WOOLWORTHS FINANCIAL SERVICES

EXTERNAL SUPPLIER CONTROL OBLIGATIONS

Payment Card Industry Data Security Standard (PCI DSS)

Version 7.2 Dated November 2018

PCI DSS OBLIGATION	CONTROL DESCRIPTION	WHY THIS IS IMPORTANT
1. Attain Card Data Compliance	The Supplier shall comply with the current versions of the PCI Standards as issued by the Payment Card Industry Security Standards Council (PCISSC), such as: • Payment Card Industry Data Security Standard (PCI-DSS) • Payment Application Data Security Standard (PA-DSS) • Payment Card Industry Point-to-Point Encryption (PCI- P2PE) • Payment Card Industry PIN Transaction Security (PCI-PTS) • Payment Card Industry Card Production (PCI-CP) Etc.	Protect Cardholder Data: The recognized standard to achieving this is PCI DSS and is a global industry regulatory requirement. PCI security standards are technical and operational requirements set by the Payment Card Industry Security Standards Council to protect cardholder data.
2. Supplier Attestation	The Supplier shall provide an Attestation of Compliance (AoC) and Report on Compliance (RoC) or Self-Assessment Attestation (SAA), applicable to the scope of the services provided to WFS, pre-contract and annually thereafter. This must be in accordance with the PCISSC requirements, see www.pcisecuritystandards.org.	Evidence that a supplier has attained the relevant Card Data compliance for the scope of the services provided to WFS and adhered to the requirements. Evidence: Attestation of adherence to PCI Standards

Use of Third-Party Service Providers I Outsourcing

A service provider or merchant may use a third-party service provider to store, process, or transmit cardholder data on their behalf, or to manage components such as routers, firewalls, databases, physical security, and or servers. If so, there may be an impact on the security of the cardholder data environment.

Parties should clearly identify the services and system components which are included in the scope of the service provider's PCI DSS assessment, the specific PCI DSS requirements covered by the service provider, and any requirements which are the responsibility of the service provider's customers to include in their own PCI DSS reviews. For example, a managed hosting provider should clearly define which of their IP addresses are scanned as part of their quarterly vulnerability scan process and which IP addresses are their customer’s responsibilities to include in their own quarterly scans.

Service providers are responsible for demonstrating their PCI DSS compliance, and may be required to do so by the payment brands. Service providers should contact their acquirer and/or payment brand to determine the appropriate compliance validation.

There are two options for third-party service providers to validate compliance:

1) **Annual assessment**: Service providers can undergo an annual PCI DSS assessment(s) on their own and provide evidence to their customers to demonstrate their compliance; or

2) **Multiple, on-demand assessments**: If they do not undergo their own annual PCI DSS assessments, service providers must undergo assessments upon request of their customers and or participate in each of their customer's PCI DSS reviews, with the results of each review provided to the respective customer(s)

If the third party undergoes their own PCI DSS assessment, they should provide sufficient evidence to their customers to verify that the scope of the service provider's PCI DSS assessment covered the services applicable to the customer and that the relevant PCI DSS requirements were examined and determined to be in place. The specific type of evidence provided by the service provider to their customers will depend on the agreements/contracts in place between those parties. For example, providing the AOC and or relevant sections of the service provider's ROC (redacted to protect any confidential information) could help provide all or some of the information.

Additionally, merchants and service providers must manage and monitor the PCI DSS compliance of all associated third-party service providers with access to cardholder data. Refer to *Requirement 12.8 in this document for details*.