Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Systems and Administrative Password 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 Systems and Administrative Password Policy Ref No. 023
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

.....0
Table of Contents 1
1 Policy Aims.....2
2 Policy Scope 2
3 Policy Delivery 2
4 Accountability.....2
5 Policy Monitoring/ Compliance.....2
6 Policy.....3
6.1 Password Requirements.....3
7 Password Protection Standards.....4
8 Application Development Standards.....5
9 Use of Passwords and Passphrases for Remote Access Users 6
10 Enforcement 6
11 Definitions.....7

1 Policy Aims

To provide clear instructions in providing a secure logon password requirement for system and administrative accounts.

2 Policy Scope

This applies to all system-level and administrative passwords (e.g. Domain and Local administrative accounts, root, service accounts, application administration accounts, etc).

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

All existing passwords will be changed to fall in line with this policy and will be enforced by group policy. All systems password will be subject to controlled penetration tests by authorised third party testers using password cracking programs to identify weak password usage. Should a breach of policy be identified, it may be used in disciplinary proceedings.

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

Systems Passwords

6.1 Password Requirements

a) All system-level passwords (e.g. Local administrative accounts, root, service accounts, application administration accounts, etc.) must be changed on at least an annual basis. They must be changed immediately if a security breach is suspected. Default password not permitted.

b) All system-level passwords must be accurately typed and stored in the passwords book and kept in the safe at all times. Any sensitive passwords must be kept in a sealed envelope. The date the password was issued must be recorded along with any password change and documentation of any dependencies. When accessing a password, the book must be replaced immediately afterwards.

c) All internal IS domain administrative user accounts must be changed every 60 days, or immediately if a security breach is suspected.

d) All system-level passwords must be unique and accounts must not be used for multiple systems.

e) Passwords must not be inserted into email messages or other forms of electronic communication.

f) For all equipment and systems, any system defaults must be changed to strong values only known by **TfGM**. This applies to any work carried out during network and system implementation and configuration tasks, especially within any cardholder data environments.

g) Where SNMP is used, the community strings must be defined as something other than the standard defaults of 'public', 'private' and 'system' and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

System Passwords are used for various purposes at **TfGM**. Some of the more common uses include administrative accounts, Service accounts, SQL application logon accounts, Web console login accounts, Switch and Router logins, 3rd party VPN access and

unloading of antivirus. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once,) strong passwords must be used

System Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*() +|~-=|'{}[]:";<>?,./
- Are at least fifteen alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family etc.
- Are randomly generated using a software password generator such as PC Tools password Utilities
- Exceptions to this may be where the password is needed to be used frequently to login to administer a system, such as CCTV or Messagelabs, in this case a randomly generated password may be too cumbersome and the password may be relaxed to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phase. For example the phrase might be: 'ThisMayBeOnToRemember' and the password could be: '?TmB1w2R' with some others added to make up the digits.

7 Password Protection Standards

a) DO not use the same password for **TfGM** accounts as for non **TfGM** access (e.g., personal internet account,) where possible, don't use the same password for various **TfGM** access needs. For example, select one password for the Websense service account and a separate password for other service accounts. Also, select a separate password to be used for a server Local Administrator account and workstation Local Administrator account.

b) Where possible enable domain Active Directory authentication for administering systems, so as an audit trail can be established.

c) Do not share **TfGM** passwords with anyone, including IS staff. All passwords are to be treated as sensitive.

Sample set of rules to be followed;

- Do not reveal a password over the phone to ANYONE
- Do not reveal a password in an email message
- Do not reveal a password to the boss
- Do not talk about a password in front of others

- Do not hint at the format of a password (e.g., my family name)
- Do not reveal a password on questionnaires or security forms
- Do not share a password with family members
- Do not reveal a password to co-workers while on vacation

a) If someone demands a password, refer them to this document or to the IS Security Officer.

b) Do not use the 'Remembered Password' feature of applications (e.g., Internet explorer, Outlook, Netscape Messenger).

c) Again, do not write passwords down and store them in any form within your office apart from in the fire safe. Do not store passwords in a file on ANY computer system (including Smart Phones or similar devices) without encryption.

d) Change passwords at least every sixty days (except system-level passwords which must be changed annually).

e) If an account or password is suspected to have been compromised, report the incident to Serviceline ex 701234 or the IS Security Officer and change all passwords.

f) Password cracking or guessing may be performed on a periodic or random basis by the IS Security Officer on a periodic or random basis, if a password is guessed or cracked during one of these scans, the user will be required to change it.

8 Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

- Should support authentication of individual users, not groups
- Should not store passwords in clear text or in any easily reversible form
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password
- Should support TACACS+, RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

9 Use of Passwords and Passphrases for Remote Access Users

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to 'unlock' the private key, the user can not gain access.

Passphrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against dictionary attacks'.

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters.

An example of a good passphrase:
"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All the rules above that apply to passwords apply to passphrases.

10 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

11 Definitions

Anti-Virus: Software is used to prevent, detect and remove malware including but not limited to computer viruses, computer worm, trojan horses, spyware and adware.

Authentication: Confirmation of a person's identity, assuring a computer program is a trusted one.

Cardholder Data: Refers to personally identifiable information about the cardholder and its relationship to the card issuer, i.e. account number, expiration date etc.

Encryption: Process of transferring information using on algorithm to make it unreadable to anyone except those processing special knowledge, usually referred to as a key.

SNMP: Simple Network Management Protocol is an Internet Standard Protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modern racks and more.

SQL: Structure Query Language is a data base computer language designed for managing data in relational database management systems.

VPN: Virtual Private Network is a computer network that uses a public telecommunication infrastructure such as the Internet to provide remote offices or individual users with secure access to their organisations network.

Websense: Web security gateway security enables businesses to block access to chosen categories of websites.

- *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
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	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