Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Technology Usage Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2019	Document Reference no.	IS Technology Usage Policy Ref No. 026
Version No.	7.0	Prepared by:	Catherine Burke
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 2019		Implementation date: 31st March 2019 Annual review date: 31st January 2020

Table of Contents

1 Policy Aims

To establish secure technology usage guidelines for PCI DSS compliance

2 Policy Scope

This policy applies to **TfGM's** cardholder data environment, including all supporting servers, infrastructure equipment and network connections.

3 Policy Delivery

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

4 Accountability

- **Responsible to the Board:** Head of IS
- **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

6.1 Technology Usage

TfGM should establish, publish, maintain and disseminate a security policy that accomplishes all PCI DSS requirements with an annual risk assessment process that identifies threats, vulnerabilities, and results in a formal risk assessment.

6.2 Authentication

a) Authentication with unique user ID and password or other authentication items (for example, token) is required for use of all technology. The use of group and shared passwords are expressly forbidden.

b) There should be a control process for additions, deletions and modifications of user ID's, credentials and other identifier objects.

c) First time passwords should be set to a unique value for each user and changed immediately after the first logon, with the password complexity feature enabled within the domain.

d) All inactive user accounts over 90 days old should be disabled or deleted.

6.3 Technology Management

- A list of all devices should be available, along with details of personnel authorised to use the devices.
- All devices should be labelled, with details of owner, contact information, and purpose.
- Acceptable uses of the technology should be established for each device.
- Acceptable network locations should be established for the technologies, with consideration given to physical security.
- Only products from the **TfGM** approved list may be used.
- The use of WEP should be precluded if a wireless network should be connected to the cardholder data environment.

6.4 Remote Access

a) Where remote access is used to connect to the TVM Network, two factor authentication must be used for all employees, administrators and service providers.

b) Automatic disconnection of sessions must be activated after 10 minutes of inactivity.

c) Where remote access is used by third party vendors, it is required that the remote access technologies are activated only when needed by vendors, with immediate deactivation after use.

d) Any password resets will only be carried out centrally at the **TfGM** IS Serviceline on request by the user and after verification of the user identity.

e) It is strictly forbidden to copy, move or store cardholder data on to local hard drives and removable electronic media when accessing such media via remote access technologies.

7 Definitions

Authentication: A security method used to verify the identity of a user and authorise access to a system or network.

PCI DSS: The Payment Card Industry Data Security Standard is worldwide information security standard defined by the Payment Card Industry Security Standards Council. The standard is created to help the payment card industry organisations that process card payments and prevent credit card fraud through increased controls around data and its exposure to compromise.

TVM: Ticket Vending Machine - self-service railway ticket system**.**

WEP: Wired Equivalent Privacy is a deprecated security algorithm for IEEE 802.11 wireless networks.

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

Policy/Procedure:				
Version	**Change**	**Reason for change**	**Date**	**Name**
1.0	Date & Version	Review	31/10/2013	C Burke
2.0	Date & Version	Review	31/03/2014	C Burke
3.0	Date & Version	Review	30/04/2015	C Burke
4.0	Date & Version	Annual Review	31/03/2016	C Burke
5.0	Date & Version	Annual Review, new Head of IS	31/03/2017	C Burke
6.0	Date & Version	Annual Review	31/03/2018	C Styler

7.0	Date & Version	Annual Review	31/03/2019	C Styler