Transport for Greater Manchester

Transport for Greater Manchester Policy

002 IS Access Control Policy

Warning:

Printed copies of this document are uncontrolled

Check issue number on Intranet before using.

Date Prepared:	31st March 2020	Document Reference no.	IS Access Control Policy 002
Version No.	8.0	Prepared by:	IS/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: Date:	Head of IS (Malcolm Lowe)		Implementation date: 31st March 2020 Annual review date: 31st January 2021

Table of Contents

1 Policy Aims

a) This policy is to describe the steps that must be taken to ensure that users connecting to **TFGM's** network are authenticated in an appropriate manner, in compliance with **TFGM** standards, and are given the appropriate level of access required to perform the duties they are carrying out at that point.

b) This policy specifies what constitutes appropriate use of network accounts and authentication standards.

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:

- Appropriate usage of IS Systems resources including, but not limited to, computer systems, email, internet and network access.

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

3 Purpose

a) Network access and authentication are critical to **TFGM's** information security and are often required by regulations or third-party agreements.

b) Any user accessing **TFGM's** computer systems has the potential to affect the security of all users of the network.

c) An appropriate IS Network Access and Authentication Policy reduces the risk of security incidents by requiring consistent application of authentication and access standards across the network.

4 Scope

a) This policy applies to users wishing to access **TfGM**'s resources and assets, this applies to employees, contractors, consultants, and other workers at **TfGM**, including all personnel affiliated with third parties.

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

ii) **Compliance**: All Staff

iii) **Awareness:** All Staff

7 Enforcement / 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.

8 Policy

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

1. A Staff Approval Form will need to be completed by a line manager and sent to HR.
2. A Service Request Form will need to be completed by the employees line manager and sent to Serviceline.
3. Serviceline will complete the account set-up upon receipt of an approved Service Request Form and when the Staff Approval Form has been processed by HR.
4. Access to the network will be granted in accordance with the policies referenced and contained within the IS Intranet area. Additionally, users acceptance of the policies is a mandatory requirement accessed from within the Learning Portal.

8.1 Account Use

Network accounts must be implemented in a standard fashion and utilised consistently across **TFGM**. The following policies apply to account use:

1. Accounts must be created using a standard format using the Lastname-initial, or an appropriate variation if a conflict with an existing username exists.
2. Accounts must be password protected (refer to the - **TfGM** Password Policy for more detailed information).
3. Accounts must be for individuals only. Account sharing and group accounts are not permitted under any circumstances.
4. User accounts must not be given administrator or local admin access unless this is necessary to perform their job function.
5. Guests must have a legitimate business need for access to the network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time and disabled when the guest's work is completed by setting an expiry date on the account.

6. Individuals requiring access to confidential data must have an individual account, and a purpose, any request but be signed off by their line manager and data owner.
7. Where administration privileges are required then a separate administration account must be set up and assigned to an individual.

8.2 Account Termination

Line-managers must inform the Human Resources Department, of any staff leavers, upon updating the SAP HR system. Serviceline will be automatically informed of the staffing change, which includes employment termination, or a change of job function (e.g. promotion, demotion, etc.).

Any staff members that are not added to the SAP system, must have their accounts set up with an expiration date that is appropriate to the expected duration the account is required and in use.

8.3 Authentication

User machines must be configured to request authentication against the domain at start-up. If the domain is not available or authentication for some reason cannot occur, then the machine must not be permitted to access the network.

8.4 Use of Passwords

When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document.

An effective and secure password requires a necessary degree of complexity to make it effective and the longer a password, the more difficult it is to crack (bigger is better).

TfGM system passwords must be a minimum length of 8 Characters and must include 3 out of the 4 character types below:-

1. An upper case letter
2. A lower case letter
3. A number from 0 to 9
4. A symbol e.g. " ! £ $ % & * ? @ # "

Any part of a username cannot be included in the password, and passwords will be required to change every 90 days.

8.5 Remote Network Access

All users accessing the network remotely must adhere to the IS Remote Access Policy.

8.6 Minimum Configuration for Access

Any machine that does not adhere to **TFGM** standards with regards to antivirus software and patch levels should not be attached to the network; this will ensure that vulnerabilities, virus, or other malware is not inadvertently introduced to the network. Any deviation to this may result in disciplinary action.

8.7 Encryption

Authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to **TFGM's** network or across a public network such as the Internet.

8.8 Failed Logons

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, accounts are locked out after 5 unsuccessful logins.

9 Definitions

Antivirus Software: An application used to protect a computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

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

Encryption: The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Password: A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

Change control record: complete each time there is a change

Policy/Procedure:				
Version	Change	Reason for change	Date	Name
1.1	4.0	ipads	31/10/2013	C. Burke
3.0	Date and Version	Annual Renewal	31/03/2014	C. Burke
4.0	Date and Version	Annual Review	30/04/2015	C. Burke
5.0	Date and Version	Annual Review	31/03/2016	C. Burke
6.0	Date and Version	Annual Review, new Head of IS	31/03/2017	C. Burke
7.0	Date and Version	Annual Review	31/03/2018	C. Styler
8.0	Date and Version	Annual Review	31/03/2019	C. Styler
8.1	Date & Version	Annual Review (8.5 Reviewed in-line with COVID-19).	321/03/2020	C. Burke