Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Operations 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 Operations Policy Ref No. 019
Version No.	7.0	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:	Malcolm Lowe (Head of IS) 31st March 2019		Implementation date: 31st March 2019 Annual review date: 31st January 2020

1 Policy Aims

This document is intended to ensure that TfGM has in place a set of policies to manage and control operations within Information Systems.

2 Policy Scope

The scope of this policy includes all the IS Infrastructure team system activities. All operating procedures should specify the instructions for the detailed execution of each job.

3 Policy Delivery

This policy will be delivered to all IS staff by internal communication and will be situated on the **TfGM** Intranet.

4 Accountability

- **Responsible to the Board:** Head of IS
- **Compliance:** IS Infrastructure team
- **Awareness:** IS Department

5 Policy Monitoring/ Compliance

Monitoring of Operations within Information Systems is audited every 12mths, should a breach of policy be identified, it may be used in disciplinary proceedings.

6 Policy

6.1 Operational Responsibilities

The Head of IS is responsible for the operational management of all **TfGM** Information Systems. If unavailable responsibility may pass to the IS Service Manager.

Operational Procedures are carried out by the IS Infrastructure team, which is split into sections consisting of Desktop support, Communications and Server and Security.

The development of appropriate operating procedures is the responsibility of the IS Security Officer.

6.1.1 Documented Operating Procedures

All IS procedures should be fully documented and reviewed on a regular basis.

TfGM Documented procedures should be prepared for all system activities including:-

1. Standard build guidelines
2. Installation and configuration of systems
3. Security patching
4. Day to day operation of systems
5. Shut down and restart of servers, including order of restart.
6. Backups and restores
7. Equipment maintenance
8. Media handling
9. Server and build room management
10. Safety procedures

The operating procedures should specify the instructions for the detailed execution of each job including:

1. Processing and handling of information.
2. Secure backup.
3. Scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times, to avoid clashes with backups or antivirus scheduled scans.
4. Instructions for dealing with errors or system failure
5. Support contacts in the event of unexpected operational or technical difficulties.
6. Special output and media handling instructions, such as the management of confidential output and procedures for secure disposal of output from failed jobs.
7. system restart and recovery procedures for use in the event of system failure;
8. The management of audit-trail and system log information.

Operating procedures, and the documented procedures for system activities, should be treated as formal documents and changes authorised by management. The documents should use version control to ensure currency.

One hardcopy should be stored in a central file for use of IS staff. The original should be electronically stored in a central documentation folder within the departmental drive

and secured so as to allow access to only those who need it. The document must have its electronic location included in the document footer.

Where technically feasible, information systems should be managed consistently, using the same procedures, tools, and utilities. Documentation should follow the pre-defined **TFGM** template.

6.1.2 Change Management

All Changes to **TfGM** IS systems should be strictly controlled.

Inadequate control of changes to IS systems is a common cause of system or security failures. Changes to the operational environment, especially when transferring a system from development to live, can impact on the reliability of applications.

Changes to operational systems should only be made when there is a valid business reason to do so.

Please refer to Change Management Policy.

6.1.3 System Planning & Acceptance

All **TfGM** systems will be subject to system planning and acceptance procedures, to minimise the risk of systems failure.

The **TfGM** Server and Network team are responsible for any advance planning and preparation which is required to ensure the availability of adequate capacity and resources to deliver the required system performance.

The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

The information manager will be consulted on requirements for systems which will be used to process personal data and/or sensitive personal data.

6.1.4 Capacity Management

The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

For each new and on-going activity, capacity requirements should be identified. System tuning and monitoring should be applied to ensure and, where necessary, improve the availability and efficiency of systems. Microsoft System Centre Operations Manager client should be installed to monitor the server, to indicate problems in due time.

Projections of future capacity requirements should take account of new business and system requirements and current and projected trends in the organisation's information processing capabilities.

Particular attention needs to be paid to any resources with long procurement lead times or high costs; therefore managers should monitor the utilisation of key system resources.

They should identify trends in usage, particularly in relation to business applications or management information system tools.

Managers should use this information to identify and avoid potential bottlenecks and dependence on key personnel that might present a threat to system security or services, and plan appropriate action.

6.1.5 Separation of Development – Test/Operational Facilities

Where possible, development, test, and operational facilities should be separated to reduce the risks of unauthorised access or changes to the operational system.
The following guidelines should be followed:

- Procedures for the transfer of software from development to live should be defined and documented in the form of an RFC.
- Development software should be run within the TfGM virtual development server environment.
- Evaluation or testing of off the shelf software should be done on a test server, either physical or virtual.
- Compilers, editors, and other development tools or system utilities should not be used on live servers.
- The test system environment should emulate the live system environment as closely as possible.
- Users should use different user accounts to logon to live and test systems. Sensitive or personal data should not be copied into the test system

6.1.6 System Acceptance

This section of the policy outlines the acceptance criteria that need to be met for new information systems, upgrades, and new versions. Suitable tests of the system(s) to be carried out during development and prior to acceptance will be the responsibility of the IS systems tester.

New information systems, upgrades, and new versions should only be migrated into production after obtaining formal acceptance at a CAB meeting.

The following criteria must be met prior to formal acceptance being provided:

a) Performance and computer capacity requirements.

b) Error recovery and restart procedures, and contingency plans.

c) Preparation and testing of routine operating procedures to defined standards.

d) Agreed set of security controls in place and evidence to verify that the security requirements have been properly addressed.

e) Effective manual procedures.

f) Business continuity arrangements.

g) Evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end.

h) Evidence that consideration has been given to the effect the new system has on the overall security of the organisation.

i.) Training requirements in the operation or use of new systems.

j) Ease of use, as this affects user performance and avoids human error.

For major new developments, the IS operations staff and users should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests should be carried out to confirm that all acceptance criteria have been fully satisfied.

6.2 Protection from Malware

Software and information processing facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs.

It is **TfGM** policy to ensure users are made aware of the dangers of malicious code – refer to **TfGM** Antivirus policy.

6.2.1 Controls against malware

In **TfGM** networks protection against malicious code should be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.

The **TfGM** IS security section must ensure the following operational measures are implemented and followed by IS staff to prevent, detect, and remove malicious code and control mobile code.

a) Ensure that no unauthorised software is installed on any **TfGM** device.

b) Take care when obtaining files and software from external networks. A reputable MD5 hash checker should be used to verify that downloaded software packages have not been tampered with before executing them.
c) Regular reviews of the software and data content of systems supporting critical business processes should be conducted, and the presence of any unapproved files or unauthorised amendments should be formally investigated.
d) Installation and regular update of **TfGM** approved antivirus software to scan computers and media as a precautionary control.
e) Carrying out routine checks on electronic or optical media, and files received over networks, for malicious code before use.
f) Checking electronic mail attachments and downloads for malicious code before delivery to users. This check should be carried out at different places, e.g. at electronic mail servers, desk top computers and by the Hosted email service provider, currently Messagelabs before entering the network of the organisation.
g) Ensure current security systems where possible are configured to check web pages for malicious code.
h) Following defined incident management procedures to deal with malicious code protection on systems. Managers must ensure operations staff are aware of their responsibilities and trained in their use to report and recover from malicious code attacks.
i) Appropriate business continuity plans should be prepared for recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements.
j) Provisions should be made to regularly collect information, such as subscribing to mailing lists and/or checking web sites giving information about new malicious code or participating in a Local Government Warning, Advice and Reporting Point (WARP).
k) Follow **TfGM** procedures to verify information relating to malicious code, and ensure that warning bulletins are accurate and informative. They should ensure that qualified sources, e.g. reputable journals, reliable Internet sites or suppliers producing software protecting against malicious code, are used to differentiate between hoaxes and real malicious code. All users should be made aware of the problem of hoaxes and what to do on receipt of them.
l) Extra care should be taken to protect against the introduction of malicious code during maintenance and emergency procedures, which may bypass normal malicious code protection controls.

6.2.2 Mobile Code

1. Mobile code is software code which transfers from one computer to another computer and then executes automatically and performs a specific function with little or no user interaction. Mobile code is commonly associated with a number of networking services, but can also take the form of malware e.g. worms such as **conficker**.

2. In addition to ensuring that mobile code does not contain malicious code, control of mobile code is essential to avoid unauthorised use or disruption of system, network, or application resources and other breaches of information security.

3. Where the use of mobile code is authorised, the configuration should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code should be prevented from executing.

    a) Authorised mobile code should be executed in a logically isolated environment.
    b) Any use of mobile code should be blocked.
    c) Receipt of mobile code should be blocked.
    d) Appropriate technical measures where available should be activated on specific systems to ensure mobile code is managed. For example in windows auto run should be disabled on external devices.
    e) The resources available to mobile code access should be limited by removing access for everyone group from the security permissions and securing access on a least privilege basis.
    f) Cryptographic controls should be implemented to uniquely authenticate mobile code.

6.3 Back-up

TfGM will carry out backups to protect against loss of data

See Back-up Policy for details of TfGM back up policy

6.4 Logging and Monitoring

Logging and monitoring will be carried out by TfGM to record events and generate evidence.

- Monitoring will be carried out to detect unauthorised information processing activities.
- Systems will be monitored and information security events recorded.

- Operator logs and fault logging will be used to ensure information system problems are identified.
- TfGM must comply with all relevant legal requirements applicable to its monitoring and logging activities.
- System monitoring will be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

6.4.1 Event Logging

Audit logs recording user activities, exceptions, and information security events will be produced and kept for an agreed period to assist in future investigations and access control monitoring.

Audit logs may contain intrusive and confidential personal data. Appropriate privacy protection measures must be taken.

Where possible, system administrators should not have permission to erase or de-activate logs of their own activities.

Audit logs will include, when relevant:-

- User logon IDs.
- Dates, times, and details of key events, e.g. log-on and log-off.
- Device name or location.
- Successful and rejected system access attempts.
- Successful and rejected data and other resource access attempts
- Changes to system configuration.
- Use of privileges
- Use of system utilities and applications
- Files accessed and the kind of access
- Network addresses and protocols
- Alarms raised by the access control system
- Activation and de-activation of protection systems, such as anti-virus systems and intrusion detection systems.

6.4.2 Protection of Log Information

Logging facilities and log information should be protected against tampering and unauthorised access. System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security.

Controls should aim to protect against unauthorised changes and operational problems with the logging facility including:

- Alterations to the message types that are recorded;
- Log files being edited or deleted;
- Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.

Some audit logs may be required to be archived as part of the record retention policy or because of requirements to collect and retain evidence.

When system logs contain a large volume of information, much of which is extraneous to security monitoring, the copying of appropriate message types automatically to a second log, and/or the use of suitable system utilities or audit tools to perform file interrogation and rationalisation may be used to help identify significant events for security monitoring purposes.
System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security.

6.4.3 Administrator and Operator Logs

System administrator and system operator activities will be logged
Logs will include:

a) The time at which an event (success or failure) occurred.
b) Information about the event (e.g. files handled) or failure (e.g. error occurred and corrective action taken).
c) The account and the administrator or operator which was involved.
d) The processes which were involved.

System administrator and operator logs will be reviewed on a regular basis.

An intrusion detection system managed outside of the control of system and network administrators should be used to monitor system and network administration activities for compliance.

6.5 Clock Synchronisation

The clocks of all relevant information processing systems within TFGM's multi service domain should be synchronised with an agreed accurate time source.

The correct setting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. Inaccurate audit logs may hinder such investigations and damage the credibility of such evidence.

TfGM uses a domain server clock linked to a radio time broadcast from a national atomic clock. A network time protocol is used to keep all of the servers in synchronisation with the master clock.

6.6 Control of operational software

Operational software will be controlled, to ensure the integrity of operational systems

6.6.1 Installation of software on operational systems

Procedures will be implemented to control the installation of software on operational systems.
The following controls apply to changes of software on TfGM operational systems:

- The updating of the operational software, applications and program libraries should only be performed by trained administrators upon appropriate management authorisation via the change advisory board.
- Operational systems should only hold approved executable code and not development code or compilers
- Applications and operating system software should only be implemented after extensive and successful testing. The tests should cover usability, security, effects on other systems and user-friendliness and should be carried out on separate systems. It should be ensured that all corresponding program source libraries have been updated.
- A configuration control system should be used to keep control of all implemented software as well as the system documentation.
- A rollback strategy should be in place before changes are implemented.
- An audit log should be maintained of all updates to operational program libraries.
- Previous versions of application software should be retained as a contingency measure;

- Old versions of software should be archived, together with all required information and parameters, procedures, configuration details and supporting software for as long as the data are retained in archive.
- Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Over time, software vendors will cease to support older versions of software. The organization should consider the risks of relying on unsupported software.
- Any decision to upgrade to a new release should take into account the business requirements for the change and the security of the release, e.g. the introduction of new information security functionality or the number and severity of information security problems affecting this version. Software patches should be applied when they can help to remove or reduce information security weaknesses.
- Physical or logical access should only be given to suppliers for support purposes when necessary and with management approval. The supplier's activities should be monitored.
- Computer software may rely on externally supplied software and modules, which should be monitored and controlled to avoid unauthorized changes, which could introduce security weaknesses.

6.7 Technical vulnerability management

Technical vulnerability management will be carried out at TfGM to prevent exploitation of technical vulnerabilities.

6.7.1 Management of technical vulnerabilities

Roles and Responsibilities

Selected members within the IS Infrastructure team will subscribe to email security notifications, to gain information about technical vulnerabilities of information systems being used, in a timely fashion.

The teams responsible for technical vulnerability management are

- IS Security
- IS Server and Data Storage Team
- IS Network and Telecoms Team

Asset Tracking Inventory

A current and complete inventory of assets is a prerequisite for effective technical vulnerability management. Specific information needed to support technical vulnerability management includes the software vendor, version

numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software. (See IS Asset Management Policy)

Vulnerability Monitoring

Essential circulars should be identified from the Asset tracking activities and should include:

- Microsoft Security Bulletin & Bulletin Summary Minor Revisions
- Microsoft Security Advisory Notification
- CISCO Notification service
- Citrix Knowledge Center Email alerts
- Patch Management Mailing List
- IT Governance Daily Sentinel
- North West WARNING, ADVICE AND REPORTING POINT Alerts, Advisory and News bulletins.
- CVE Details – the ultimate security vulnerability data source Feed
- Tenable Nessus circulars

This list should be updated based on changes in the inventory or when other new or useful resources are found

Risk Assessment

Upon receipt of the notification TfGM's exposure to such vulnerabilities will be evaluated and appropriate actions identified to address the associated risk. Such action could involve patching of vulnerable systems or applying other controls. If a patch is available from a legitimate source, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch).

Risk Treatment

Appropriate and timely action should be taken in response to the identification of potential technical vulnerabilities. Upon notification of new vulnerabilities, the following timescales should be observed

- High Risk Vulnerabilities should be remediated as soon as possible and no longer than 2 weeks after notification. Exceptions to this should be notified and authorised by the head of IS
- Medium Risk vulnerabilities should be remediated within 30 days of the release of the fix.

Technical vulnerability management can be viewed as a sub-function of change management and as such should adhere to the change management processes and procedures.

Depending on how urgently a technical vulnerability needs to be addressed, the action taken should be carried out according to the controls related to change management or by following information security incident response procedures.

Vendors are often under significant pressure to release patches as soon as possible. Therefore, there is a possibility that a patch does not address the problem adequately and has negative side effects. Also, in some cases, uninstalling a patch cannot be easily achieved once the patch has been applied. For this reason, patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated.

If no patch is available, other controls should be considered, such as:

- Turning off services or capabilities related to the vulnerability.
- Adapting or adding access controls, e.g. firewalls, at network borders.
- Increased monitoring to detect actual attacks.
- Raising awareness of the vulnerability.

Coordination responsibilities

The IS Security Technician will be responsible for ensuring that any necessary patches or remedial work is approved by the Change Advisory Board and a timetable for changes arranged within the above timescales.

The IS Security Technician will also ensure that:

- An audit log is kept for all procedures undertaken.

- The technical vulnerability management process is regularly monitored and evaluated in order to ensure its effectiveness and efficiency.
- Systems at high risk are addressed first.
- An effective technical vulnerability management process is aligned with incident management activities, to communicate data on vulnerabilities to the incident response function and provide technical procedures to be carried out should an incident occur.
- Define a procedure to address the situation where a vulnerability may have been identified but there is no suitable countermeasure. In this situation, Risks should be evaluated relating to the known vulnerability and appropriate detective and corrective actions defined.

6.7.2 Restrictions on software installation

TfGM operates a strict policy on software installation. Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights.

Software Requests
All new software installations must be requested, with business justification using the Service request form.

Software Approvals
Approval for the installation of the software will be granted by IS if an appropriate license is available or the budget is available to purchase additional licenses. Where a license is freely available, such as open source software, the license conditions should be checked to ensure the software may be used in corporate environments, and the use of the software for the purpose requested, does not contravene the license conditions. Furthermore, approval will only be granted if the software can be safely run within TfGM's network, without introducing security vulnerabilities, or detrimental performance issues on local PC's. Where non-standard software is approved, this does not necessarily mean that it will be supported by Serviceline.

Software Installation

Software installation must only be carried out by authorised members of the Serviceline team.

Installation restrictions

Computer users outside of IS must have restrictions placed on their accounts to prevent them from being able to install software.
Restrictions will also be put in place to prevent software executables from being received via email or as a download from the internet.
Where enhanced privileges are granted to users outside of Serviceline, these are granted on the condition that the privileges are not abused, to install unauthorised software.

6.8 Information systems audit considerations

TfGM should ensure that any audit requirements and activities involving verification of operational systems are carefully planned and agreed to minimize disruptions to business processes.

The following requirements should be observed:

- Audit requirements for access to systems and data should be agreed with appropriate management.
- The scope of technical audit tests should be agreed and controlled.
- Audit tests should be limited to read-only access to software and data.
- Access other than read-only should only be allowed for isolated copies of system files, which should be erased when the audit is completed, or given appropriate protection if there is an obligation to keep such files under audit documentation requirements.
- Requirements for special or additional processing should be identified and agreed.
- Audit tests that could affect system availability should be run outside business hours.
- All access should be monitored and logged to produce a reference trail.

7 Definitions

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

Policy/Procedure:				
Version	**Change**	**Reason for change**	**Date**	**Name**
3.0	Version & Date	Annual Review	06/03/2014	C Burke
3.1	Technical Vulnerability Management	Aligned to ISO27001	28/07/2015	J Singleton
4.0	Version and Date	Annual Review	31/03/2016	C Burke
5.0	Version and Date	Annual Review, new Head of IS	31/03/2017	C Burke
6.0	Version and Date	Annual Review	31/03/2018	C Styler
7.0	Replaced operations manager with head of IS	Annual Review	31/03/2019	C Styler