Transport for Greater Manchester

Transport for Greater Manchester Policy

P06 – IS Acceptable Use Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	26th March 2022	Document Reference no.	IS Acceptable Use Policy P06
Version No.	7.0	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:	Head of IS Operations (Ricard Fuertes)		Implementation date: 31st March 2022
Date:	31st March 2022		Annual review date: 31st January 2023

Table of Contents

1 Policy Aims

a) This document describes what is acceptable usage on **TfGM's** Information Systems.

b) This document details **TfGM's** policy in relation to acceptable use of networks and applications residing within the networks that store, process and transmit payment card data. These procedures have been developed according to the standards as set by the Payment Card Industry Data Security Standard.

c) This document should be viewed in conjunction with:

- **TfGM's** top level security policy: P01 – IS Security Policy.
- **TfGM's** E-mail policy, published on the corporate Intranet.
- **TfGM's** Acceptable Use Policy, published on the corporate Intranet.

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 Operations Team** ensure:

- Appropriate usage of IS Systems resources including, but not limited to, computer systems, email, internet and the network.
- the business meets its compliance obligations to the Payment Card Industry Data Security Standard (the PCI DSS), and

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

b) The **IS Operations Team** will undertake the review of this policy statement and associated company Policies.

3 Purpose

a) The purpose of the policy is to outline the acceptable use of card data processing computer systems of **TfGM**.

b) These rules are in place to protect both employees and **TfGM**, as inappropriate use exposes **TfGM** to risks including virus attacks, compromise of network systems & services, and legal issues.

4 Scope

a) This policy applies to **TfGM**'s networks including any and all IS resources, email, internet and systems processing card data that are accessed by employees, contractors, consultants, temporaries, and other workers at **TfGM**, including all personnel affiliated with third parties.

b) This policy applies to all associated equipment that is owned or leased by **TfGM**.

5 Policy Delivery

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

6 Accountability

i) **Responsible to the Board**: Head of IS Operations

ii) **Compliance**: All Staff

iii) **Awareness:** All Staff

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

a) **TfGM** is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

b) Electronic systems are the property of **TfGM** and are only to be used for business purposes. Serving the interests of the company, clients and customers in the course of normal operations. Please refer to **TfGM's** internal Information System policies for further details.

c) Effective security involves the participation and support of every employee and affiliate who deals with card processing systems. Each employee has a duty to know these guidelines, and to conduct their activities accordingly.

8.2 Duty of Care

a) Whilst **TfGM** shall ensure that all necessary and prudent measures are taken to secure its infrastructure from attack, it is the user's individual responsibility to maintain the confidentiality of his or her account.

b) Each User must not disclose their password(s) to anyone under any circumstances.

c) If a User knows or suspects that their account password has been compromised, they must immediately inform the IS Lead Compliance and Security Analyst or Head if IS Operations of their concerns and carry out the instructions issued to them by the IS Operations Team.

8.3 Acceptable Locations of Resources

a) Users shall not move equipment from their installed locations without prior authorisation from the **Head of IS Operations**.

b) Users shall only have access to those machines that their roles entitle them to, provided that all pertinent paperwork has been completed and signed off by the necessary parties.

8.4 Acceptable Use of Resources

8.4.1 General Use and Ownership

a) While **TfGM's** network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on card data system(s) remains the property of **TfGM** Because of the need to protect **TfGM's** network, management cannot guarantee the confidentiality of information stored on any network device belonging to **TfGM**.

b) **TfGM** must define guidelines concerning the use of devices and systems used to access the cardholder data environment, including remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data / digital assistants (PDAs), PEDs, e-mail and Internet usage.

c) The **IS Operations Team** recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see P08 Information Classification Policy.

d) It is expressly forbidden to connect mobile and non-company-owned (private) devices to the company network, and any non-compliance would be dealt with by the **TfGM** disciplinary processes.

e) For security and network maintenance purposes, authorised individuals within **TfGM** may monitor equipment, systems and network traffic at any time.

f) **TfGM** reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

g) Persons with authorised business need to view or process cardholder data shall protect the Cardhoder Data in accordance with all applicable PCI DSS Requirements.

8.4.2 Internet Access

a) The access provided to the Internet (e.g. World Wide Web access) is for the sole purpose of conducting the functions of the employee's role.

b) **TfGM** accepts that Employees may wish to use the Internet for personal reasons and request that such activity is limited to lunch periods or breaks.

c) **TfGM** have outlined the restrictions on use of e-mail and internet services within the **TfGM** E-mail Policy and Internet use Policy.

d) TfGM does not permit Cardholder Data, encrypted or uncrypted to be sent by end user messaging technologies or similar technologies under any circumstances.

8.4.3 Software

a) Software provided by **TfGM** will only be used on machines owned or operated by the Company.

b) Software licences procured by **TfGM** shall be monitored by the IS Department.

c) **TfGM** uses Auditing and Security software to ascertain whether installed software is legal. Unauthorised and illegal software will be deleted and the source will be ascertained and disciplinary action may be taken.

8.5 Remote Working

The Acceptable Use Regulations shall apply to members of staff accessing the cardholder data environment remotely.

8.6 Server Usage

a) Machines that have access to the **TfGM** network that hold shared resources shall be considered to be a Network Servers.

b) Network Servers deemed to be part of the Cardholder Data Environment shall be isolated from other networks.

c) Only those deemed as having the need to know shall have access to servers containing or processing Cardholder Data.

d) Servers shall only perform one role on the network. Exceptions to this would be if one role requires the presence of another role (e.g. an Intrusion detection service requiring an email service to be present).

e) The Acceptable Use Regulations shall apply to members of staff accessing network servers.

9 Glossary & References

9.1 Glossary

See document – P99 Glossary

9.1.1 References

- P01 – IS Security Policy
- P08 – IS Information Classification Policy

Policy: P06 – IS Acceptable Use Policy				
Version	**Change**	**Reason for change**	**Date**	**Name**
2.0	Date & Version	Update policy	31/10/2013	C.Burke
2.1	Date & Version	Update Policy	06/03/2014	C.Burke
3.0	V2-V3	Change variations to version 3.0	16/02/2015	C Burke
3.1	Role names	Department name change	10/08/2015	J Singleton
3.2	Date & Version	Annual Update	31/03/2016	C. Burke
3.4	8.4.d) 8.4.1	Deleted not used activity Protection of Cardholder Data	24/01/2017	C Burke
4.0	Date & Version	Annual Review	31/03/2017	C. Burke
5.0	Date & Version	Annual Review	31/03/2018	C. Styler
6.0	Date & Change	Annual Review & changed IS Infrastructure Manager to Head of IS	19/02/2019	C. Styler
6.0	No Change	Annual Review	11/03/2019	C. Burke

7.0	Annual Review and change	Annual Review & changed Head of IS to Head of IS Operations, IS Team to IS Operations Team and IS Security Officer to Lead Compliance and Security analyst	26/03/2020	C. Styler
7.0	Annual Review	No Change	31/03/2021	C. Burke
7.0	Annual Review	Date & Version	31/03/2022	C. Burke