INSTRUCTIONS FOR COMPLETION - PLEASE READ BEFORE YOU RESPOND TO THE PCI-DSS STANDARDS

1 Providers must ensure they provide sufficient supporting explanation for GCC to evaluate their capability or their planned capability should they win the contract

2 Answers should refer to those parts of the Provider service that are involved in the storage, processing or transmission of Cardholder Data on behalf of GCC or those which supply or use services on behalf of GCC that could impact the security of Cardholder Data

3 Providers should ask for clarification regarding any security standards that they do not fully understand.

4 Where technical expertise is required, we expect relevant technicians to be consulted and their responses provided.

5 Where the exact security standard cannot be met, but the Provider believes that they can deliver a compensating control which provides an equivalent level of security to the required standard, then this should be documented in their response.

6 Where the information required is not applicable to the service, the Provider must detail why they believe this is the case.

7 Where supporting documentation is included, the Provider must reference the applicable paragraphs in their response.

8 Where Providers are planning to make changes which will impact their responses to the information requested, they must specify what changes are planned in the 'Supporting Explanation' column including the date by which these will be operational.

9 For all security standards the Provider must complete:

9a *Provider Response* : Select the appropriate rating for each security standard from the list:

- *Comply* - Where all elements of the requirement have been met as stated.
- *Comply with CCW* - The requirement has been met with the assistance of a compensating control. For all responses marked 'Comply with CCW', the Provider must complete the Compensating Control Worksheet (CCW) in columns I to N or attach the CCW separately clearly referenced. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in the PCI DSS (https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-A.pdf)
- *Do not comply* - Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before it will be known if they are in place.
- *Not applicable* - The requirement does not apply to the organisation's environment. All 'Not Applicable' responses require a supporting explanation in column H.

9b *Supporting Explanation* : The Provider must enter full details of how they meet each applicable security standard.

10 For further guidance regarding the various clauses refer to PCI DSS, please visit: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1551703069610

PCI-DSS Security Standards

Paritor does not store or take any cardholder data, this will all be done by the elected card provider. https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

No.	Requirement Reference	Area	Requirement	PCI DSS Security Standards	Paritor Response	Supporting Explanation
1	1.1	Install and maintain a firewall configuration to protect cardholder data	Establish and implement firewall and router configuration standards	Firewall / router policy needs to be maintained. This must include ensuring: * All firewall /router rules specifically relating to the cardholder data environment are documented including justification of all inbound and outbound services. * Network diagrams are maintained including data flows relating to payment data. * Firewall checks are enforced on a biannual basis * All policies are reviewed annually.	Not Applicable	We do not hold card data. Card data is held by the service provider e.g. sage, world pay, stripe etc.
2	2.1a	Build and Maintain a Secure Network and System	Do not use vendor-supplied defaults for system passwords and other security parameters	Vendor-supplied defaults must always be changed before installing a system on the network.	Comply	
3	2.1b	Build and Maintain a Secure Network and System	Do not use vendor-supplied defaults for system passwords and other security parameters	Unnecessary default accounts must be removed or disabled before installing a system on the network	Comply	
4	3.1	Protect stored cardholder data	Implement data retention and disposal policies, procedures if cardholder data is stored	Technical controls must be in place to safeguard stored cardholder data. Retention policies must be in place, and data must be reviewed quarterly to ensure legacy data is securely deleted as per retention period	Not Applicable	We do not hold card data. Card data is held by the service provider e.g. sage, world pay, stripe etc.
5	4.1	Encrypt transmission of cardholder data across open, public networks	Use strong cryptography and security protocols to safeguard transmission	All cardholder data must be encrypted through its journey over open, public networks. The use of weak protocols is prohibited, industry standards must be used in line with PCI DSS (v3.2.1, latest TLS 1.1/1.2). Transmission policy must be documented, maintained and reviewed yearly. It must clearly state that PANs are not to be sent over insecure media.	Not Applicable	We do not hold card data. Card data is held by the service provider e.g. sage, world pay, stripe etc.
6	5.1	Protect all systems against malware	Deploy anti-virus software on all systems	All systems within the cardholder environment that are processing, storing or transmitting payment card data must be protected against malware. Anti-virus software must be capable of detecting all known malicious software. Software must be maintained and kept current. Periodic scans must be performed and audit logs retained for one year as per clause 10.7	Comply	All our systems and data are maintained by microsoft azure, and as such a high level of security is maintained.
7	6.2	Develop and maintain systems and applications	Install vendor patches within one month if critical, all other patches should be installed within appropriate time not exceeding 2.5 months from date of release unless its deemed a business risk	Vendor supplied patches must be installed to ensure all system components are protected from known vulnerabilities. Critical patches must be installed within one month of release.	Comply	All our systems and data are maintained by microsoft azure, and all patches are applied by them in a timely fashion.
8	7.1	Restrict access to cardholder data by business need to know	Limit access to system components and cardholder data to only those individuals whose job requires such access	Documented policies defining access needs and privileges assigned to individuals must be maintained. All access must be through a formal process and authorised and access to system components should be by default deny all.	Not Applicable	We do not hold card data. Card data is held by the service provider e.g. sage, world pay, stripe etc.
9	8.1.1	Implement Strong Access Control Measures	Identify and authenticate access to system components	All users must be assigned a unique ID before allowing them to access system components or cardholder data	Comply	
10	8.1.3	Implement Strong Access Control Measures	Identify and authenticate access to system components	Access for any terminated users must be immediately deactivated or removed	Comply	
11	8.2	Implement Strong Access Control Measures	Identify and authenticate access to system components	In addition to assigning a unique ID, one or more of the following methods must be employed to authenticate all users: * Something you know, such as a password or passphrase * Something you have, such as a token device or smart card * Something you are, such as a biometric	Comply	All access to the system is managed via microsoft azure B2C active directory. We employ two factor authentication.

12	8.2.3a	Implement Strong Access Control Measures	Identify and authenticate access to system components	User password parameters must be configured to require passwords/passphrases that meet the following: * A minimum password length of at least seven characters * Contain both numeric and alphabetic characters Alternatively, the passwords/passphrases must have complexity and strength at least equivalent to the parameters specified above.	Comply	
13	8.5	Implement Strong Access Control Measures	Identify and authenticate access to system components	Group, shared, or generic accounts, passwords, or other authentication methods must be prohibited as follows: * Generic user IDs and accounts are disabled or removed; * Shared user IDs for system administration activities and other critical functions do not exist; and * Shared and generic user IDs are not used to administer any system components	Comply	
14	9.5	Implement Strong Access Control Measures	Restrict physical access to cardholder data	All media must be physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes). For purposes of Requirement 9, "media" refers to all paper and electronic media containing cardholder data	Comply	
15	9.6a	Implement Strong Access Control Measures	Restrict physical access to cardholder data	Strict control must be maintained over the internal and external distribution of any kind of media	Comply	We do not hold card data. Card data is held by the service provider e.g. sage, world pay, stripe etc.
16	9.6.1	Implement Strong Access Control Measures	Restrict physical access to cardholder data	Media must be classified so the sensitivity of the data can be determined.	Comply	We do not hold card data. Card data is held by the service provider e.g. sage, world pay, stripe etc.
17	9.6.2	Implement Strong Access Control Measures	Restrict physical access to cardholder data	Media must be sent by secured courier or other delivery method that can be accurately tracked	Not Applicable	We do not manage media containing any senstive data.
18	9.6.3	Implement Strong Access Control Measures	Restrict physical access to cardholder data	Management approval must be obtained prior to moving the media (especially when media is distributed to individuals)	Not Applicable	We do not manage media containing any senstive data.
19	9.7	Implement Strong Access Control Measures	Restrict physical access to cardholder data	Strict control must be maintained over the storage and accessibility of media	Not Applicable	We do not manage media containing any senstive data.
20	9.8a	Implement Strong Access Control Measures	Restrict physical access to cardholder data	All media must be destroyed when it is no longer needed for business or legal reasons	Not Applicable	We do not manage media containing any senstive data.
21	9.8.1a	Implement Strong Access Control Measures	Restrict physical access to cardholder data	Hardcopy materials must be cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed	Not Applicable	We do not manage or hold any hard copy data.
22	9.8.1b	Implement Strong Access Control Measures	Restrict physical access to cardholder data	Storage containers used for materials that contain information must be destroyed securely to prevent access to the contents	Not Applicable	
23	10.1	Monitor and test networks	Track and monitor all access	Audit trails must be implemented to ensure all access to systems components is tracked including actions taken by individuals (creation, deletion, edition etc). The event should be identifiable through logging the following: user, location, time, date, success and failure. Documented policy should be maintained and reviewed annually	Comply	
24	11.1 - 11.3	Regularly test security systems and processes	System components, processes and software should be tested frequently to ensure security is maintained.	Processes must be implemented to test for the presence of wireless access points. An inventory must be maintained of wireless access points and if unauthorised wireless access points are detected, an incident response implemented. Internal / external scans must be carried out as mandated in clause 11.2. Penetration testing must be carried out as per clause 11.3.	Comply	
25	11.4	Regularly test security systems and processes	Detect and prevent intrusions into the network	Network intrusion detection and intrusion prevention techniques must be used to detect and prevent intrusions into the network.	Comply	
26	11.5	Regularly test security systems and processes	Deploy a change detection mechanism	A change detection mechanism, such as file integrity monitoring tools, which alerts personnel to unauthorised modification, must be deployed for system components that process, transmit and store payment card data.	Comply	
27	12.8.1	Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel	A list of service providers must be maintained, including a description of the service(s) provided	Comply	

28	12.8.2	Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel	A written agreement must be maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.	Not Applicable	We do not hold card data. Card data is held by the service provider e.g. sage, world pay, stripe etc.
29	12.8.3	Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel	An established process for engaging service providers, including proper due diligence prior to engagement must be in place	Comply	
30	12.8.4	Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel	A program must be maintained to monitor service providers' PCI DSS compliance status at least annually	Comply	
31	12.8.5	Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel	Information must be maintained about which PCI DSS requirements are managed by each service provider, and which are managed by the entity	Comply	
32	12.10.1	Maintain an Information Security Policy	Maintain a policy that addresses information security for all personnel	An incident response plan must have been created to be implemented in the event of system breach	Comply	