PCI Customer Agreement Addendum

As a 3rd party service provider, Tucasi acknowledges it has an important role to play in protecting card data.

Tucasi acknowledges that it is responsible for the security of cardholder data we possess or otherwise store, process, or transmit on behalf of the customer, or to the extent that we could impact the security of the customer's cardholder data environment.

To show our commitment to protecting card data, Tucasi agrees to maintain PCI DSS compliance and will treat card data that we inadvertently have access to appropriately.

Tucasi will perform Quarterly ASV (Approved Scanning Vendor) scans and an annual QSA RoC (Qualified Security Assessor, Report on Compliance). Attestation of Compliance and executive summary of ASV scans will be made available to customers upon request. This documentation will help satisfy your PCI compliance as a merchant.

PCI Scope

Tucasi will ensure the security of cardholder data through adherence to the requirements of Payment Card Industry Data Security Standard (PCI DSS).

Tucasi does not store, process or transmit cardholder data at any point. Tucasi has deployed systems to ensure that card data is only processed, stored and transmitted by certified Payment Service Providers (PSP).

Tucasi has a single channel for card payment processing, a full redirect to PSP for processing of payments which is initiated from the e-commerce website (scopay.com) and the mobile application (SCOPAY).

PCI Responsibility Matrix

Below are the details for the PCI DSS version 3.2.1 requirements that Tucasi is responsible for. All other PCI DSS version 3.2.1 requirements are the responsibility of the merchant or other parties involved in the processing, transition, storage, or other parties that could impact the security of the customers cardholder data environment.

Requirement	Requirement Detail
2.1.a	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor supplied security patches. Install critical security patches within one month of release.
8.1.1	Assign all users a unique ID before allowing them to access system components or cardholder data.
8.1.3	Immediately revoke access for any terminated users.
8.2	In addition to assigning a unique ID, ensure proper user authentication management for non-consumer users and administrators on all system

	components by employing at least one of the following methods 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.
8.2.3.a	Passwords/phrases must meet the following: + Require a minimum length of at least seven characters. + Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.
8.5.a	Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: + Generic user IDs are disabled or removed. + Shared user IDs do not exist for system administration and other critical functions. + Shared and generic user IDs are not used to administer any system components.
12.4.1	Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: - Overall accountability for maintaining PCI DSS compliance - Defining a charter for a PCI DSS compliance program and communication to executive management
12.8	Are policies and procedures maintained and implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data.
12.9	Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.
12.10.1.a	Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: + Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum + Specific incident response procedures + Business recovery and continuity procedures + Data backup processes + Analysis of legal requirements for reporting compromises + Coverage and responses of all critical system components + Reference or inclusion of incident response procedures from the payment brands.
ASV Scans	Attested ASV scans showing no vulnerabilities above CVSS score 3.9 for each quarter.

Tucasi PCI Contact

The primary point of contact within Tucasi for any PCI DSS queries is:

Name: Nathan Foley

Position: Head of Development and Infrastructure

Telephone: 02380 016 564 (ext 215)

Email: nfoley@tucasi.com

Supplier Approval

Signature: S Parrott

Print name: Steve Parrott

Title: Managing Director

Date: 001/11/2021

Document control

Date	Version	Editor	Comments
23/04/2018	**1.1**	**Nathan Foley**	**Initial document**
02/05/2018	**1.2**	**Nathan Foley**	**Changes after QSA review**
10/05/2018	**1.3**	**Nathan Foley**	**Minor changes after QSA review**
14/05/2019	**1.4**	**Dave Goodman**	**Reflect PCI scope changes to include 6.2 & mobile application**
07/01/2020	**1.5**	**Nathan Foley**	**Update job titles and personnel**
23/04/2021	**1.6**	**Dave Goodman**	**Update Nathan Foley's job title**