Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Remote 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 Remote Policy Ref No. 021
Version No.	8.0	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

a) This policy defines standards for accessing **TfGM's** information systems resources from outside the network. This includes access for any reason from the employee's home, remote working locations or while travelling.

b) The purpose is to define how to protect information assets when using an insecure transmission medium.

2 Policy Scope

a) It is often necessary to provide access to information resources to employees or others working outside **TfGM's** network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly.

b) The scope of this policy covers all employees, contractors, and external parties that access **TfGM's** resources over a third-party network, whether such access is performed with **TfGM's**-provided or non-**TfGM's**-provided equipment.

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 Prohibited Actions

1. Remote access to IS systems is only to be offered through a secure **TfGM**-provided means of remote access. The following are specifically prohibited:
2. Installing a modem, router, or other remote access device on a **TfGM** system without the approval of the Head of IS or the IS Director.
3. Remotely accessing corporate systems with a remote desktop tool, such as VNC, Citrix, or GoToMyPC without the approval of the Head of IS.
4. Use of non-**TfGM**-provided remote access software.
5. Split Tunnelling to connect to an insecure network in addition to the **TfGM** network, or in order to bypass security restrictions.

7 Use of non-TfGM's-provided Machines

Accessing the network through home or public machines can present a security risk, as **TfGM** cannot completely control the security of the system accessing the network. Use of non-**TfGM**-provided machines to access the network is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

- It has up-to-date antivirus software installed on a daily basis.
- Its software patch levels are current.
- It is protected by a firewall.

When accessing the network remotely, users must not store confidential information on home or public machines.

8 Client Software

a) **TfGM** reserve the right to determine which users may have remote access client software; this will be determined on the business need for accessing IS systems remotely.

b) Unless provided by default, users requiring remote access should document their needs in a request to the Head of IS, who will determine if the request is feasible from a security and technology perspective, and will be responsible for deploying any necessary remote access in such a manner that is consistent with the security strategy.
c) At a minimum, the software will include data encryption with industry-standard encryption algorithms. Additional security options, such as a bundled client firewall, can be included at the discretion of the Head of IS.

9 Network Access

There are no restrictions on what information or network segments users can access when working remotely, however the level of access should not exceed the access a user receives when working in the office.

10 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the network must be timed out after 10 minutes of inactivity.

11 Enforcement

This policy will be enforced by the Executive and violations may result in disciplinary action in accordance with TfGM disciplinary policy.

12 Definitions

Modem: A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access: The act of communicating with a computer or network from an off-site location. Often performed by home-based or travelling users to access documents, email, or other resources at a main site.

Split Tunnelling: A method of accessing a local network and a public network, such as the Internet, using the same connection.

Timeout: A technique that drops or closes a connection after a certain period of inactivity.

Two Factor Authentication: A means of authenticating a user that utilises two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

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

Policy/Procedure:				
Version	Change	Reason for change	Date	Name
3.0	Date & version	Annual Review	06/03/2014	C Burke
4.0	Date & Version	Annual Review	30/04/2015	C Burke
5.0	Date & Version	Annual Review	31/03/2016	C Burke
6.0	Date & Version	Annual Review	31/03/2017	C Burke
7.0	Date & Version	Annual Review	31/03/2018	C Styler
8.0	Date & Version	Annual Review	31/03/2019	C Styler