



Payment Card Industry Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Revision 2

Publication Date: August 2024

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

Entity Name: Linkly Technologies Pty Ltd

Assessment End Date: 2025-03-24

Date of Report as noted in the Report on Compliance: 2025-03-28

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:	Linkly Technologies Pty Ltd
DBA (doing business as):	Linkly
Company mailing address:	Level 8, 401 Collins Street Melbourne Victoria 3000 Australia
Company main website:	https://linkly.com.au
Company contact name:	Leron Zinatullin
Company contact title:	Chief Information Security Officer
Contact phone number:	+61 1300 697 848
Contact e-mail address:	info@linkly.com.au

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:	Foregenix Ltd
Company mailing address:	1 Watts Barn Badbury Swindon Wiltshire

	SN4 0EU United Kingdom
Company website:	https://www.foregenix.com
Lead Assessor name:	Sylvia Choa
Assessor phone number:	+61 412 961 415
Assessor e-mail address:	schoa@foregenix.com
Assessor certificate number:	PCI QSA (201-108), PCI QPA (1300-209)

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: Payment Gateway (including MerchantSuite, VicRoads and BPOINT)

Type of service(s) assessed:

Hosting Provider:

- ☐ Applications / software
- ☐ Hardware
- ☐ Infrastructure / Network
- ☐ Physical space (co-location)
- ☐ Storage
- ☐ Web
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):
Not Applicable

Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):
Not Applicable

Payment Processing:

- ☐ POS / card present
- ☒ Internet / e-commerce
- ☒ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):
Not Applicable

<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input checked="" type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input checked="" type="checkbox"/> Billing Management	<input type="checkbox"/> Loyalty Programs	<input type="checkbox"/> Records Management
<input type="checkbox"/> Clearing and Settlement	<input type="checkbox"/> Merchant Services	<input type="checkbox"/> Tax/Government Payments
<input type="checkbox"/> Network Provider		

☐ Others (specify): Not Applicable

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
- ☐ Security services
- ☐ 3-D Secure Hosting Provider
- ☐ Shared Hosting Provider
- ☐ Other Hosting (specify):
Not Applicable

Managed Services (specify):

- ☐ Systems security services
- ☐ IT support
- ☐ Physical security
- ☐ Terminal Management System
- ☐ Other services (specify):
Not Applicable

Payment Processing:

- ☐ POS / card present
- ☐ Internet / e-commerce
- ☐ MOTO / Call Center
- ☐ ATM
- ☐ Other processing (specify):
Not Applicable

☐ 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): Not Applicable

Provide a brief explanation why any checked services were not included in the Assessment:

Not Applicable

Part 2b. Description of Role with Payment Cards (ROC Section 2.1)

Describe how the business stores, processes, and/or transmits account data.

Linkly Technologies Pty Ltd (hereafter referred to as Linkly) is a payment gateway service provider for merchants to receive payments through online and interactive voice response (IVR) channels. As part of the web-based and IVR (via Secure Call Interface - SCI) solution, Linkly facilitates merchants in accepting credit card details for payment processing.

Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.

As a payment gateway, Linkly receives authorisation requests containing CHD (PAN, expiry, name, and CV2) from their client's customers via web (e-commerce) or via SIP (IVR) and then sends the authorisation requests to the fraud detection providers, who return a response ("accept", "deny", or a challenge) without any CHD. Finally, the authorisation request is sent to the payment processors and the response from the payment processors which does not contain any CHD is sent back to the customer via Linkly.

These are the card-not-present (CNP) transaction types supported by Linkly:

- Payment: Authorisation requests on behalf of Linkly's clients. Fraud detection services are optionally included in this process.
- Preauth: Pre-authorisation requests to reserve a certain amount of money.
- Capture: In Linkly's context, capture is the process to take up to the pre-authorised amount.
- Reversal or Void: Process to void a transaction before it is settled, normally within the same day.
- Refund: Process to reverse a transaction after it was settled and within a period of twelve months.
- Credit: These transactions require the cardholder's details to send the money back to its account.
- Zero Dollar Authentication: Used by merchants to verify that card details are valid. Requires PAN, expiry, and CV2.
- 3DS2 Payer Authentication: An additional payer authentication flow, depending on the value of the transaction and the risk. It is not driven by third-party processes.
- Bank Account Payment and Rejection (not available on SMEs): Payments related with bank account numbers not related to credit or debit cards
- Tokenization: A 16-digit number following the Luhn algorithm, There is no mathematical relation between the PAN and the token.
- Recurring payments: Periodic payments on behalf of a Linkly's client. This process stores the token and not the PAN. When the

	payments are requested, the token is converted to the PAN to send the authorisation request.
Describe system components that could impact the security of account data.	Not Applicable

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.*

Linkly is using physical location segregation and firewalls to isolate the CDE from the networks out-of-scope. These out of scope networks are not permitted to transmit or receive information to or from the CDE networks.

All the corporate network is out of scope. This network is physically segmented from the CDE as there are no direct connections between the corporate office and the data centers. The only option to connect to systems located in the data center is via a VPN requiring an authorised user (only system administrators) and multi-factor authentication (MFA).

In the data centers, there are VLANs considered out of scope. The Fortinet firewall is implementing the isolation of these networks by restricting the traffic between these VLANs and the CDE.

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)
<i>Example: Data centers</i>	3	<i>Boston, MA, USA</i>
Data Center ME1 (Equinix)	1	Melbourne, Victoria, Australia
Data Center SY4 (Equinix)	1	Sydney, New South Wales, Australia

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
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

* 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)) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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) | <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No |
| • Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers). | <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |

If Yes:

Name of Service Provider:	Description of Services Provided:
ACI Worldwide Corp. and Affiliates	Fraud prevention for BPOINT
Equinix, Inc	Data center provider (co-location)
Mastercard, Inc.	Payment gateway for CBA
Microsoft Corporation – Microsoft Azure	Audit logs storage
Qvalent Pty Ltd	Payment gateway for Westpac
Amazon Web Services, Inc.	Used by Keeper to provide Keeper Password Manager Used for DNS - Route 53

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: Payment Gateway (including MerchantSuite, VicRoads and BPOINT)

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If Below Method(s) Was Used	
	In Place	Not Applicable	Not Tested	Not in Place	Customized Approach	Compensating Controls
Requirement 1:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 3:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 5:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 7:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Requirement 9:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 10:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Appendix A2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.

1.3.3 - Not Applicable.
The assessor verified by interview with P-1 and review of the network diagram (DOC-38) that confirm that no wireless connection was permitted between the wireless environment and the CDE.

2.3.1 - Not Applicable.
Linkly have no wireless networks connecting to the CDE. The assessor verified this by interview with P-14 and review of network diagram (DOC-38).

2.3.2 - Not Applicable.
Linkly have no wireless networks connecting to the CDE. The assessor verified this by interview with P-14 and review of network diagram (DOC-38).

3.3.1.1 - Not Applicable.
The assessor verified by interview with P-3 and confirmed that track data is not received by Linkly.

3.3.1.3 - Not Applicable.
The assessor verified by interview with P-3 and confirmed that PIN and the PIN block are not received by Linkly.

3.3.3 - Not Applicable.
Linkly is neither an issuer nor supports issuing services.

3.4.1 - Not Applicable.
The assessor verified by interview with P-3 and confirmed that Linkly only stores truncated PAN and encrypted CHD, no masked PAN exists.

3.4.2 - Not Applicable.
This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.

3.5.1.1 - Not Applicable.
The assessor verified by interview and review of cardholder data stores that hashing is not used to render the PAN unreadable. Encryption and truncation are used.

3.5.1.2 - Not Applicable.
Disk or partition-level encryption is not used to render PAN unreadable. Column-level database encryption is used.

3.5.1.3 - Not Applicable.
Disk or partition-level encryption is not used to render PAN unreadable. The assessor verified this by interview with P-3 and confirmed that Linkly only uses column-level database encryption.

3.6.1.3 - Not Applicable.
Linkly does not use clear text key components. The assessor verified this by interview with P-3 and review of cryptographic key processes.

3.7.2 - Not Applicable.
The assessor confirmed through interview with P-3 and P-14 that encryption keys are exclusively stored in the HSM and are never distributed to other systems or locations.

3.7.6 - Not Applicable.
There are no manual cleartext cryptographic key-management operations within Linkly because key exchange is managed through asymmetric techniques. Based on the HSM design, the

	<p>DEK is never in cleartext outside the HSM and the HSM enforces dual control for any operations that can export the cleartext key components.</p> <p>3.7.9 - Not Applicable.</p> <p>The assessor interviewed P-3 and P-14 and confirmed that the DEK is never shared under any circumstances.</p> <p>4.2.1.2 - Not Applicable.</p> <p>Wireless networks are not used to transmit cardholder data or to connect to the CDE. The assessor verified this by interview with P-14 and review of network diagram (DOC-38).</p> <p>4.2.2 - Not Applicable.</p> <p>End-user technologies are not used to transmit cardholder data. The assessor verified this by interview with P-14 and review of network diagram (DOC-38).</p> <p>5.2.3 - Not Applicable.</p> <p>The assessor reviewed the software inventory, observed in the anti-malware solution the managed systems, and confirmed that the antimalware agent is deployed on all the applicable system components, including both Windows and Linux system components.</p> <p>5.2.3.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>5.3.2.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>5.3.3 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>5.4.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>6.4.2 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>6.4.3 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>6.5.6 - Not Applicable.</p> <p>The assessor verified through interview with P-6 and review of the deployment and release process, that there is no data transfer that is part of the release process. It was also verified that at no time are test accounts present in the pre-production components.</p> <p>7.2.4 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p>
--	--

	<p>7.2.5 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>7.2.5.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>8.2.3 - Not Applicable.</p> <p>Linkly does not have remote access to customer premises. The assessor verified this by interview with P-8.</p> <p>8.2.7 - Not applicable.</p> <p>The assessor verified by interview with P-8 and review of user accounts in the Sample Set-1 that no third parties have access to the CDE.</p> <p>8.3.10 - Not Applicable.</p> <p>Customers do not have access to cardholder data. This assessor verified this by interview with P-1.</p> <p>8.3.10.1 - Not Applicable.</p> <p>Customers do not have access to cardholder data. This assessor verified this by interview with P-1.</p> <p>8.5.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>8.6.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>8.6.3 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>9.4.1.1 - Not Applicable.</p> <p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.4.1.2 - Not Applicable.</p> <p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.4.2 - Not Applicable.</p> <p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.4.3 - Not Applicable.</p> <p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.4.4 - Not Applicable.</p> <p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.4.5 - Not Applicable.</p> <p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.4.5.1 - Not Applicable.</p>
--	--

	<p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.4.6 - Not Applicable.</p> <p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.4.7 - Not Applicable.</p> <p>No backup tapes or offline media backup exist or are stored at the Equinix ME-1 or SY4 data centers.</p> <p>9.5.1 - Not Applicable.</p> <p>POI devices are not used by Linkly. The assessor verified this by interview with P-1 and review of the Linkly asset inventories.</p> <p>9.5.1.1 - Not Applicable.</p> <p>POI devices are not used by Linkly. The assessor verified this by interview with P-1 and review of the Linkly asset inventories.</p> <p>9.5.1.2 - Not Applicable.</p> <p>POI devices are not used by Linkly. The assessor verified this by interview with P-1 and review of the Linkly asset inventories.</p> <p>9.5.1.2.1 - Not Applicable.</p> <p>POI devices are not used by Linkly. The assessor verified this by interview with P-1 and review of the Linkly asset inventories.</p> <p>9.5.1.3 - Not Applicable.</p> <p>POI devices are not used by Linkly. The assessor verified this by interview with P-1 and review of the Linkly asset inventories.</p> <p>10.4.2.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>10.7.2 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>10.7.3 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>11.2.2 - Not Applicable.</p> <p>Linkly does not have any authorised wireless access point in the data centers. The assessor verified this by interview with P-11 and review of network diagrams.</p> <p>11.3.1.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>11.3.1.2 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>11.4.7 - Not Applicable.</p> <p>The assessor reviewed the business functions provided by Linkly and determined that it is not a multi-tenant service provider.</p> <p>11.5.1.1 - Not Applicable.</p>
--	--

	<p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>11.6.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.3.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.3.2 - Not Applicable.</p> <p>The assessor validated all the requirements within this report and verified with P-12 that Linkly does not use the customised approach to meet any of the PCI DSS requirements.</p> <p>12.3.3 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.3.4 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.5.2.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.5.3 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.6.3.2 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.10.4.1 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.10.5 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>12.10.7 - Not Applicable.</p> <p>This requirement is considered a best practice until 31 March, 2025. Linkly is actively working towards achieving compliance of this requirement by this deadline.</p> <p>A1.1.1 - Not Applicable.</p> <p>The assessor reviewed the business functions provided by Linkly and determined that the company is not a multi-tenant service provider.</p> <p>A1.1.2 - Not Applicable.</p>
--	--

	<p>The assessor reviewed the business functions provided by Linkly and determined that the company is not a multi-tenant service provider.</p> <p>A1.1.3 - Not Applicable.</p> <p>The assessor reviewed the business functions provided by Linkly and determined that the company is not a multi-tenant service provider.</p> <p>A1.1.4 - Not Applicable.</p> <p>The assessor reviewed the business functions provided by Linkly and determined that the company is not a multi-tenant service provider.</p> <p>A1.2.1 - Not Applicable.</p> <p>The assessor reviewed the business functions provided by Linkly and determined that the company is not a multi-tenant service provider.</p> <p>A1.2.2 - Not Applicable.</p> <p>The assessor reviewed the business functions provided by Linkly and determined that the company is not a multi-tenant service provider.</p> <p>A1.2.3 - Not Applicable.</p> <p>The assessor reviewed the business functions provided by Linkly and determined that the company is not a multi-tenant service provider.</p> <p>A2.1.1 - Not Applicable.</p> <p>The assessor reviewed software and hardware inventory and found no POI terminals in-scope.</p> <p>A2.1.2 - Not Applicable.</p> <p>The assessor reviewed software and hardware inventory and found no POI terminals in-scope.</p> <p>A2.1.3 - Not Applicable.</p> <p>The assessor reviewed software and hardware inventory and found no POI terminals in-scope.</p>
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 1.3.2)

Date Assessment began: Note: <i>This is the first date that evidence was gathered, or observations were made.</i>	2025-02-03
Date Assessment ended: Note: <i>This is the last date that evidence was gathered, or observations were made.</i>	2025-03-24
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any testing activities performed remotely?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> 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 2025-03-28)*.

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*):

<input checked="" type="checkbox"/>	<p>Compliant: All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall COMPLIANT rating; thereby Linkly Technologies Pty Ltd has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.</p>				
<input type="checkbox"/>	<p>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 Linkly Technologies Pty Ltd has not demonstrated compliance with PCI DSS requirements.</p> <p>Target Date for Compliance:</p> <p>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.</p>				
<input type="checkbox"/>	<p>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 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall COMPLIANT BUT WITH LEGAL EXCEPTION rating; thereby Linkly Technologies Pty Ltd 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.</p> <p>This option requires additional review from the entity to which this AOC will be submitted.</p> <p><i>If selected, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement from being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement from being met		
Affected Requirement	Details of how legal constraint prevents requirement from being met				

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

<input checked="" type="checkbox"/>	The ROC was completed according to <i>PCI DSS</i> , Version 4.0.1 and was completed according to the instructions therein.
<input checked="" type="checkbox"/>	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
<input checked="" type="checkbox"/>	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Leron Zinatullin

Signature of Service Provider Executive Officer ↑	Date: 28-MAR-2025
Service Provider Executive Officer Name: Leron Zinatullin	Title: Chief Information Security Officer

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: Completion of the ROC.

Sylvia Choa

Signature of Lead QSA ↑	Date: 28-MAR-2025
Lead QSA Name: Sylvia Choa	

Daniel Farr

Signature of Duly Authorized Officer of QSA Company ↑	Date: 28-MAR-2025
Duly Authorized Officer Name: Daniel Farr	QSA Company: Foregenix 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: Not Applicable

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	<input type="checkbox"/>	<input type="checkbox"/>	
2	Apply secure configurations to all system components	<input type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored account data	<input type="checkbox"/>	<input type="checkbox"/>	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	<input type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems and networks from malicious software	<input type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and software	<input type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to system components and cardholder data by business need to know	<input type="checkbox"/>	<input type="checkbox"/>	
8	Identify users and authenticate access to system components	<input type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
10	Log and monitor all access to system components and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>	
11	Test security systems and networks regularly	<input type="checkbox"/>	<input type="checkbox"/>	
12	Support information security with organizational policies and programs	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	<input type="checkbox"/>	<input type="checkbox"/>	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	<input type="checkbox"/>	<input type="checkbox"/>	

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/