Transport for
Greater Manchester

Transport for Greater Manchester Policy

IS Test Security System Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	6th March 2014	Document Reference no.	IS Test Security System Policy Ref No. 025
Version No.	3.0	Prepared by:	Catherine Burke/Jude Singleton
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:	IS Director		Implementation date: 31st March 2014
Date:			Annual review date: 31st January 2015

Table of Contents

1 Policy Aims

To establish the security testing requirements for **TfGM's** multi service network.

2 Policy Scope

This will apply to the **TfGM's** multi service network, including the Manmetro TVM system components and Cardholder data in line with PCI requirements.

3 Policy Delivery

The tests will be carried out by an approved third party ASV (Approved Scanning Vendor)

4 Accountability

- **Responsible to the Board:** IS Director
- **Compliance:** IS Operations
- **Awareness:** IS Department

5 Policy Monitoring/ Compliance

a) This policy will be enforced by the Executive.

b) Information including logon dates, times, usage duration and device identity will be logged and maybe used for monitoring purposes, and 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.

d) In extreme circumstances Audit & Assurance may access equipment or information to help support investigations.

6 Policy

Security testing shall be performed on a periodic basis to ensure that information resources are adequately protected. The security testing policy applies to all systems/applications, the network and the physical infrastructure to evaluate the effectiveness of the security measures and controls implemented.

The following types of test will be carried out.

1.) Network Mapping

Network mapping involves using a port scanner to identify all active hosts connected to an organisation's network, network services operating on those hosts (e.g., file transfer protocol and hypertext transfer protocol), and the specific application running the identified service. The result of the scan is a comprehensive list of all active hosts and services.

2.) Vulnerability Scanning

Vulnerability scanners identify not just the hosts and open ports but any associated vulnerabilities automatically instead of relying on human interpretation of the results. Most vulnerability scanners probe for a finite number of problems and attempt to provide information on mitigating discovered vulnerabilities. Vulnerability scanners can be either network scanners or host scanners.

3.) Penetration Testing

Penetration testing is security testing in which evaluators attempt to circumvent the security features of a system based on their understanding of the system design and implementation.

4.) Password Cracking

Password cracking programs can be used to identify weak password usage.

5.) File Integrity Checkers

A file integrity checker computes and stores a checksum for every file to be protected and establishes a database of the checksums. It provides a tool for system administrators to recognise when changes were made to files, particularly unauthorised changes.

6.) Anti-Virus and Malicious Code Detection

Anti-Virus software programs shall be installed to protect both the network and systems in the operating environment

7.) Wireless Security

Scanning software will be used to detect the use of unauthorised wireless devices that might be used to bypass existing security measures

8.) Physical Access Testing

Physical access testing (both perimeter and internal) shall be performed on a periodic basis. This will check that internal and external barriers and access controls cannot be breached.

9.) Annual Tests

Network layer and Application layer penetration tests as described in above must be carried out at least annually in both the **TfGM** and MANMETRO cardholder data environment.
In the case of any significant changes within the cardholder environment retesting must be carried out immediately afterwards.

10.) Quarterly Tests

A review of all the facilities that make up the cardholder environment must be made every quarter. The immediate vicinity of these facilities must be scanned to detect any rogue wireless devices.

Internal and external network vulnerability scans must be conducted by an Approved Scanning Vendor (ASV) in the cardholder environment every quarter.

Physical Access Tests should be done at least quarterly. Between tests staff should be always vigilant to ensure that no breaches occur.

11.) Intrusion Prevention

An intrusion prevention system with up to date engines should be present within the cardholder environment to monitor all traffic. This system must alert personnel to all suspected compromises.

12.) File Integrity Monitoring Software

File integrity Monitoring software must be present to alert personnel to unauthorised modification of critical system files, configuration files or content files.
The software should be configured to perform critical file comparisons at least weekly.

13.) Log Reviews

Various system logs (e.g., firewall logs, IDS logs, server logs) can be used to identify deviations from security policy. In conjunction with security testing, log review and analysis will provide a more comprehensive evaluation of the operational environment.

7 Definitions

File Transfer Protocol: is a standard network used to copy a file from one to another.

Hyper Text Transfer Protocol: is a networking protocol for distribution, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.

Wireless Device: A wireless device can refer to any kind of communications equipment that does not require a physical wire for relaying information to another device.

- *Change control record: complete each time there is a change*

Policy/Procedure:				
Version	**Change**	**Reason for change**	**Date**	**Name**
3.0	Date and Version	Annual Review	06/03/2014	C Burke