Transport for Greater Manchester Policy

P01 Information Systems Security Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31/03/2021	Document Reference no.	IS Security Policy P01
Version No.	9.1	Prepared by:	Catherine Burke
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:	Head of IS (Malcolm Lowe)		Implementation date: 31st March 2021
Date:	31st March 2021		Annual review date: 31st Jan 2022

Table of Contents

1. Policy Aims

a) This **TfGM** Information Systems Security Policy Statement ("Policy Statement"):

   i) Sets out **TfGM** high level requirements for the management of Information Security across **TfGM** in relation to the storage, processing and transmission of Payment Card data.

   ii) Defines the Information Security Policy Statement for the business.

   iii) Applies to Payment Card all processing operations for the business.

2. Review and Update of the Policy Statement

a) The Policy Statement and associated company Policies are reviewed at least annually by **IS InfoSec Practice** to ensure:

   i) the business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS), and

   ii) it maintains its relevance to the business' current operations and Payment Card processing operations.

b) The **IS InfoSec Practice** will undertake the review of this policy and associated company policies. The annual review will be assessed by the **InfoSec Practice**.

c) The **IS InfoSec Practice** undertake a review of this policy as needed to reflect changes to business objectives or the risk environment.

3. Purpose

a) This document reflects the security strategy for **TfGM** in relation to the storage, processing and transmission of Payment Card data. Its aim is to provide a detailed understanding of Information Security responsibilities for all levels of staff, contractors, partners and third parties that access **TfGM's** Card Data Environment (CDE).

b) As part of **TfGM's** Payment Card Industry (PCI) Compliance programme, consideration has been made to Payment Card Processing operations. Guidelines and controls form an essential part of the company's compliance status against the PCI Data Security Standard.

4. Scope

a) This document must be reviewed by parties involved with **TfGM's** Payment Card processing operations. Specifically:

   i) Day-to-day Payment Card processing operations (including IS systems);

   ii) Manual and automated operations;

   iii) Implementation of new Payment Card processing systems;

   iv) Maintenance of existing Payment Card processing;

   v) Retirement and subsequent secure destruction of Payment Card Processing systems.

b) This document should also be used for reference purposes when **TfGM's** undertakes its annual PCI compliance review.

c) The policy framework maps directly to the PCI DSS, and that information can be found in F16 - Standards Matrix.

5. Policy Delivery

a) This policy will be delivered to all staff by internal communication and will be published on the **TfGM** Intranet.

b) Any changes to this policy will be communicated all staff of **TfGM** and any other stakeholders, which may include vendors and business partners.

6. Accountability

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

7. Enforcement / Monitoring/ Compliance

a. This policy will be enforced by the Executive.

b. Information including dates, times, duration and device identity will be logged and maybe used for monitoring purposes, and may be used in disciplinary proceedings.

c. Should a breach or violation of this policy be identified, it may result in disciplinary action in accordance with **TfGM** disciplinary policy.

8. Policy

8.1 Information Security Framework

8.1.1 Reporting Structure for the Business

a) Within **TfGM**, the **Head of IS** is responsible for matters relating to Information Security and is designated the Head of Information Security.

Name	Title / Description	Contact Details
Malcolm Lowe	TfGM – Head of IS	malcolm.lowe@tfgm.com 0161 244 1545 ex 701545

b) This role has responsibility for:

i) Overall responsibility for Information Security and related issues.

ii) Development and maintenance of Information Security Policies (including distribution to; and training of, staff in policies).

iii) Communication and review of Information Security Policies.

iv) Coordination of PCI Security Audit Tasks.

v) Coordination with PCI Accredited Security Auditors (QSA).

vi) Ensure monitoring and analysing of security alerts and distributing information to appropriate **TfGM's** Information Security & Business Unit management personnel.

vii) Establishing, documenting, and distributing Information Security Incident response and escalation procedures.

viii) Keeping IT security staff and management updated on all security related issues.

8.1.2 Associated Teams

The following teams are directly involved in **TfGM's** PCI DSS compliance programme. References to these teams are made throughout **TfGM's** suite of PCI DSS policies.

Team Name	Functions (with respect to PCI)	Team Contact Details
PCI review team	Sec-1 Wayne Murphy	Waynem@Sec-1.com 01924 284 240
IS Team	Malcolm Lowe (TfGM Head of IS) Ricard Fuertes (TfGM Head of IS Operations) Rohan Mendis (Enterprise Technical Architect) Catherine Burke (Lead Security & Compliance) Matthew Haynes (Security & Compliance Analyst) Christopher Brown (IS Training Manager)	malcolm.lowe@tfgm.com 0161 244 1545 ext 701545 Ricard.fuertes@tfgm.com 0161 244 0955 ext 700955 Rohan.mendis@tfgm.com 0161 244 1353 ext 701353 Catherine.burke@tfgm.com 0161 244 1216 ext 701216 Matthew.haynes@tfgm.com 0161 244 1768 ext 701768 Christopher.brown@tfgm.com 0161 244 1177 ext 701177

Team Name	Functions (with respect to PCI)	Team Contact Details
IS Service Team	IS Infrastructure Practice (Networks) Team Members • Russell Baucutt • Chris Budnar • Julian Parker • Daniel Wynn • Danny Trainer • Mark Richardson • Piyal Weerasingha • Sahal Kaka IS Infrastructure (DCS) Team Members • Jason Higgins • Chris Leigh • John McLaughlin • Basit Khan • Alex Bunton • Ivan Arteaga • Joseph Kinney • Phil Ireland • Tim Cowley • Tony Brown IS Serviceline • Colin Birnie • Edward Reilly • David Brown • Darren Clare First Line Support • Peter Wallwork • Karin Murray • Alex Tierney • Matthew Hallam • Christian Botham • James Tierney • David Brown • Mark Greenwood • Christopher Wong • Craig Hallsworth	infrastructure@tfgm.com 0161 244 1214 / 07834 119 061 dcsops@tfgm.com 0161 244 1221 / 07789 395834 Serviceline@tfgm.com 0161 244 1234 Serviceline@tfgm.com 0161 244 1234

Team Name	Functions (with respect to PCI)	Team Contact Details
Change Control Team	Mat Clayton (IS Senior Service Manager) Malcolm Davidson (IS Service Manager) Lee Higgins (IS Service Manager) Shaun Pollard (Service Analyst)	mat.clayton@tfgm.com 0161 244 1208 ext 701208 Malcolm.Davidson@tfgm.com 0161 244 1647 ext 701647 Lee.higgins@tfgm.com 0161 244 1030 ext 701030 Shaun.Pollard@tfgm.com 0161 244 1030 ext 701030
Internal Audit Team	David Knight	David.knight@tfgm.com 0161 244 1139 ex 701139

8.2 Annual Policy Review

a) All Information Security Policies are updated at least annually or upon implementation of a significant change to **TfGM's** CDE, whichever happens first.

b) The review process ensures that:

   i) Policies in place are still required;

   ii) Perceived threats facing **TfGM** are identified and consideration included in procedural documentation;

   iii) Any new legal issues are identified that require changes in current policy or practice;

   iv) **TfGM** meets current PCI compliance standards;

   v) Any changes to network configuration or new applications are included in **TfGM's** security policy.

c) The Annual Policy Review must also include a formal Risk Assessment Process to identify key business assets (including CDE Payment Card data stores and supporting networks) and potential threats. This will lead into the review of the Risk Assessment Process for all business assets.

8.3 Policy Breaches

TfGM's disciplinary procedures will be invoked in the case of staff or third parties breaching the policy standards and/or the IS supporting policies or standards.

8.4 Individual Policies

a) The policies listed below have been developed in accordance with the current version of the PCI Data Security Standard. This is currently: Version 3.2.1.

b) Policies address all requirements listed in the PCI Data Security Standard.

c) Specific policies are listed below.

Policy Name	Document Name
Information Security Policy	P01 - IS Security Policy
Audit Policy	P02 - IS Audit Policy
Disaster Recovery & Security Incident Response Policy	P03 - IS Disaster Recovery & Security Incident Response Policy
Wireless Access Policy	P04 - IS Wireless Access Policy
Operational Policy	P05 - IS Operational Policy
Acceptable Use Policy	P06 - IS Acceptable Use Policy
Third Parties Policy	P07 - IS Third Parties Policy
Information Classification Policy	P08 - IS Information Classification Policy
Key Management Policy	P09 - IS Key Management Policy
Physical Security Policy	P10 - IS Physical Security Policy
Systems and Application Development Policy.	P11 - IS Systems & Application Development Policy
Penetration Testing Policy	P12 – Penetration Testing Policy

8.5 Policy Communication

8.5.1 Policy Creation and Distribution

a) The **Head of IS** has overall responsibility for the creation and distribution of IS Security Policy. All IS policies, procedures and forms are available on the PCI DSS SharePoint Site /**TfGM** Intranet.

b) All staff are reminded that the documents are sensitive and should not be removed from **TfGM's** buildings/offices and networks.

8.5.2 Security Training

a) All changes and additions to policies are circulated to stakeholders at least one (1) day in advance to allow time for them to adapt to changes. **TfGM** does however reserve the right to modify policy immediately and without prior notice.

b) Staffs are kept aware of policies via the following methods of communication.

   i) Staff meetings.

   ii) Emails, Intranet or Staff Bulletins.

   iii) Posters.

   iv) Mock exercises.

   v) Annual workshops and E-Learning

c) Security awareness training, including authentication procedures and policies, and (for POS environment) awareness of the risks of Pin Entry Device (PED) tampering is to be conducted for new starters during induction, and for all staff, at least annually to make all personnel are aware of the importance of cardholder data security.

d) The training, including E-Learning shall address the following areas as a minimum.

   i) Guidance on selecting strong authentication credentials.

   ii) Guidance for how users should protect their authentication credentials, and why sharing passwords is a poor security choice.

   iii) Why it is important not to reuse previously used passwords.

   iv) How to change passwords if there is any suspicion the password could be compromised.

v) Training personnel to be aware of suspicious behaviour and to report tampering or substitution of POS devices to **TfGM IS Serviceline**.

e) **TfGM** shall also ensure that vendors, contractors, and business partners covered by this policy are familiar with these requirements.

f) Once a new policy has been introduced, and following significant changes, and at least annually, all staff must endorse the IS Security Policies. This ensures that they have read and understood the policy (or changes) and accept any consequences should they fail to adhere to them.

g) Users will be made familiar with the password procedures for **TfGM** and will be offered specialist training if necessary.

8.5.3 Staff with cardholder data access or access to the cardholder data environment

TfGM staff with privileged access, deemed to have the need to know (see PCI DSS Requirement 7 must be given extra training to ensure they are aware of the significance of the data being held and the repercussions of disclosing it to those who do not have the need to know.

8.5.4 Staff Acknowledgement

TfGM staff are required to acknowledge (in writing, or electronically) that they have attended any security awareness courses, and a log must be maintained to that effect.

8.6 Employment Checks

8.6.1 TfGM Permanent Staff

a) **TfGM** shall ensure that any new employee directly hired by the company shall be subjected to the following checks:

i) Two satisfactory previous employee Reference Checks.

ii) Proof of the right to work in the UK in accordance with the Asylum and Immigration Act.

b) **TfGM** shall ensure that any agency providing temporary staff at any point within the year shall ensure that the agency contracted to provide such staff have conducted the above checks and can produce the relevant documentation upon request (see also P07 – Service Provider & Third Parties Policy).

c) All information gathered for employment checks shall be maintained in the employee's personnel file.

8.6.2 Agency background Checks on Temporary Staff

a) **TfGM** shall employ temporary staff through the Preferred Supplier List.

b) **TfGM** shall ensure that, through its' preferred suppliers, they have conducted the following background checks against the temporary employee being provided, where the employee will have access to cardholder data or the cardholder data environment.

   i) A minimum of two years referencing, one reference from the current or last employer.

   ii) History and evidence to demonstrate continuity of employment.

   iii) Evidence of the workers right to work in the United Kingdom in accordance with the Asylum and Immigration Act.

c) **TfGM** shall ensure that any agency providing temporary staff at any point within the year shall ensure that the agency contracted, to provide such staff, has conducted the above checks and can produce the relevant documentation upon request (see also P07 - Third Party & Service Provider Policy).

d) All information gathered for employment checks shall be maintained in the employee's personnel file.

8.7 Data Confidentiality for Service Providers & Third Parties

a) **TfGM** has a duty of care to its customers and a PCI DSS Compliance obligation to ensure that Service Provider and Third Parties processing or given access to confidential cardholder data/cardholder data environment uphold suitable Data and Information Security Practices and Policies.

b) PCI Compliance for Service Providers follows the PCI DSS. For more information on Service Providers and Third Parties with access & processing responsibility for card holder data see P07 – Third Party & Service Provider Policy.

9. Glossary and References

9.1 Glossary

- See document P99 - Glossary.

9.2 References

9.2.1 Policies

- P01 – IS Security Policy
- P02 – IS Security Audit Policy
- P03 – IS Disaster Recovery & Security Incident Response Policy
- P04 – IS Wireless Access Policy
- P05 – IS Operational Policy
- P06 – IS Acceptable Use Policy
- P07 – IS Service Provider & Third Parties Policy
- P08 – IS Information Classification Policy
- P09 – IS Key Management Policy
- P10 – IS Physical Security Policy
- P11 – Information Systems & Application Development Policy
- P12 - Penetration Testing Policy

9.2.2 Procedures

Nil

9.2.3 Forms

- F16 - Standards Matrix

Policy: P01 – IS Security Policy				
Version	**Change**	**Reason for change**	**Date**	**Name**
1.0		Initial Version	31/10/2012	C Burke
2.0	Version & Date	Annual Review & Update	31/10/2013	C. Burke
2.1	8.1 & 8.6.2 c)	Information Manager Name Change & Supplier change for temporary workers	10/09/2014	C. Burke
3.0	Update	Updated to include Version 3.0 change variations	16/02/2015	C. Burke
3.1	8.1.2 & 8.4	2 new members of staff. Updated v3 to v3.1	16/09/2016	C. Burke
3.2	Version & Date	Annual Review & Update	31/03/2016	C. Burke
4.0	IS Team Changes	Temporary change for IS Security & Standards Officer, Apprentice Role removed, 1st Line – Serviceline moves to second line & 2 new starters on 1st Line in Serviceline.	14/11/2016	C Burke
5.0	8.5.2 d)	E-Leaning minimum requirements	24/01/2017	C Burke
6.0	Annual Review	Version, date, new Head of IS	26/03/2017	C. Burke
6.1	Name Change	Michelle Peel name change to Michelle Brown	01/08/2017	C. Burke
7.0	Update and Annual Review	C Styler and K Murray added	31/03/2018	C. Styler
8.0	Update	M Wojick & G Bradley removed, B Khan swapped roles and J Parkin, B Mottram, H Gerrard added. Hays changed to 'preferred supplier'.	15/02/2019	C.Styler
9.0	No Change	Annual Review	11/03/2019	C.Burke
9.0	8.1	New Head of Operations	15/03/2020	C Burke
9.1	8.1	New staff added/old removed	31/03/2021	C Burke
10.0	Update	Annual review and change to risk (Covid-19)	19/03/2021	C. Burke
10.1	Update	New Lead ServiceLine/New Service Management Analyst	14/07/2021	C. Burke