Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Encryption 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 Encryption Policy Ref No. 011
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		31st March 2019 Annual review date: 31st January 2020

Table of Contents

1 Policy Aims

a) The purpose of this policy is to outline TfGM's standards for use of encryption technology so that it is used securely and managed appropriately. This policy does not cover what data is to be encrypted, but rather how encryption must be implemented and controlled.

b) Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data TfGM must store digitally increases, the use of encryption must be defined and consistently implemented in order to ensure that the security potential of this technology is realised.

2 Policy Scope

This policy covers all data stored on or transmitted across TfGM's IS systems.

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 Staff
- Awareness: All

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 Encryption Policy

Applicability of Encryption

6.1 Data while stored

Stored data includes any data located on TfGM-owned or TfGM-provided systems, devices, media, etc. Examples of encryption options for stored data include:

1. Whole disk encryption.
2. Encryption of partitions/files.
3. Encryption of disk drives.
4. Encryption of personal storage media/USB drives.
5. Encryption of backups.
6. Encryption of data generated by applications.

6.2 Data while transmitted

Transmitted data includes any data sent across TfGM' network, or any data sent to or from a TfGM-owned or TfGM-provided system. Types of transmitted data that can be encrypted include:

- VPN tunnels.
- Remote access sessions.
- Web applications.
- Email and email attachments.
- Remote desktop access.
- Communications with applications/databases.

6.3 Encryption Key Management

Encryption key management is critical to the success of an implementation of encryption technology. The following points apply to TfGM's encryption keys and key management:

- Management of keys must ensure that data is available for decryption when needed.
- Keys must be backed up.
- Keys must be stored in a locked and secure location.
- Keys must never be transmitted in clear text.
- Keys are confidential data.
- Keys must not be shared.
- Physical key generation materials must be destroyed within 5 business days.
- Keys must be used and changed in accordance with the password policy.
- When user encryption is employed, minimum key length is 10 characters.

6.4 Acceptable Encryption Algorithms

Only the strongest types of generally-accepted, non-proprietary encryption algorithms are allowed, such as AES or 3DES. Acceptable algorithms must be re-evaluated as encryption technology changes.

Use of proprietary encryption is specifically forbidden since it has not been subjected to public inspection and its security cannot be assured.

7 Legal Use

TfGM must conform with all encryption regulations and legislation applying to the use and import/export of encryption technology.

TfGM specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so is in violation of this policy and will face immediate consequences per the Enforcement section of this document.

8 Enforcement

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

9 Definitions

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.

Encryption Key: An alphanumeric series of characters that enables data to be encrypted and decrypted.

Mobile Storage Media: A data storage device that utilises flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

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.

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.

Remote Desktop Access: Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Virtual Private Network (VPN): A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

Whole Disk Encryption: A method of encryption that encrypts all data on a particular drive or volume, including swap space and temporary files.

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

Policy/Procedure:				
Version	Change	Reason for change	Date	Name
3.0	Version and Date	Annual Review	31/03/2014	C Burke
4.0	Version and Date	Annual Review	30/04/2015	C Burke
5.0	Version and Date	Annual Review	31/03/2016	C Burke
6.0	Version and Date	Annual Review, new Head of IS	31/03/2017	C Burke
7.0	Version and Date	Annual Review	31/03/2018	C. Styler
8.0	Version and Date	Annual Review	31/03/2019	C. Styler