Transport for Greater Manchester

Transport for Greater Manchester Policy

P12 Penetration Testing Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	11th March 2019	Document Reference no.	P12 Penetration Testing Procedure P12
Version No.	4.0	Prepared by:	Claire Styler, Catherine Burke & Rohan Mendis
Equality Impact Assessment	Validation of Initial Screening Equality Officer: Muhammad Karim		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 (Malcolm Lowe) 31st March 2018		Implementation date: 31st March 2018 Annual review date: 31st January 2020

1 Policy Aims 2
2 Review and Update of the Policy Statement 2
3 Purpose 2
4 Scope 3
5 Policy Delivery 3
6 Accountability 3
7 Enforcement / Monitoring/Compliance 3
8 Policy 4
8.1 General Approach to Testing 4
9 Overall responsibility 4
9.1 Testing Coverage 4
9.2 Extent of Testing 5
9.3 Frequency of Testing 5
9.4 Testers 6
9.5 Review and Processing of results 6
10 Glossary and References 7
10.1 Glossary 7
10.2 References 7

1 Policy Aims

a) This document details **TFGM's** policy with respect to penetration testing the cardholder data environment.

b) This document, supported by PR12 – Penetration Testing Procedure constitutes **TfGM's** penetration Testing methodology.

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's IS Team** to ensure:

- The business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS).
- Application and network components supporting the Cardholder Data Environment are periodically reviewed to identify any security weaknesses that might adversely affect business operations.
- **TfGM** maintains its relevance to the business' current and planned payment card processing operations.

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

3 Purpose

a) This document identifies how TfGM performs penetration testing against its cardholder data environment to identify security weaknesses.

b) Penetration Testing supports TfGM's security best practice by confirming the controls protecting the storage, processing or transmission of Cardholder Data are effective and keep pace with i) changes to both the Cardholder Data Environment and ii) newly identified security vulnerabilities.

c) The frequency and nature of penetration testing meets with PCI DSS testing controls detailed in section 11.3 of the PCI DSS.

4 Scope

This document identifies the targets and testing tasks required for **TfGM** to complete penetration testing to meet PCI DSS requirements**.**

The policy and supporting procedures contain the following considerations:

- Purpose of penetration testing. Overall objectives.
- Industry standards employed during penetration testing.
- Definition of targets for penetration testing.
- Staff and third parties used in the testing process.
- Frequency of penetration testing.
- Dissemination, processing and follow up of test results.

5 Policy Delivery

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

6 Accountability

- Responsible to the board: IS Director
- 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 General Approach to Testing

Penetration testing is a key tool that is used to identify threats to the Cardholder Data Environment. To ensure that test techniques and tools meet an acceptable level of assessment, the following standards are used to define an acceptable level of testing:

- NIST Technical Guide to IS Testing and Assessment (Special Publication 800-115). Referenced at http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf
- Application vulnerabilities as detailed in Open Web Application Security Project (OWASP). Specific reference to attack references found at: https://www.owasp.org/index.php/Category:Attack

9 Overall responsibility

The person with overall responsibility for Penetration Testing at **TfGM** is **the IS Security Technician.**

Responsibilities will include:

- Selection of testers.
- Scheduling tests.
- Identifying test targets.
- Primary point of contact during test exercises.
- Receipt and dissemination of test results and reports.
- Scheduling re-tests as required.

9.1 Testing Coverage

TfGM has two categories of penetration testing.

d) Internal Testing. To assess the security of the internal network and the internal interfaces to the Cardholder Data Environment. This will also include assessing any segmentation configuration that supports the reduction of scope of the Cardholder Data Environment.

e) Testing performed from within TfGM's internal network. Testing to be performed against the internal Cardholder Data Environment network boundary and also inside the Cardholder Data Environment.

Internal targets are detailed in PR12-Penetration Testing-Procedure & F21 - Penetration Test Targets.

9.2 Extent of Testing

All network and application components that are contained in or are directly connected to the Cardholder Data Environment will be tested.

A complete list of internal and external targets are detailed in F21 - Penetration Test Targets.

Testing will consist of the following types / categories of testing:

- Network Testing. Specific network tests are detailed in PR12-Penetration Testing-Procedure.
- Application Testing. Specific application tests are detailed in PR12-Penetration Testing-Procedure.
- Wireless Testing. Specific wireless tests are detailed in PR12-Penetration Testing-Procedure.

9.3 Frequency of Testing

The Cardholder Data Environment must be Penetration Tested at least annually. This penetration test will consist of all components as listed in 9.2.

The date for penetration testing and the associated preparation and execution tasks are detailed in Network Testing. Specific network tests are detailed in PR12-Penetration Testing-Procedure.

New applications, networks or significant changes to existing Cardholder Data Environment components must undergo penetration testing at the time of the change being promoted to the 'live' or Production environment. In these cases testing of all new or changed components will be performed in:

- A Pre-production test environment that accurately reflects the existing live Cardholder Data Environment.
- On go-live in the production Cardholder Data Environment. In these cases, testing must be completed and all high level vulnerabilities fixed within 30 days of detection.

A significant change is considered to be a change that impacts the storage, processing or transmission of Cardholder Data in any way. **TfGM** recognises that this could be:

- A new system component is introduced to the Cardholder Data Environment. For example a new server or servers.

- A new sub network that is directly connected to the Cardholder Data Environment.
- Major release changes to applications or operating systems that support the Cardholder Data Environment.

9.4 Testers

Penetration Testing is performed by 3rd Party Approved companies

Currently **Sec-1** performs all penetration testing against the Cardholder Data Environment. The organisation has the following security testing credentials:

- CREST Registered Penetration Tester
- CREST Certified Infrastructure Tester
- CREST Certified Web Application Tester

9.5 Review and Processing of results

All penetration test results will be detailed in a comprehensive report. The results will be rated, clearly showing all high, medium and low severity vulnerabilities.

All high level vulnerabilities identified during test exercises will be immediately communicated to **IS Security Technician at TfGM.**

IS Security Technician will communicate all penetration test report results to the following teams.

- IS Management Team
- Server Infrastructure and Data Storage Team
- Telecommunications and Networks Team

All high level vulnerabilities identified during testing will be addressed as soon as possible. Once the vulnerability has been fixed a further retest will be commissioned within **30 days** to confirm the fix has been successful.

Further re-tests will be commissioned until any high vulnerabilities are confirmed as fixed.

Penetration Test reports will be held **in the PCI-DSS SharePoint site** for a minimum period of **5 Years.** Results will be held under the control **of the IS Security Technician.**

An annual review, performed within 30 days of completion of the annual penetration test, will review all potential and identified threats to the Cardholder Data Environment. Penetration Test results will support this review, along with ASV scanning results, systems patching results, hardware and software vendor communications and general IT security industry updates.

10 Glossary and References

10.1 Glossary

See document P99 - Glossary

10.2 References

- P01 - Information Security Policy
- PR12 - Penetration Testing Procedure
- F21 - Penetration Test Targets

Policy: P12 Penetration Testing				
Version	**Change**	**Reason for change**	**Date**	**Name**
1.0		Initial Version	31/05/2015	J. Singleton
2.0	Date and version	Annual Review	31/03/2016	C. Burke
3.0	Date and Version	Annual Review	31/03/2017	C. Burke
4.0	Date Reviewed	Annual Review	11/03/2019	C.Burke