



# **Payment Card Industry (PCI) Data Security Standard**

---

## **Attestation of Compliance for Onsite Assessments – Service Providers**

**Version 3.2.1**

June 2018



## Section 1: Assessment Information

### Instructions for Submission

This Attestation of Compliance must be completed as a declaration of the results of the service provider's assessment with the *Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS)*. Complete all sections: The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the requesting payment brand for reporting and submission procedures.

### Part 1. Service Provider and Qualified Security Assessor Information

#### Part 1a. Service Provider Organization Information

Company Name:	Huge Connect (Pty) Ltd.	DBA (doing business as):	Huge Connect (Pty) Ltd.		
Contact Name:	Mark Fenner	Title:	Network Specialist		
Telephone:	+27 87 820 0220	E-mail:	mark@hugeconnect.co.za		
Business Address:	2nd Floor, 267 West Building, 267 West Avenue, Centurion.	City:	Pretoria		
State/Province:	Gauteng	Country:	South Africa	Zip:	0157
URL:	<a href="https://hugeconnect.co.za/">https://hugeconnect.co.za/</a>				

#### Part 1b. Qualified Security Assessor Company Information (if applicable)

Company Name:	Risk X Data Assurance (Pty) Ltd.				
Lead QSA Contact Name:	Christine Fernandez	Title:	Senior Consultant		
Telephone:	+27 (0) 67 424 3597	E-mail:	christine.fernandez@risk-x.co.za		
Business Address:	11 Imam Haron Road, Claremont.	City:	Cape Town		
State/Province:	Western Cape	Country:	South Africa	Zip:	7708
URL:	<a href="https://www.risk-x.co.za">https://www.risk-x.co.za</a>				



## Part 2. Executive Summary

### Part 2a. Scope Verification

**Services that were INCLUDED in the scope of the PCI DSS Assessment (check all that apply):**

Name of service(s) assessed:	Network provider	
Type of service(s) assessed:		
<b>Hosting Provider:</b> <input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<b>Managed Services (specify):</b> <input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<b>Payment Processing:</b> <input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input 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 checked="" type="checkbox"/> Network Provider		
<input type="checkbox"/> Others (specify):		

**Note:** These categories are provided for assistance only, and are not intended to limit or predetermine an entity's service description. If you feel these categories don't apply to your service, complete "Others." If you're unsure whether a category could apply to your service, consult with the applicable payment brand.


**Part 2a. Scope Verification (continued)**
**Services that are provided by the service provider but were NOT INCLUDED in the scope of the PCI DSS Assessment (check all that apply):**

Name of service(s) not assessed: N/A

Type of service(s) not assessed:

<b>Hosting Provider:</b>	<b>Managed Services (specify):</b>	<b>Payment Processing:</b>
<input type="checkbox"/> Applications / software <input type="checkbox"/> Hardware <input type="checkbox"/> Infrastructure / Network <input type="checkbox"/> Physical space (co-location) <input type="checkbox"/> Storage <input type="checkbox"/> Web <input type="checkbox"/> Security services <input type="checkbox"/> 3-D Secure Hosting Provider <input type="checkbox"/> Shared Hosting Provider <input type="checkbox"/> Other Hosting (specify):	<input type="checkbox"/> Systems security services <input type="checkbox"/> IT support <input type="checkbox"/> Physical security <input type="checkbox"/> Terminal Management System <input type="checkbox"/> Other services (specify):	<input type="checkbox"/> POS / card present <input type="checkbox"/> Internet / e-commerce <input type="checkbox"/> MOTO / Call Center <input type="checkbox"/> ATM <input type="checkbox"/> Other processing (specify):
<input type="checkbox"/> Account Management	<input type="checkbox"/> Fraud and Chargeback	<input type="checkbox"/> Payment Gateway/Switch
<input type="checkbox"/> Back-Office Services	<input type="checkbox"/> Issuer Processing	<input type="checkbox"/> Prepaid Services
<input 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		
<input type="checkbox"/> Others (specify):		
Provide a brief explanation why any checked services were not included in the assessment:		N/A

**Part 2b. Description of Payment Card Business**

Describe how and in what capacity your business stores, processes, and/or transmits cardholder data.

Huge Connect (Pty) Ltd, formerly known as ConnectNet Broadband Wireless (Pty) Ltd, is a trusted Level 1 communications service provider since 2004. Huge Connect provides customers with reliable and managed bi-directional Machine to Machine (M2M) and Business to Business (B2B) telecommunication solutions utilising various platforms such as GSM Data, ADSL and point-to-point links. Huge Connect is a provider of reliable telecommunications services, between merchants and their acquiring banks.

According to the PCI DSS Glossary of Terms, Abbreviations and Acronyms v3.2.1: "If an entity provides a service that involves only the provision of public network access - such as a telecommunications company only providing just a communications link - the entity would not be considered a service provider for that service".



	<p>Thus, Huge Connect is not obligated to comply with PCI DSS. However, Huge Connected decided to undergo a PCI DSS assessment.</p> <p>Huge Connect does not store or process any cardholder data. Transmission of cardholder data is performed on the application level by Huge Connect's clients who make use of Huge Connect's network on the data-link layer. Hence, Huge Connect does not transmit any cardholder data but do facilitate the process.</p>
<p>Describe how and in what capacity your business is otherwise involved in or has the ability to impact the security of cardholder data.</p>	<p>Huge Connect does not have the ability to access any cardholder data. Cardholder data is securely transmitted from the client across the Huge Connect network to the acquiring bank on the data-link layer where Huge Connect does not have access to cardholder data. Huge Connect does not store or process any cardholder data.</p>

**Part 2c. Locations**

List types of facilities (for example, retail outlets, corporate offices, data centers, call centers, etc.) and a summary of locations included in the PCI DSS review.

Type of facility:	Number of facilities of this type	Location(s) of facility (city, country):
<i>Example: Retail outlets</i>	3	<i>Boston, MA, USA</i>
Data Centres	2	Teraco - Bredell, Johannesburg, Gauteng, South Africa. Teraco - Isando, Johannesburg, Gauteng, South Africa.
Corporate Office	1	Centurion, Gauteng, South Africa.

**Part 2d. Payment Applications**

Does the organization use one or more Payment Applications?  Yes  No

Provide the following information regarding the Payment Applications your organization uses:

Payment Application Name	Version Number	Application Vendor	Is application PA-DSS Listed?	PA-DSS Listing Expiry date (if applicable)
N/A	N/A	N/A	<input type="checkbox"/> Yes <input type="checkbox"/> No	N/A
			<input type="checkbox"/> Yes <input type="checkbox"/> No	
			<input type="checkbox"/> Yes <input type="checkbox"/> No	



			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No
			<input type="checkbox"/> Yes <input type="checkbox"/> No

**Part 2e. Description of 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 POS devices, databases, web servers, etc., and any other necessary payment components, as applicable.*

Transactions are initiated at the client's premises via Point-of-Sale or handheld PDQ's and delivered over the Huge Connect network infrastructure to the acquiring banks.

Huge Connect does not store or process data packets, but simply routes the packets to their destination. Access to packets at a data-link network level is available via authorised Huge Connect systems only for management and diagnostic purposes.

Huge Connect manages the the data path for the client's payment connection, but does not store or process any of the data. The data is transmitted through a secure tunnel provided by Huge Connect to clients, but Huge Connect does not have visibility of the data itself.

Critical system components include firewalls, routers and switches for data transport, including servers used for controlling the client's devices.

<p>Does your business use network segmentation to affect the scope of your PCI DSS environment?</p> <p><i>(Refer to "Network Segmentation" section of PCI DSS for guidance on network segmentation)</i></p>	<p><input checked="" type="checkbox"/> Yes <input type="checkbox"/> No</p>
---	--



**Part 2f. Third-Party Service Providers**

Does your company have a relationship with a Qualified Integrator & Reseller (QIR) for the purpose of the services being validated?  Yes  No

**If Yes:**

Name of QIR Company: N/A

QIR Individual Name: N/A

Description of services provided by QIR: N/A

Does your company have a relationship with one or more third-party service providers (for example, Qualified Integrator Resellers (QIR), gateways, payment processors, payment service providers (PSP), web-hosting companies, airline booking agents, loyalty program agents, etc.) for the purpose of the services being validated?  Yes  No

**If Yes:**

Name of service provider:	Description of services provided:
Teraco Data Environments (Pty) Ltd.	Data Centre - Physical Hosting

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



## Part 2g. Summary of Requirements Tested

For each PCI DSS Requirement, select one of the following:

- **Full** – The requirement and all sub-requirements of that requirement were assessed, and no sub-requirements were marked as “Not Tested” or “Not Applicable” in the ROC.
- **Partial** – One or more sub-requirements of that requirement were marked as “Not Tested” or “Not Applicable” in the ROC.
- **None** – All sub-requirements of that requirement were marked as “Not Tested” and/or “Not Applicable” in the ROC.

For all requirements identified as either “Partial” or “None,” provide details in the “Justification for Approach” column, including:

- Details of specific sub-requirements that were marked as either “Not Tested” and/or “Not Applicable” in the ROC
- Reason why sub-requirement(s) were not tested or not applicable

**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:		Network Provider		
PCI DSS Requirement	Details of Requirements Assessed			Justification for Approach (Required for all “Partial” and “None” responses. Identify which sub-requirements were not tested and the reason.)
	Full	Partial	None	
Requirement 1:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A - 1.1.3 - Huge Connect do not store or process cardholder data (CHD). Huge Connect provide the secure data transmission of encrypted CHD between merchants and the acquiring banks only.  N/A - 1.2.3 - There are no wireless networks in scope.  N/A - 1.3.6 - Huge Connect do not store or process cardholder data (CHD). Huge Connect provide the secure data transmission of encrypted CHD between merchants and the acquiring banks only.
Requirement 2:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A - 2.1.1 - There are no wireless networks in scope.  N/A - 2.2.3 - No insecure services, daemons or protocols are enabled.  N/A - 2.6 - Huge Connect is not a shared hosting provider.
Requirement 3:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A - Requirement 3 - Huge Connect does not store, process or transmit cardholder data.
Requirement 4:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Requirement 4 - Huge Connect does not store, process or transmit cardholder data. Huge Connect only provides the secure encrypted communications infrastructure for clients to pass traffic between





				<p>entities. Huge Connect do not play any role in the encryption / decryption key management process and can therefore at no time access client cardholder data.</p> <p>N/A - 4.1.1 - There are no wireless networks in scope.</p> <p>N/A - 4.2 - Cardholder data is not sent or received by any means using end-user messaging.</p>
Requirement 5:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 6:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A - 6.3 to 6.6 - Huge Connect does not develop applications that store, process or transmit cardholder data and there are no public facing web applications in scope.
Requirement 7:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Requirement 8:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>N/A - 8.1.5 - Vendors do not have access to the Huge Connect environment.</p> <p>N/A - 8.5.1 - Huge Connect does not have remote access to clients' environments.</p> <p>N/A - 8.7 - Huge Connect does not store, process or transmit cardholder data.</p>
Requirement 9:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A - 9.5 to 9.9.3 - Huge Connect does not store, process or transmit cardholder data. Huge Connect does not own or manage POI devices.
Requirement 10:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A - 10.2.1 - No individual in Huge Connect has access to cardholder data.
Requirement 11:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<p>N/A - 11.1.1 - All cardholder data environment components are hosted at Teraco data centres. There are no wireless adapters installed.</p> <p>N/A - 11.3 to 11.3.4.1 - Due to Huge Connect not storing, processing or transmitting cardholder data, penetration testing is not required.</p> <p>N/A - 11.4 - Huge Connect does not store, process or transmit cardholder data.</p>
Requirement 12:	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	N/A - 12.3.9 to 12.3.10 - Huge Connect does not store, process or transmit cardholder data.
Appendix A1:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A - Huge Connect is not a shared hosting provider.
Appendix A2:	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	N/A - Huge Connect does not make use of early TLS or SSL.



## Section 2: Report on Compliance

---

This Attestation of Compliance reflects the results of an onsite assessment, which is documented in an accompanying Report on Compliance (ROC).

The assessment documented in this attestation and in the ROC was completed on:	1 August 2022
Have compensating controls been used to meet any requirement in the ROC?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC identified as being not applicable (N/A)?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Were any requirements not tested?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Were any requirements in the ROC unable to be met due to a legal constraint?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No



## Section 3: Validation and Attestation Details

### Part 3. PCI DSS Validation

This AOC is based on results noted in the ROC dated 1 August 2022.

Based on the results documented in the ROC noted above, the signatories identified in Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (**check one**):

<input checked="" type="checkbox"/>	<p><b>Compliant:</b> All sections of the PCI DSS ROC are complete, all questions answered affirmatively, resulting in an overall <b>COMPLIANT</b> rating; thereby Huge Connect (Pty) Ltd has demonstrated full compliance with the PCI DSS.</p>						
<input type="checkbox"/>	<p><b>Non-Compliant:</b> Not all sections of the PCI DSS ROC are complete, or not all questions are answered affirmatively, resulting in an overall <b>NON-COMPLIANT</b> rating, thereby <i>(Service Provider Company Name)</i> has not demonstrated full compliance with the PCI DSS.</p> <p><b>Target Date</b> for Compliance:</p> <p>An entity submitting this form with a status of Non-Compliant may be required to complete the Action Plan in Part 4 of this document. <i>Check with the payment brand(s) before completing Part 4.</i></p>						
<input type="checkbox"/>	<p><b>Compliant but with Legal exception:</b> One or more requirements are marked "Not in Place" due to a legal restriction that prevents the requirement from being met. This option requires additional review from acquirer or payment brand.</p> <p><i>If checked, complete the following:</i></p> <table border="1"> <thead> <tr> <th>Affected Requirement</th> <th>Details of how legal constraint prevents requirement being met</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Affected Requirement	Details of how legal constraint prevents requirement being met				
Affected Requirement	Details of how legal constraint prevents requirement being met						

### Part 3a. Acknowledgement of Status

Signatory(s) confirms:

**(Check all that apply)**

<input checked="" type="checkbox"/>	The ROC was completed according to the <i>PCI DSS Requirements and Security Assessment Procedures</i> , Version 3.2.1, 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 my assessment in all material respects.
<input type="checkbox"/>	I have confirmed with my payment application vendor that my payment system does not store sensitive authentication data after authorization.
<input checked="" type="checkbox"/>	I have read the PCI DSS and I recognize that I must maintain PCI DSS compliance, as applicable to my environment, at all times.
<input checked="" type="checkbox"/>	If my environment changes, I recognize I must reassess my environment and implement any additional PCI DSS requirements that apply.



### Part 3a. Acknowledgement of Status (continued)

- No evidence of full track data<sup>1</sup>, CAV2, CVC2, CID, or CVV2 data<sup>2</sup>, or PIN data<sup>3</sup> storage after transaction authorization was found on ANY system reviewed during this assessment.
- ASV scans are being completed by the PCI SSC Approved Scanning Vendor Hacker Guardian

### Part 3b. Service Provider Attestation

DocuSigned by:

D6C291C41E01406...

Signature of Service Provider Executive Officer ↑

Date: 1 August 2022

Service Provider Executive Officer Name: Louis Antunes

Title: Network Executive

### Part 3c. Qualified Security Assessor (QSA) Acknowledgement (if applicable)

If a QSA was involved or assisted with this assessment, describe the role performed:

The QSA performed a full remote assessment of the PCI DSS requirements applicable to the environment and in accordance with the PCI DSS testing procedures.

DocuSigned by:

E5869722BB2140B...

Signature of Duly Authorized Officer of QSA Company ↑

Date: 1 August 2022

Duly Authorized Officer Name: Johan van Zyl

QSA Company: Risk X Data Assurance (Pty) Ltd.

### Part 3d. Internal Security Assessor (ISA) Involvement (if applicable)

If an ISA(s) was involved or assisted with this assessment, identify the ISA personnel and describe the role performed:

N/A

<sup>1</sup> Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full track data after transaction authorization. The only elements of track data that may be retained are primary account number (PAN), expiration date, and cardholder name.

<sup>2</sup> The three- or four-digit value printed by the signature panel or on the face of a payment card used to verify card-not-present transactions.

<sup>3</sup> Personal identification number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.



## Part 4. Action Plan for Non-Compliant Requirements

Select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement. If you answer “No” to any of the requirements, you may be required to provide the date your Company expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

*Check with the applicable payment brand(s) before completing Part 4.*

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 a firewall configuration to protect cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
2	Do not use vendor-supplied defaults for system passwords and other security parameters	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
3	Protect stored cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
4	Encrypt transmission of cardholder data across open, public networks	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
5	Protect all systems against malware and regularly update anti-virus software or programs	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
6	Develop and maintain secure systems and applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
7	Restrict access to cardholder data by business need to know	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
8	Identify and authenticate access to system components	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
9	Restrict physical access to cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
10	Track and monitor all access to network resources and cardholder data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
11	Regularly test security systems and processes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
12	Maintain a policy that addresses information security for all personnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Appendix A1	Additional PCI DSS Requirements for Shared Hosting Providers	<input checked="" 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 checked="" type="checkbox"/>	<input type="checkbox"/>	

