Transport for Greater Manchester

Transport for Greater Manchester Policy

P02 Information Systems Security Audit Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2021	Document Reference no.	Information System Security Audit Policy P02
Version No.	6.0	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: Date:	Head of IS (Malcom Lowe) 31st March 2021		Implementation date: 31st March 2021 Annual Review Date 31st Jan 2022

Table of Contents

1. Policy Aims

a) This document details **TfGM's** policy with respect to audit activities.

b) This document should be viewed in conjunction with **TfGM's** Information Systems Security policy: P01 – IS Security Policy.

2. Review and Update of Policy Statement

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

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

   ii) it maintains its relevance to the business' current and planned credit card processing operations.

b) The **IS Team** will undertake the technical review of this policy statement and associated company Policies. The review will be reported to **TfGM's** Internal Audit Department.

c) Any changes to this policy will be distributed to all members of the **TfGM's IS Team** and other necessary stakeholders.

3. Purpose

This document identifies audit tasks that are performed by **TfGM** and approved third parties that perform audit tasks for **TfGM**.

4. Scope

a) This document identifies audit tasks that are performed by **TfGM**.

b) As per PCI compliance guidelines, **TfGM** performs the following PCI audit activities:

   i) Annual completion of the Payment Card Industry (PCI) On-site PCI Audit.

ii) Payment Card Industry Approved Scanning Vendors (ASV) scans. This is a quarterly vulnerability assessment performed by a qualified company to locate any weaknesses in an organisation's internet-facing infrastructure. Review Security Scanning procedures document at http://www.pcisecuritystandards.org for more information.

iii) External penetration testing of the cardholder data environment. See section 11.3 of the PCI Data Security Standard.

iv) Internal penetration testing of the cardholder data environment. See section 11.3 of the PCI Data Security Standard.

v) Internal vulnerability assessment of the cardholder data environment. See section 11.2 of the PCI Data Security Standard.

For more information on section 11.2 of the PCI Data Security Standard, see here: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

5. Policy Delivery

This policy will be delivered by **TfGM** IS Staff by internal communication and will be situated on the **TfGM** Intranet.

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

The following audit activities are performed by **TfGM**.

a) Payment Card Industry (PCI) Onsite Audit.

8.1 PCI Onsite Audit

a) **TfGM** has been identified as a level 1 Merchant that stores, processes or transmits Credit Card Data. As such, **TfGM** must successfully comply with the PCI DSS.

b) **TfGM** must successfully comply with the Data Security Standard on an annual basis. Compliance audits are performed by a registered Qualified Security Assessor (QSA).

c) QSA Contact Reference

Sec-1 Ltd
Unit 1, Centre 27 Business Park
Bankwood Way
Birstall
WF17 9TB
Tel: +44 (0) 1924 284 240

PCI Security Standards QSA reference:
https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

d) On-Site Activity Log of QSA

The log can be found on the form F20 – QSA Activity Log.

8.2 Payment Card Industry Approved Scanning Vendor Scans

a) **TfGM** has been identified as a level 1 Merchant that stores, processes and transmits Credit Card Data on behalf of multiple merchants. As such, **TfGM** must (successfully) perform external Vulnerability Assessment scans to PCI DSS standards. These scans are referred to as Approved Scanning Vendor (ASV) scans.

b) **TfGM** must successfully complete ASV scans on a quarterly basis. Audits are performed by a registered Approved Scanning Vendor (ASV).

c) ASV Contact Reference:

Sec-1 Limited
Unit 1 Bankwood Way
Birstall West
Yorkshire WF17 9TB
Tel: +44 (0) 134 466 8600

PCI Security Standards ASV reference:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php#

8.3 External Penetration Testing of the Cardholder Data Environment

a) As per section 11.3 of the PCI DSS, **TfGM** must perform a Penetration Test of all external entry points to its Cardholder Data environment(s). A full penetration test must be performed at least annually or after each major system upgrade.

b) External Penetration Test Contact Reference:

Sec-1 Ltd
Unit 1,
Centre 27 Business Park
Bankwood Way
Birstall

WF17 9TB
Tel: +44 (0) 1924 284 240

8.4 Internal Penetration Testing of the Cardholder data environment

a) As per section 11.3 of the PCI DSS, **TfGM** must perform a Penetration Test of the internal cardholder data environment(s). A full penetration test must be performed at least annually or after each major system upgrade.

b) Internal Penetration Test Contact Reference:

Sec-1 Ltd
Unit 1,
Centre 27 Business Park
Bankwood Way
Birstall
WF17 9TB
Tel: +44 (0) 1924 284 240

8.5 Wireless Access Points Scans

a) As per requirement 11.1 of the PCI DSS, **TfGM** must detect and identify any and all wireless access points, authorised or otherwise. This can be achieved either by using a wireless detection scanner (such as INSSIDER) or via a continuous monitoring system using technologies such as, wireless IDS/IPS or NAC (network access control).

b) In either case, the wireless solution must be capable of detecting the following:

- WLAN cards being inserted into system components
- Authorised and unauthorised wireless access points

c) If continuous monitoring is employed, then the system must be configured to generate alerts to **TfGM**.

d) If a scanning solution is employed, the scan must be conducted at least quarterly.

e) Perform a sweep of all physical locations in scope for audit for any wireless devices which may be connected to the Cardholder Data Environment. Such a scan must be conducted on a quarterly basis.

f) The scans to identify any rough wireless devices shall be conducted by a qualified staff member of **TfGM** using Kismet 2011.03R2 network detector, packet sniffer and intrusion detection application for 802.11 wireless LANs. Kismet application is an industry standard tool for mobile auditing troubleshooting Wi-Fi networks.

8.6 Internal Vulnerability Scanning of the CDE

a) As per section 11.2 of the PCI DSS, **TfGM** must successfully perform external Vulnerability Assessment scans to PCI standards, at least quarterly or after any significant change to the CDE.

b) The internal vulnerability scans shall be conducted by a qualified staff member of **TfGM** using Tenable 'Nessus' scanner, an industry approved vulnerability and configuration assessment product.

9. Glossary & References

9.1 Glossary

- See document P99-Glossary

9.2 References

9.2.1 Policies

- P01 – Information Systems Security Policy

9.2.2 Procedures

Nil

9.2.3 Forms

- F20 - QSA Activity Log.
- F21 - ASV Scans Activity Log.
- F22 - Internal Vulnerability Scans Activity Log.
- F23 - External Penetration Test Activity Log.
- F24 - Internal Penetration Test Activity Log.
- F25 - Wireless Access Point Scan Activity Log.
- F35 – Authorised Wireless Access Points Inventory.

Policy: P02 – IS Security Audit Policy				
Version	**Change**	**Reason for change**	**Date**	**Name**
2.0	Version & Date	Annual Review Update	31/10/2013	C. Burke
3.0	Version & Date	Annual Review Update	06/03/2014	C. Burke
3.1	Update	Updated to include Version 3.0 change variations	16/02/2015	C.Burke
3.2	Update	8.2c 8.3b & 8.4b Change of supplier address	17/09/2015	J. Singleton
3.3	Update	Annual Review Update	31/03/2016	C. Burke
4.0	QSA	New QSA	14/11/2015	C. Burke
4.1	Update	A new form number for Authorised Wirless Access Points inventory	11/01/2017	C. Burke
4.2	Version & Date	Annual Review new Head of IS	31/03/2017	C. Burke
5.0	Annual Review	Annual Review	31/03/2018	C. Styler
6.0	Update	Changed Tier 2 Merchant to Level 1 & Annual review	18/02/2019	C.Styler
6.0	No Change	Annual Review	11/03/02019	C. Burke