrypted form on the AWS RDS managed service. • To collect payments associated with these reservations, AstroHMS integrates with payment gateways (e.g., Redsys, Paytef, Ecopaynet) or with the acquiring bank, and the reservation payment is made. It should be noted that the payment gateways are contracted by the AstroHMS customers. AstroHMS does not have a direct contractual relationship with them. **3. Reservations through hotel Call Centers:** • The final guest calls the hotel's Call Center service (AstroHMS customer) to make a reservation through that service. It should be noted that the call center agent is not an employee of AstroHMS; the agent is employed by the hotel itself. AstroHMS only provides the technological infrastructure to manage the associated reservation. • The hotel agent logs into AstroHMS and manages the reservation. Once the guest has indicated their destination and personal details, they must provide their card details to the hotel call center agent in order to complete the reservation.

	• AstroHMS displays a form to capture the guest's card details via the web service. The guest dictates the card details and the call center agent enters them into the web form displayed so that, after 15 days, the reservation payment is made through the integrated payment gateways. • In the same way as the previous flow, the card details are stored in encrypted form on the AWS RDS managed service. • *NOTE: In some cases, the Call Center agent can use Redsys' PayGold (Pay-By-Link) service to allow guests to make payment before arrival. With this service, the agent sends a payment link via email through PayGold (Redsys). The customer accesses the link, enters their card details, and the information is transmitted directly to Redsys, without going through AstroHMS.* In relation to stored cardholder data, the following considerations are taken into account: • Cardholder data is stored in AWS RDS in encrypted form using cryptographic keys managed through the AWS KMS service. It should be noted that, in particular cases, the CVV is also stored encrypted. The CVV is never stored after transaction authorization. • AstroHMS has defined automatic jobs whereby stored cardholder data is securely deleted after exceeding the defined retention period (60 days after checkout, configurable by the customer (hotel)), with only the last 4 digits of the PAN remaining visible.
Describe system components that could impact the security of account data.	The AstroHMS solution is hosted entirely on Amazon Web Services (AWS) in a specific account. In this sense, the resources and technologies used are, among others: • AWS Load Balancer as a proxy and load balancer for AstroHMS web applications and services. • AWS WAF to protect web applications and respond to common attack patterns. • Amazon Elastic Kubernetes Service (EKS), which manages the shared Kubernetes cluster where worker nodes run workloads belonging to different customers. • AWS RDS as a managed database where card data is stored in encrypted form using cryptographic keys managed by the AWS KMS service. • AWS IAM service is used to manage identities and access to AWS resources and services. • AWS CloudTrail and AWS CloudWatch are used to monitor the infrastructure, log events and generate alerts based on these events. • Amazon Inspector as a service for managing internal vulnerabilities. • AWS Systems Manager Session Manager for secure access to EKS cluster instances/nodes.

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 PCI DSS environment is hosted on AWS. All cardholder data processed by AstroHMS and transmitted to the payment gateways (contracted by the clients) are encrypted and sent via HTTPS protocol. The AstroHMS solution is hosted entirely on Amazon Web Services (AWS) in a specific account. In this sense, the resources and technologies used are, among others: • AWS Load Balancer as a proxy and load balancer for AstroHMS web applications and services. • AWS WAF to protect web applications and respond to common attack patterns. • Amazon Elastic Kubernetes Service (EKS), which manages the shared Kubernetes cluster where worker nodes run workloads belonging to different customers. • AWS RDS as a managed database where card data is stored in encrypted form using cryptographic keys managed by the AWS KMS service. • AWS IAM service is used to manage identities and access to AWS resources and services. • AWS CloudTrail and AWS CloudWatch are used to monitor the infrastructure, log events and generate alerts based on these events. • Amazon Inspector as a service for managing internal vulnerabilities. • AWS Systems Manager Session Manager for secure access to EKS cluster instances/nodes.
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*
Astro Hotel Offices	1	Carrer Galileo Galilei, 2, Oficina 16, Parc Bit, 07121. Palma, Spain

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
N/A	N/A	N/A	N/A	N/A

* 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	Hosting 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: AstroHMS demo 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.	1.2.6: There are no insecure services, ports, or protocols. 1.3.3: There are no wireless networks within the PCI DSS scope. 2.2.5: There are no insecure services, ports, or protocols. 2.3.1: AstroHMS does not have wireless networks within the PCI-DS scope. 2.3.2: AstroHMS does not have wireless networks within the PCI-DS scope. 3.3.3: AstroHMS is not an issuer or a company that supports these services. 3.5.1.c: AstroHMS does not use hashing methods to store the PAN. 3.5.1.1: AstroHMS does not use hashing methods to store the PAN. 3.7.6: Cryptographic values are not managed in clear text 3.7.9: AstroHMS does not share cryptographic keys with its clients. 4.2.1.2: There are no wireless networks within the PCI DSS scope. 4.2.2: AstroHMS does not allow the use of end-user messaging technologies to transmit card data. 5.2.1.a: The systems are classified as systems not commonly affected by malware. 5.2.2: The systems are classified as systems not commonly affected by malware. 5.3.1, 5.3.2, 5.3.2.1: AstroHMS has not deployed systems commonly affected by malware on the PCI-DSS platform. 5.3.3, 5.3.4, 5.3.5: The systems are classified as not commonly affected by malware. 6.5.1 6.5.2: There are no significant changes (this is the first PCI DSS assessment) 7.2.3: It has been verified that there have been no additions or removals in the last year (this is the first PCI DSS assessment). 8.2.3: AstroHMS does not have remote access to the clients' PCI DSS environments. 8.2.4, 8.2.5: There are no addition, modification or termination of users as this is the first PCI DSS assessment. 8.2.7: There are no third-party accounts with remote access to the AstroHMS PCI DSS infrastructure. 8.3.9: AstroHMS uses more than one authentication factor for user access. 8.3.11: AstroHMS does not have physical authentication factors 8.6.1, 8.6.2, 8.6.3: There are no application or system accounts that can be used for interactive login. 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, 9.4.7: AstroHMS does not store card data on paper or external media.

	9.5.1, 9.5.1.1, 9.5.1.2, 9.5.1.2.1, 9.5.1.3: AstroHMS does not directly use physical card data reading devices (POS terminals) of the POI, POS, or any other type. 10.4.2.1: There are no other system components that are out of the log reviews. 10.7.2.b, 10.7.3.b: The organization confirms that it has not experienced any failures in critical security control systems (this is the first PCI DSS assessment). 11.3.1.2.c, 11.3.1.2.d: The vulnerability scans are managed via AWS Inspector and there are no accounts used for the management of the authenticated scans. 11.3.1.3, 11.3.2.1: This is the first evaluation (there are no significant changes). 11.4.5, 11.4.6: The PCI DSS environment is located exclusively in a dedicated AWS account. 11.4.7: AstroHMS is not a multi-tenant service provider. 12.3.2: AstroHMS does not use the customized approach. 12.5.3: There were no significant changes to organizational structure as this is the first evaluation.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	N/A

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.*	24 Sep 2025
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	16 Jan 2026
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 16 Jan 2026)*
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 Mallorca Software Hotelero, S.L. 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: 16 Jan 2026
Service Provider Executive Officer Name: Fernando Romera	Title: CEO

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: *QSA has assisted with knowledge on PCI DSS and consultancy on how to interpret requirements*

Signature of Lead QSA ↑	Date: 16 Jan 2026
Lead QSA Name: Miquel Casasayas (QSA Certificate Number: 206-455)	

Signature of Duly Authorized Officer of QSA Company ↑	Date: 16 Jan 2026
Duly Authorized Officer Name: Albert Morell (QSA Certificate Number: 203-790)	QSA Company: A2Secure Technologias informatica, Sociedad 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:

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/