Transport for Greater Manchester Policy

P07 Information Systems Service Providers & Third Party Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	11th March 2022	Document Reference no.	IS Service Providers & Third Party Policy P07
Version No.	4.0	Prepared by:	Catherine Burke & Rohan Mendis
Equality Impact Assessment	Validation of Initial Screening Equality Officer: Muhammad Karim **Date:**		Full Impact Assessment completed: YES **Validated by Equality Officer signature:** **Date:**
Authorisation Level required:	Executive Group/Director		Staff Applicable to: All Staff
Authorised by: Date:	Head of IS Operations (Ricard Fuertes) 31st March 2022		Implementation Date: 31st March 2022 Annual review date: 31st January 2023

Table of Contents

Policy Aims

a) This document details **TfGM's** policy in relation to Service Providers and Third Parties that store, process or transmit **TfGM's** payment card data.

b) This policy covers PCI compliance activities, security standards and procedures required of these service providers and third parties.

c) This document should be viewed in conjunction with **TfGM's** top-level security policy: P01 – Information Security Policy.

Review and Update of the Policy Statement

a) The Policy Statement and associated company Policies are reviewed at least annually by **TfGM's IS Team** to ensure:

- the business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS); and
- it maintains its relevance to the business' current and planned payment card processing operations.

b) The **IS Team** will undertake the review of this policy statement and associated company Policies.

Purpose

a) This document details what is expected of each Service Provider and Third Party when storing, processing or transmitting **TfGM's** payment card data.

b) It is very important that each identified external organisation that has access to credit card data exercises a duty of care. In certain cases, such as with Payment Gateways, Payment Processors, Hosting Providers and Third Party Application Providers, proof of PCI compliance must be provided. This information will feed directly into **TfGM's** PCI compliance programme.

c) Current Service Providers and Third Parties are listed in F20 – Service Providers Log.

Scope

a) This document provides instruction on dealing with external companies that have access to **TfGM's** payment card data or credit card processing facilities.

b) It is restricted to those companies or contractors that process, store or transmit card data on behalf of **TfGM**, or have access to such systems.

Policy Delivery

This policy will be delivered to all staff by internal communication and will be situated on the **TFGM** Intranet.

Accountability

- **Responsible to the Board:** Head of IS
- **Compliance:** All Staff
- **Awareness:** IS Department

Enforcement / Monitoring / Compliance

a) Monitoring and compliance against PCI DSS requirements will be managed through regular service performance reviews.

b) Should a breach of policy be identified, it will be remediated through the contract management process.

External Company Definitions

8.1 General

a) It is important to distinguish between Service Providers and Third Parties.

b) Once Service Providers have been identified, supporting PCI audit materials shall be requested as proof of compliance. Proof of compliance ensures that the Service Provider is meeting its security obligations when handling card data on behalf of **TfGM. TfGM** shall ensure that each Service Provider's continued PCI DSS compliance status is confirmed at least annually.

8.2 Service Providers

a) An entity that stores, processes or transmits data on behalf of another organisation, or has access to another organisation's CDE.

b) This also includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data.

c) Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

d) **TfGM** must maintain a:

- List of service providers; and
- Written agreement with each service provider that includes an acknowledgement by the service provider that they reponsible for the security of **TfGM's** cardholder data, they possess or otherwise store, process or transmit on behalf of **TfGM** or to the extent that they could impact the security of the client's cardholder data environment.
- If **TfGM** is also acting as a service, provider, then **TfGM** must provide a written agreement to clients as per the point above, in order for clients to maintain their own PCI compliance.

e) Service Providers are categorised by the nature of card processing activity and/or the number of card transactions that they process on behalf of their clients. There are two levels:

Service Provider Level	Description
1	Any service provider that stores, processes, or transmits more than 300,000 card transactions annually.
2	Any service provider that stores, processes, or transmits fewer than 300,000 card transactions annually.

8.3 Service Providers Providing Card Processing Software.

a) Third parties providing card data processing systems such as payment gateways, PED terminals or payment processing software are required to do so in accordance with the relevant PCI standard.

See section 9.1 below.

Policy

9.1 General

a) As part of **TfGM's** continuing obligation to PCI compliance, due diligence check such as:

i) Confirmation of PCI compliance status, including which specific PCI DSS requirements are being met or supported by the service being offered (this may include details of the provider's PCI DSS compliance, PA DSS compliance, PTS compliance, or P2PE compliance, as applicable.

ii) Their ability to achieve and maintain PCI DSS compliance shall be conducted before:

- selecting and implementing a new Service provider;
- connecting a service provider to the **TfGM** card processing network;
- granting a Service Provider access or control over **TfGM's** card data;
- selecting and deploying payment card processing software or services within **TfGM**.

b) **TfGM** shall maintain a program to monitor service providers' PCI DSS compliance status at least annually.

c) **TfGM** shall maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by **TfGM**.

d) A full list of service providers and third parties accessing card networks can be found in the document F20 – Service Providers Log.

Note: PCI compliance status of all service providers, and the corresponding PCI DSS requirements that are being met or supported by the provider needs to be reconfirmed and documented annually.

9.2 Agency Background Checks

a) **TfGM** shall ensure that any and all agencies providing staff on a temporary basis have conducted background checks against the staff being provided, including:

i) Reference Checks.

ii) Employment History Checks.

iii) Immigration Status & Right to work checks.

b) **TfGM** shall maintain a list of the Agencies used, and the checks performed by each agency.

c) A full list of Agencies used by the TfGM can be found in the document: F20 – Service Providers Log.

Glossary and References

10.1 Glossary

See document P99 - Glossary

10.2 References

- P01 – Information Security Policy
- P05 – IS Operational Policy
- F20 – Service Providers Log

Policy: P05 – IS Operational Policy				
Version	**Change**	**Reason for change**	**Date**	**Name**
1.0	Date & Version	Updated review	31/10/2013	C. Burke
2.0	Date & version	Annual review	06/03/2014	C. Burke
2.1	Update	Updated to include Version 3.0 change variations	16/03/2015	C.Burke
2.2	Date and Version	Annual review	31/03/2016	C. Burke
2.3	Date & Version	Annual Review	31/03/2017	C.Burke
3.0	Date & Version	Annual Review	31/03/2018	C. Styler
4.0	Date & Version	Annual Review	11/03/2019	C. Burke
4.0	Date & Version	Annual Review	11/03/2020	C. Burke & M. Cunliffe
4.0	Date & Version	Annual Review	31/03/2021	C. Burke
4.0	Date & Version	Annual Review	31/03/2022	C. Burke