Transport for Greater Manchester

Transport for Greater Manchester Policy

IS System Acquisition Development and Maintenance 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 System Acquisition Development and Maintenance Policy Ref No.25
Version No.	4.0	Prepared by:	Gordon Bradley/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:	Head of IS (Malcolm Lowe)		Implementation date: 31st March 2019
Date:	31st March 2019		Annual review date: 31st January 2020

Table of Contents

1 Policy Aims

This policy describes the requirements to ensure that information security is established and maintained within the scope of information systems provided both within TfGM and by TfGM across public networks.

2 Policy Scope

This policy applies to all users of TfGM's computer systems and to all systems, processes and procedures that are in use within TfGM, or are provided by TfGM across public networks.

3 Policy Delivery

The 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

All managers are responsible for ensuring compliance with identified legal requirements and security procedures within their department.

Should a breach of this policy be identified, it may be used in disciplinary proceedings.

6 Policy

6.1 Security requirements of information systems

Information security related requirements are considered within the defined scope of both new information systems and enhancements to existing operational services. Legacy programs will be subject to this policy whenever a formal review of any respective system is undertaken.

Security requirements that are identified at the inception of a project will be defined, justified, agreed and documented within the business case for an information system, which will be subject to review by relevant stakeholders.

6.1.1 Information security requirements analysis and specification

Business requirements for new systems or enhancements to existing services shall reflect the required controls. The business case will provide a mechanism to identify any potential negative business impact that may result from a lack of adequate security.

6.1.2 Securing application services on public networks

Information involved in application services passing over public networks should be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.

Information security considerations for application services passing over public networks will be provided by considering the following:

- the level of confidence each party requires in other’s identities;
- authorisation processes associated with content approvals;
- ensuring that partners are fully informed of the required authorisations for provision or use of the service;
- specifying and achieving confidentiality, integrity, proof of dispatch and receipt of key documents and the non-repudiation of contracts;
- the level of trust required in the integrity of key documents;
- the protection requirements of any confidential information;
- the confidentiality and integrity of any order transactions, payment information, delivery address details and confirmation of receipts;
- the degree of verification appropriate to verify payment information supplied by a customer;
- selecting the most appropriate settlement form of payment to guard against fraud;
- the level of protection required to maintain the confidentiality and integrity of order information;
- avoidance of loss or duplication of transaction information;
- liability associated with any fraudulent transactions;
- insurance requirements.

Application service arrangements between partners should be supported by a documented agreement, which commits both parties to agreed terms of services.
Resilience requirements against attacks should be considered, which can include requirements for protecting the involved application servers or ensuring the availability of network interconnections, required to deliver the service.
As applications accessible via public networks are subject to a range of network related threats, such as fraudulent activities, contract disputes or disclosure of information to the public, detailed risk assessments and proper selection of controls are indispensable.

6.1.3 Protecting application services transactions

All transactions to be input to a multi-user application on a network must be subject to a form of validation to ensure that processing is checked. Those transactions that fail such checks should be:

- rejected with a notification of the rejection sent to the submitter;
- corrected and resubmitted;
- suspended pending further investigation.

Data that is input to application systems should be validated to ensure it is correct and appropriate. Validation should include inspection of sample data, sanity checking of values and units, and data quality analysis for unusual values, trends or repetitions. Corrective action should be part of the business process checks and could include dual input checks; range values; invalid characters; incomplete data; exceeding data volume limits; unauthorised control data; review of data validity and integrity; input document inspection.

Data security controls should maintain the accuracy, completeness and currency of data input, held and processed. Such controls should include integrity and validity checking: cross checking of logical consistency between data fields; alpha and numeric validity checking; system reconciliation.

Any loss or corruption of data should be reported to the IT Security Officer.
The report should include:

- date and time of discovery;
- which data has been lost or corrupted;
- remedial action taken;
- reason for the loss or corruption;
- follow up action taken or required.

6.1.4 Control of internal processing

Validation checks are incorporated into systems to detect the corruption of data processed. Such checks will consider the use and location of programs; the functionality to implement data changes; procedures to prevent programs running in the wrong order or running after processing failures; recovery procedures; Checks and controls: batch reconciliation; balancing controls; run controls; file update totals; data integrity checks; operational processing checks.

Additionally, data validation checks will be applied to avoid corruption by processing errors or deliberate acts. Validation checks are incorporated to detect such corruption and potentially include session or batch controls; balance reconciliation; balancing controls; validation of system generated data; data integrity checks.

An audit trail facility, to trace all transactions in a system, will be implemented where appropriate and the data owner will specify the retention period of the audit trail, which will be agreed with the IT Security Officer and detailed in the system security policy.

6.1.5 Message integrity

Message authentication will be used where there is a requirement to protect the integrity of the message content.

6.1.6 Output data validation

Where appropriate, data output from an application system shall be validated to ensure that the information processing is correct and accurate for the specific circumstances. Validation checks include reasonableness of the output data; reconciliation control; counts to ensure processing of all data; accuracy; completeness; precision and classification of the information.

6.2 Security in development and support processes

TfGM ensures that information security is designed and implemented within the development lifecycle of information systems, which include the full documentation of changes to development and support processes.

6.2.1 Secure development policy

Within TfGM, established rules are applied to the development of software and systems.

Secure development is considered to be a pre-requisite to build up a secure service, architecture, software and system.

The development processes considered a variety of aspects of security including the development environment; the software development lifecycle: the development methodology; coding guidelines; the design requirements; Project checkpoints; data repositories; version controls; application security knowledge; developers' capability; identification and correction of vulnerabilities.

If development is outsourced, then TfGM will seek assurance that the external party complies with internal organisational controls for secure development.

6.2.2 System change control procedures

Ad-hoc uncontrolled modifications to software packages are discouraged in favour of essential change controls, which are applied through TfGM's ITIL compliant Change Management processes.

Change control documentation is maintain for all changes and includes: recording agreed authorisations; ensuring changes are submitted by authorised users; reviewing controls and integrity procedures to ensure that they will not be compromised by the changes; identifying all computer software, information, database entities and hardware that require amendment; obtaining formal approval for detailed proposals before work commences; ensuring that the authorised user accepts changes prior to any implementation; ensuring that implementation is carried out to minimise business disruption; ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of; maintaining a version control for all software updates; maintaining an audit trail of all change requests; ensuring that operating documentation and user procedures are changed as necessary to be appropriate; ensuring that the implementation of changes takes place at the scheduled time.

6.2.3 Technical review of applications after operating platform changes

Application systems shall be reviewed and tested when changes have been applied.

The relevant operational checks will consider:

Review of application control and integrity procedures to ensure that they have not been compromised by the operating system changes;

ensuring that any necessary annual support plans will cover reviews and system testing resulting from operating system changes;

ensuring that notification of changes is provided in advance, to allow appropriate reviews to take place before implementation; ensuring that appropriate changes are made to the business continuity plans.

6.2.4 Restrictions on changes to software packages

Ad-hoc uncontrolled modifications to software packages are discouraged and essential changes are strictly controlled.
Such controls consider:
The risk of built-in controls and integrity processes being compromised; whether the consent of the vendor should be obtained; the possibility of obtaining the required changes from the vendor as standard program updates; the impact if TfGM becomes responsible for the future maintenance of the software as a result of changes.

6.2.5 Secure system engineering principles

TfGM has established principles for engineering secure systems, which are maintained and applied to any information system implementation.
The established procedures are based on best practice principles and are applied to in-house information system activities. Where appropriate, security is designed into all architecture layers (business, data, applications and technology) in order to balance information security with system accessibility.

6.2.6 Secure development environment

TfGM has established and appropriately protects a secure development environment for system development and integration. The security measures consider the entire system development lifecycle.
The secure development environment includes people, processes and technology associated with system development and integration.
TfGM assess risks associated with individual system developments and establishes secure development environments which consider:
sensitivity of data; applicable external and internal requirements; security regulations and policies; existing security controls; trustworthiness of personnel working in the environment; the degree of outsourcing associated with system development; the need for segregation between different development environments; access controls; environment changes; backups are stored at secure offsite locations; control over movement of data from and to the environment.

6.2.7 Outsourced development

TfGM applies controls to outsourced software developments. Relevant procedures will consider licensing arrangements; code ownership and intellectual property rights; certification of the quality and accuracy of the work carried out; any necessary escrow arrangements in the event of failure of the third party; rights of access for audit of the quality and accuracy of work done; contractual requirements.

6.2.8 System security testing

TfGM ensures that necessary testing of security functionality is carried out during developments.

Any new and updated systems that require thorough testing and verification during the development processes, including the preparation of a detailed schedule of activities are tested under a range of conditions, with actual results compared with expected outputs. For in-house developments, such tests are initially performed by the development team. Where necessary, independent acceptance testing is undertaken for in-house and outsourced developments, to ensure that the system works as expected.

6.2.9 System acceptance testing

TfGM ensure that acceptance tests and related criteria are established for new information systems, upgrades and new versions.
System acceptance tests include testing of information security requirements and adherence to secure system development practices.
Testing is performed in a realistic test environment to ensure that the system will not introduce vulnerabilities to the organization’s environment and that the tests are reliable.

6.3 Test data

TfGM protects stored data to ensure the integrity of tests and respective test results.

The use of operational data containing personally identifiable information or any other confidential information for testing purposes is avoided, wherever possible. If personally identifiable information or otherwise confidential information is used for testing purposes, TfGM ensures that all sensitive details and content should be protected by removal or modification.

The following guidelines are considered to protect operational data, when used for testing purposes:
access control procedures, which apply to operational application systems, are also applied to test application systems; separate authorisation are applied when operational information is copied to a test environment; operational information is erased from a test environment following completion of testing; the copying and use of operational information is recorded to provide an audit trail.

6.3.1 Protection of test data

TfGM protects and controls test data. The use of live data, for testing or testing on live systems is not sanctioned. All tests are subject to formal approval, with the business by the creation, review and agreement of a test plan.

The access control procedures, which apply to operational application systems, are also applied to test application programs. Access to operational application systems is limited to those that use the software, whilst access to test programs is, where practical, limited to development staff. It is recognised that a failure to separate development and operational responsibilities increases the risk of procedures and confidentiality being compromised.

Where possible, live sensitive data is not used for testing, training or demonstration purposes unless it is transformed such that identification of any individual is not possible (pseudonymised, or anonymised).

7 Enforcement

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

8 Definitions

Change control record: complete each time there is a change

Policy/Procedure:				
Version	Change	Reason for change	Date	Name
1.0	Date & Version	Annual Review	31/03/2015	C Burke
2.0	Date & Version	Annual Review	31/03/2016	C Burke
3.0	Date & Version	Annual Review, new Head of IS	31/03/2017	C Burke
4.0	Date & Version	Annual Review	31/03/2018	C Styler
5.0	Date & Version	Annual Review	31/03/2019	C Styler