Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Back-up 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 Back-up Policy Ref No. 004
Version No.	8.0	Prepared by:	Catherine Burke/DCS
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: IS 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) To provide a consistent framework to apply to the backup process.

b) To provide specific information to ensure backups are available and useful when required - whether to simply recover a specific file or when a larger-scale recovery effort is required.

c) Backups are not a substitute for archiving and should not be relied upon to store archive documents.

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 use 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

The policy is designed to protect data within **TfGM**, to ensure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

4 Scope

This policy applies to all equipment and data owned and operated by the **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

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

a) This policy applies to all data stored on **TfGM** systems. The policy covers such specifics as the type of data to be backed up, frequency of backups, storage of backups, retention of backups, and restoration procedures.

b) This Back-up policy also applies to **TfGM's** IS Resilience facilities. Systems hosted by external agencies will have their back-up policy aligned to this policy.

8.1 Identification of Critical Data

TfGM must identify what data is most critical to its organisation through a formal data classification process or through an informal review of information assets. Critical data should be identified so that it can be given the highest priority during the backup process.

8.2 Data to be Backed-Up

A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:

1. All data determined to be critical to **TfGM's** operation and/or employee job function.
2. All information stored on the **TfGM** file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.
3. All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.

8.3 Backup Frequency

Backup frequency is critical to successful data recovery. **TfGM** has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

- **Differential: every day from Monday to Friday.**
- **Full: every 7 days.**

8.4 Off-Site Rotation

Geographic separation from the backups must be maintained in order to protect from fire, flood, or other regional or large-scale catastrophes. The following points apply to the offsite rotation:

1. Backup media must be rotated off-site at least once per day Monday - Friday.
2. All backup tapes must be encrypted.
3. All backup tapes must be transported in a lockable carry case.

8.5 Backup Storage

As backups contain critical and/or confidential data, precautions must be taken that are commensurate to the type of data being stored. The following points apply to backup storage:

1. Backups must be kept in a access-controlled area.
2. Backup tapes must be kept in a heat resistant safe.
3. The storage area must contain fire suppression.
4. Access control must include a CCTV monitoring secure entry, exit facilities, audit trail entry access.

8.6 Backup Retention

The retention period for backup tapes must adhere to the following:

- Differential Backups must be saved for one month with the associated full back up.
- Every 5 weeks a full back-up must be taken out of the back-up cycle and saved for six months.

8.7 Restoration Procedures & Documentation

The data restoration procedures must be tested and documented. Documentation must include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not;

- Misinterpreted by readers other than the backup administrator, and
- Confusing during a time of crisis.

8.8 Restoration Testing

a) To ensure integrity of the backups the restoration process must be periodically tested to ensure and confirm the restore procedures, ensure tape integrity and to eliminate potential problems.

b) Backup restores must be tested when any change is made that may affect the backup system, as well as once every month.

8.9 Expiration of Backup Media

a) Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use or write cycle exceeds manufacturer specifications.

b) Any media must be wiped clean and securely destroyed with a recognised auditable process.

9 Definitions

Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

Backup Media: Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.

Full Back up: A backup that makes a complete copy of the target data.

Incremental Back up: A backup that only backs up files that have changed since the last backup was run.

Differential Back up: A back up that only backs up files that have been changed since the last FULL back up was run

Restoration: Also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

Change control record: complete each time there is a change

Policy/Procedure:				
Version	Change	Reason for change	Date	Name
3.0	Date & Version	Annual Update	31/03/2014	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 and Version	Annual Review	31/03/2018	C. Styler
8.0	Date and Version	Annual Review	31/03/2019	C. Styler