Transport for Greater Manchester

Transport for Greater Manchester Policy

P08 Information Classification Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	26th March 2021	Document Reference no.	IS Classification Policy P08
Version No.	5.0	Prepared by:	Information Manager
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 2021		Implementation date: 31st March 2021 Annual review date: 31st January 2022

Table of Contents

1 Policy Aims

This document details **TfGM's** policy with respect to classification of confidential data. Particular emphasis is placed on Cardholder data.

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

2 Review and Update of the Policy Statement

a) The Policy Statement and associated company Policies are reviewed at least annually by **TfGM IS Operations 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 processing operations.

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

3 Purpose

a) This document identifies confidential information that is stored, processed or transmitted by **TfGM**.

b) All identified confidential data must be treated as confidential and subject to strict storage and management procedures.

c) All cardholder data is subject to PCI DSS regulatory controls.

d) All sensitive personal information is subject to the Data Protection Act (2018).

4 Scope

a) The scope of this policy covers all:

- **TfGM** information stored on **TfGM**-owned, **TfGM**-leased, and otherwise **TfGM**-provided systems and media, regardless of location; and
- hardcopies of **TfGM** data, such as printouts, faxes, notes, etc.

b) This document also identifies sensitive and confidential information that is stored, processed or transmitted by **TfGM**.

c) The following data categories are listed:

- Cardholder data (a.k.a "payment card data").
- Sensitive personal data.

5 Policy Delivery

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

6 Accountability

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

7 Enforcement / Monitoring / Compliance

a) This policy will be enforced by the Executive.

b) All managers are responsible for classifying information within their department.

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

8 Policy

8.1 Information Assets

a) Information assets are assets to **TfGM** just like physical property.

b) In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to **TfGM** operations and the confidentiality of its contents.

c) Once this has been determined, **TfGM** can take steps to ensure that data is treated appropriately.

8.2 Information Classification

a) Confidential Information

Confidential data:

- refers to data whereby should it be released, is likely to cause harm or have a detrimental impact upon an individual or individuals;
- is subject to significant scrutiny in relation to appropriate exemptions/ public interest and legal considerations; and
- is normally accessible to only specified members of staff.

b) Examples of confidential include; cardholder data, health; ethnicity, age, salary information; bank details; draft research reports; passwords etc

8.3 Confidential Data

a) Card Holder Data

The following Payment Card Payment Data has been identified as confidential:

Data Item	**Description**
Primary Account Number (PAN)	The number that identifies the issuer and the particular cardholder account. Also called Account Number
Cardholder Name	Name of the person the card is registered to
Service Code	Three of four digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe transaction
Expiration Date	Date the card expires
Full Magnetic Stripe Data / Track Data	Data encoded in the magnetic stripe used for authorisation during transaction when the card is presented.

Data Item	Description
Card Validation Code (CVV2)	Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe and reveals any alteration or counterfeiting.
Encrypted PIN block	The part of the PIN stored on chip located on *Chip & PIN* cards.
PIN or PIN Verification Values	The card PIN or codes used to ensure the PIN is the correct one for the card in question.

b) The IP addresses and routing information of the TfGM Multiservice Network has been identified as Confidential Data.

c) Personal Data

The following special category personal data has been identified as confidential.

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Health.
- Sexual life or sexual orientation.
- Data concerning criminal offences.

8.4 Information Security

a) All users of confidential information must ensure that all confidential information they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise.

8.5 Information Storage

a) The preface of the PCI Data Security Standard, details the controls needing to be placed upon each cardholder data element, and which elements may not be stored post-authorisation even with controls applied.

b) The following apply to the storage of confidential data.

- All confidential information must be removed from desks, computer screens, and common areas unless it is currently in use.
- Confidential information must be strictly controlled and stored in a secure location.
- Access to confidential information must only be granted to authorised personnel.

c) If cardholder data is being stored on any electronic media, controls must be applied to that data to ensure it is not stored in plain-text, by using one or more of the following techniques:

- Encryption, using an industry-recognised strong encryption algorithm, with associated key-management processes and procedures.
- Truncation of the PAN, retaining at most the first 6 and last 4 numbers only.
- Hashing, using a secure one-way hashing algorithm with a salt.
- Index tokens and pads, with the pads being securely stored

d) When displaying a Primary Account Number (on screen or paper receipts) only the first 6 digits (identifier of the issuer) and the last four digits of the PAN should be displayed.

e) When full card numbers are required for business reasons, **TfGM** must ensure that viewing of a full PAN can be traced back to the individual user.

f) Cardholder data stored for any length of time must comply with the procedure in the PR10 – Data Retention Procedure.

g) The truncated or the encrypted full PAN with other details of the transaction should be held for 12 months with permanent deletion occurring on a monthly basis.

h) Refer to the preface of the PCI Data Security Standard, on page 2, which details the controls needing to be placed upon each cardholder data element, and which elements may not be stored post-authorisation even with controls applied.

i) By default, all users will only be able to view a masked or truncated PAN.

j) Users who have a legitimate business need to see the PAN may do so, and a list of roles who are explicitly permitted to view the full PAN will be maintained by **TfGM's** Head of IS Operations.

k) List containing the role names and the business justification for being able to view the full PAN is given in the following table.

Role	Business Justification
Customer Support Officer: TfGM Customer Support Centre	Processing of following forms rejected by the mail application processing Centre • Concessionery Travel Replacement Application Form • New/Replacement IGO Application Form • Travel Voucher Order Form
DriveSafe – Business Support Officer	Recieveing phone calls, on PCI secure phoneline, where full PAN's are given to process payments via a PCI compliant terminal.

8.6 Data Transmission

a) The following apply to the transmission of confidential information.

- All electronic methods of transmission outside of **TfGM** must utilise an IS approved encryption method.
- For non-electronic information transfers a method that returns a delivery receipt must be used.

8.7 PCI Information Destruction

a) The following apply to the destruction of confidential information.

- Confidential information must be destroyed in a manner that makes recovery of the information impossible, e.g. shredding, permanent delete.
- The process must be audit trailed.

9 Glossary & References

9.1 Glossary

See document P99 - Glossary

9.2 References

- P01 – IS Security Policy
- PR10 - Data Retention Procedure

Change control record: complete each time there is a change

Policy:				
Version	**Change**	**Reason for change**	**Date**	**Name**
1.0		Approved by Exec Group	Sept 11	KB
2.0	Included further PCI DSS requirements in Policy	Met with PCI DSS Consultants who suggested some changes to Policy	Nov 11	CB
2.1	Review	Review of Policy	Feb 13	CB
2.2	Removal of requirement for transfer form prior to transmission of data.	Review of policy.	Feb 14	MP
2.3	Version and Date.	Annual Review	March 14	RM
2.4	Update	Update to include Version 3.1 change variations	16/02/2015	CB
2.5	Version and Date	Annual Review	31/03/2016	CB
2.6	Version & Date	Annual Review	31/03/2017	C. Burke
3.0	Version, Date and removal of Eccles	Annual Review and Removal of Eccles from 8.5 K)	31/03/2018	C. Styler
4.0	Version, Date and change of IS Infrastructure Manager to Head of IS.	Annual Review and change of IS Infrastructure Manager to Head of IS. Updated to reflect GDPR.	19/02/2019	C. Styler
4.0	No change	Annual Review	11/03/2019	C. Burke
5.0	Annual Revoew and Change	Annual Review and change from IS Team to IS Operations Team and Head of IS to Head of IS operations	26/03/2020	C. Styler
5.0	No Change	Annual Review	31/03/2021	C. Burke