Transport for Greater Manchester

Transport for Greater Manchester Policy

P10 – IS Physical Security Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2021	Document Reference no.	IS Physical Security Policy P10
Version No.	9.0	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 2021		Implementation date: 31st March 2021 Annual review date: 31st January 2022

Table of Contents

Policy Aims

This document details TfGM's policy in relation to protect TfGM's security of physical information and systems by setting standards for secure operations.

This document should be viewed in conjunction with TfGM's security policy: P01 - IS Security Policy.

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 (PCI DSS); and
- it maintains its relevance to the business' current and planned payment card processing operations.

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

c) Any changes to this policy will be communicated to TfGM's IS Operations Team and any other necessary 3rd Parties.

Purpose

a) Physical Security arrangements for organisations processing card data are extremely important.

b) This document details the standards employed by **TfGM** to ensure physical access to information, systems the cardholder data environment is appropriately secured and monitored.

Scope

a) The security standards and procedures required for physical security of the cardholder data environment is covered in this policy. These standards have been developed according to the standards set by the PCI DSS.

b) This policy applies to the physical security of **TfGM's** information systems, including, but not limited to, all **TfGM** managed network devices, servers, personal computers, mobile devices, and storage media.

c) This document provides operational guidelines for individuals having physical access to payment card processing networks at **TfGM**. This includes (and is not limited to):

- Permanent members of staff.
- Contract members of staff.
- Service Providers and Third Parties.
- Site Visitors

d) Any person working in or visiting **TfGM's** office is also covered by this policy.

For the purpose of this policy, the terms "media" or "physical media" shall refer (but not be limited to) computers, removable electronic media, tapes, disks, paper receipts, paper reports, and faxes.

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 Operations
- **Compliance**: All
- **Awareness**: All

Enforcement / Monitoring / Compliance

a) The physical security standards are in place to secure **TfGM**'s operations.

b) Adherence to physical security standards shall be monitored on a regular basis to ensure all operations are protected,

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

Policy

8.1 Physical Access Controls

8.1.1 Internal Perimeter

a) Any area containing hosts or systems with cardholder data shall be considered inside the *internal perimeter*.

b) The *internal perimeter* shall be subject to access controls, using badge-readers and other devices including authorised badges, and lock & key.

c) CCTV cameras and / or other access controls mechanisms will be used to monitor individual physical access to sensitive areas.

8.1.2 External Perimeter Entry/Exit Points

a) CCTV Cameras shall be placed within the external perimeter.

b) CCTV Cameras and access control systems shall be sufficiently secured to prevent physical tampering or disabling.

c) Recording the entry/exit points and shall be positioned to record in detail sufficient to later identify the person who gained access.

d) For shared environments such as a common server room in a shared office, or within a co-location facility, camera coverage should include any server rack access for front and rear doors.

e) The system that controls the identification badges must be strictly limitied to authorised personnel only. Access levels to be directly related to job functions of staff.

8.1.3 Central Server System Security

TfGM shall ensure that central (payment card processing) computing facilities only have physical entry points from within the building housing them.

8.1.4 Terminal & Console Security

When not in use, all machines contained within the internal and external perimeters must have any console access locked to prevent unauthorised use.

8.2 Identification

8.2.1 Distinction of Badges

TfGM shall ensure that badges issued to staff have a different appearance to those issued to visitors.

8.2.2 Staff

a) All staff shall wear identity badges when inside the building. These badges shall have the staff member's photograph and shall also be used as an access token to enter secured areas.

b) Staff forgetting their identity badges must obtain a temporary badge valid for a single day.

c) Identity badges or access cards lost or stolen must be reported immediately to Reception Desk.

d) Under certain circumstances staff may require greater access to the building or may need to change their access requirements, this can only be authorised with approval by the Directors.

e) Staff undergoing disciplinary procedures or have had their employment terminated shall be required to surrender their identification badge and be escorted from the premises.

f) **TfGM** has documented procedures or assigning badges to onsite personnel and visitors, and verify these processes include the following:

- Granting new badges.
- Changing access requirements.
- Revoking terminated onsite personnel and visitor badges.

8.2.3 Visitors

a) Visitor badges can only be issued from the Reception Desk and should be clearly distinguishable from staff badges.

b) Visitors must sign in at the reception, detailing who it is they are to see, which company they work for and their time of arrival.

c) Visitor badges shall only be valid on the day of issue.

d) All visitors to **TfGM** shall be issued with (and be required to wear) identity badges whilst on site.

e) Individuals without identity badge must be challenged by any member of staff.

f) Under special circumstances, the Directors may choose to authorise the issuing of access token to visitors to allow them access to restricted areas within the building. In this situation, the Reception Desk will record the issuing of an access token and retain the records in accordance with **TfGM's** access log process.

g) Upon leaving the building, or expiration of the badge, visitors shall return the badges to their named contact and sign out of the building.

h) The Third Parties are allowed to work unaccompanied in an assigned area of the building.

i) Visitors shall under no circumstances be allowed to move unaccompanied through the building.

j) Third Parties given access to the *Internal Perimeter* must be escorted at all times.

k) A visitor log must also be used to record physical access to computer rooms and data centres where cardholder data is transmitted.

Procedure for the above is documented in PR09 – Physical Security Procedure

8.3 Backup Security and Physical Media

8.3.1 Physical Data Security

a) Any physical media which contains confidential and sensitive information is logged and locked away in a secured area or storage unit to prevent unauthorised access when it is not being used.

b) **TfGM** shall only allow confidential and sensitive information to be transported on physical media if this movement is authorised by management and it is being transported from one secured area to another.

8.3.2 Logging

a) Any staff member who produces hard copy or transfers confidential and sensitive data to another medium must log the creation and document the date of destruction as defined in (PR06 – Back-up Procedure).

b) The **TfGM's Data Protection Officer** shall perform audits at least annually to inspect whether or not confidential and sensitive data have been destroyed and the pertinent paperwork completed.

8.3.3 Backups

c) **TfGM** shall store media backups in a secure location, preferably an off-site facility, and the locations security shall be reviewed at least annually.

d) **TfGM** shall conduct regular inventory checks of the offsite tape copy store to ensure that all media is accounted for and that it is secure and the storage remains fireproof.

e) The storage facilities security needs to be checked at least annually.

f) Details of any third parties that perform/store offsite card data backups: (also can be found F20 – Service Providers Log).

8.3.4 Secure Disposal of Physical Media

a) When no longer required for legal, regulatory, or business requirements Data which is subject to Access Controls must be disposed of in a secured fashion to avoid accidental leakage of confidential and sensitive information.

   i) Confidential and sensitive Data in Digital Format (Hard Disk, Backup Tapes etc.) shall be disposed of using secure delete facilities (e.g. write-rewrite multiple times) prior to the disposal of the hardware.

   ii) Backup media shall be physically destroyed prior to disposal to ensure data cannot be recovered from them.

   iii) Any physical media which contains *sensitive information* is logged and locked away in a secured area or storage unit to prevent unauthorised access when it is not being used.

   iv) **TfGM** shall only allow *sensitive information* to be transported on physical media if this movement is authorised by management and it is being transported from one secured area to another.

8.3.5 Hard Copy

a) PR10 – Cardholder Data Retention Procedure should be followed, during process, store and destrurct phases of hard copies of Confidential Data as a part of daily business operations and work flow of a business unit.

b) Confidential and Sensitive Data in hardcopy format must be shredded using a cross-cut shredder using a shred size that prevents cardholder data from being reconstructed, and the waste must then be disposed of securely.

c) Any Sensitive Data in hardcopy format that is to be retained needs to be logged and locked away in a secured area or storage unit to prevent unauthorised access when it is not being used.

d) **TfGM** shall ensure that Sensitive Data printed in any medium is destroyed as soon as possible in accordance with the **TfGM's** data disposal standards.

e) Any materials to be shredded shall be placed in a sealed bin marked for that purpose and the contents disposed of securely (in accordance with ISO 9564-1 or ISO 11568-3e). If a Third Party is used, they must be compliant with BS 8470:2006 (Secure Destruction of Confidential Material) and a Certificate of Destruction must be provided by the 3rd party.

8.4 Logs and Video Monitoring

8.4.1 Use of Video Monitoring

a) Video Surveillance shall be used to monitor access to and from the *External Perimeter* and record access into and out of the *Internal Perimeter.*

b) Video Surveillance shall be used to monitor access to all data centres, server rooms, or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only points of sale terminals are present, such as the cashier area in a retail store.

8.4.2 Retention of Logs and Videos

TfGM shall retain all logbooks, videos and written access records for a minimum of three months.

8.5 Infrastructure Protection

8.5.1 Communications Infrastructure

a) **TfGM** must disable all physical network sockets are not in use.

b) If a socket is required, then a request shall be made through the **IS Serviceline** for the **IS Operations Team** to activate the required port for the specified time.

c) **TfGM** shall ensure that all network infrastructure equipment necessary for **TfGM** to perform its functions is secured within the Internal Perimeter.

d) In the case of network equipment in other sections of the building, **TfGM** shall ensure that all data cabinets are locked at all times.

e) If Wireless access points are deployed within the **TfGM** CDE, they shall be sufficiently secured to prevent physical tampering.

f) **TfGM** shall ensure protection of power supplies to servers holding payment card data by means of use of a generator and or UPS.

g) **TfGM** shall ensure the security of cabling & cabinets transmitting and storing payment card data. Network cabling must not run through non-secured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).

8.5.2 IT Infrastructure

a) Certain physical precautions must be taken to ensure the integrity of **TfGM's** data.

b) At a minimum, the following guidelines must be followed:

i) Computer screens must be positioned where information on the screens cannot be seen by outsiders.

ii) Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorised to view the information.

iii) Users must lock their workstations whenever they leave the workstation unattended.

iv) Users must logoff or shut down their workstations when leaving for an extended time period.

v) Users must shut down their workstations prior to leaving the office.

vi) Users must shutdown their workstations at the end of the workday.

8.5.3 Protection of Devices

a) **TfGM** shall protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

b) **TfGM** shall as a minimum:

i) maintain a list of devices that interacts directly with the payment cards;

ii) inspect the listed devices every week to look for tampering or substitution;

iii) train staff to be aware of suspicious behaviour and to report tampering or substitution of devices.

8.5.4 Mobile & Wireless Devices

a) **TfGM** shall maintain a log of all mobile & wireless network devices.

b) These logs must detail which staff member is responsible for the device, when it was taken and when it is returned.

8.5.5 Facility Access

a) Access Control tokens used to gain entry to the building shall be configured according to the access requirements of the individual's job function.

b) The table below illustrates the allocation of access:

Role Name	Access	**Reference**
IS Service Line	All Floors (except roof)	IS Infrastructure Team
IS Operations Team	All Floors (except roof)	IS Infrastructure Team

Glossary and References

9.1 Glossary

See document P99 - Glossary

9.1.1 References

- P01 – IS Security Policy
- P09 – IS Key Management Policy Procedures

9.1.2 Procedures

- PR06 – Backup Procedure
- PR10 – Cardholder Data Retention Procedure

9.1.3 Forms

- F20 – Service Providers Log

Change control record: complete each time there is a change

P10: IS Physical Security Policy				
Version	**Change**	**Reason for change**	**Date**	**Name**
2.0	Version and Date	Annual Review	31/10/2013	C.Burke
3.0	Version and date	Annual Review	06/03/2014	C Burke
4.0	Update	Updated to include Version 3.0 and change variations	16/03/2015	C. Burke
5.0	Version and Date	Annual Review	31/03/2016	C. Burke
6.0	8.3.5	CHD Hardcopy handling, storage & descruction clarified	24/01/2017	C Burke
7.0	Version & Date	Annual Review	31/03/2017	C. Burke
8.0	Version and Date	Annual Review	11/03/2019	C. Burke
9.0	Annual Review & Change	Annual Change & change of Head of IS to Head of IS Operations and IS Team to IS Operations Team	26/03/2020	C. Styler
9.0	Version & Date	Annual Review	31/03/2021	C. Burke