Transport for Greater Manchester

Transport for Greater Manchester Policy

IS Compliance 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 Compliance Policy Ref No. 007
Version No.	5.0	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:	Malcolm Lowe (Head of IS)		Implementation date: 31st March 2019
Date:	31st March 2019		Annual review date: 31st January 2020

Table of Contents

1 Policy Aims

a. The purpose of this policy is to ensure compliance with legal requirements, so as to avoid breaches of any law, statutory, regulatory or contractual obligations.
b. The policy also covers the requirements to ensure compliance of systems with organisational security policies and standards

2 Policy Scope

The scope of this policy covers all TfGM devices and information stored on TfGM-owned, TfGM-leased, and otherwise TfGM-provided systems and media, regardless of location. Also covered by the policy are hardcopies of TfGM data, such as printouts, faxes, notes, etc.

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 Compliance with legal and contractual requirements

Many systems at TfGM contain data, which is subject to legal, statutory, regulatory or contractual obligations and requirements.
The main laws that affect information security policy include:

- The Data Protection Act 2018
  http://www.legislation.gov.uk/ukpga/2018/12/contents
- The computer misuse Act 1990
  http://www.legislation.gov.uk/ukpga/1990/18/contents
  Copyright, Designs and Patents Act 1988
- http://www.legislation.gov.uk/ukpga/1988/48/contents
- Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002
  http://www.legislation.gov.uk/ukpga/2002/25/contents
- The Health and Safety at Work Act 1974
  http://www.legislation.gov.uk/ukpga/1974/37
- Human Rights Act 1988
  http://www.legislation.gov.uk/ukpga/1998/42/contents
- The Freedom of Information Act 2000
  http://www.legislation.gov.uk/ukpga/2000/36/contents
- Equality Act 2010
  http://www.legislation.gov.uk/ukpga/2010/15/contents

Other legislation that needs to be considered is;

- PCI-DSS V3.2
- Privacy and Electronic Communications Regulations 2003
  http://www.legislation.gov.uk/uksi/2003/2426/contents/made
- Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011
  http://www.legislation.gov.uk/uksi/2011/1208/contents/made
- Regulation of Investigatory Powers Act 2000
  http://www.legislation.gov.uk/ukpga/2000/23/contents
- Limitation Act 1980
  http://www.legislation.gov.uk/ukpga/1980/58
- Malicious Communications Act 1988
  http://www.legislation.gov.uk/ukpga/1988/27/contents

A complete list can be found at http://www.legislation.gov.uk/ukpga

In order to build a robust Information Systems Management System (ISMs), TfGM will consider controls identified within the requirements of various standards including:

- PCI-DSS V3.2,
- ISO/IEC 27001,
- ISO/IEC 27002,
- ITIL
- Cyber Security Essentials.

Compliance with the TfGM Security Policy and Information Security Procedures and Guidelines within the TfGM Information Security Management System (ISMS) is mandatory for all users.

6.1.1 Identification of applicable legislation and contractual requirements

All relevant legislative, statutory, regulatory and contractual requirements shall be explicitly identified, documented and kept up to date for each identified information system. As an organisation, TfGM's approach to meet these requirements should be clearly defined and communicated to all users of these systems. Individual end-users must be aware of the extent to which they must comply through detailed procedures and guidelines.

6.1.2 Intellectual property rights

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.
The following guidelines must be observed to protect any material that may be considered to be intellectual property, in order to meet the provisions of the Copyright, Designs and Patents Act 1998:

- Publish an intellectual property rights compliance policy which defines the legal use of software and information products. (See Intellectual Property Rights Policy)
- Software should only be acquired through known and reputable sources, to ensure that copyright is not violated. (See Software Asset Management Policy)
- Maintain awareness of policies to protect intellectual property rights and give notice of the intent to take disciplinary action against personnel breaching them.
- Maintain appropriate asset registers and identify all assets with requirements to protect intellectual property rights.

- Maintain proof and evidence of ownership of licences; install media, manuals, etc.
- Implement controls to ensure that any maximum number of users permitted within the licence purchased is not exceeded.
- Carry out reviews to check that only authorized software and licensed products are installed.
- Provide a policy for maintaining appropriate licence conditions (See Software Asset Management Policy)
- Provide a policy for disposing of or transferring software to others. (See Software Asset Management Policy)
- Comply with terms and conditions for software and information obtained from public networks or internet.
- Do not duplicate, convert to another format or extract material from commercial recordings (film, audio) other than is permitted by copyright law.
- Do not copy in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

6.1.3 Protection of records

Important records of TfGM and its stakeholders should be protected from loss, destruction, falsification, unauthorised access and unauthorised release. This includes records that need to be securely retained to meet identified regulatory or contractual requirements, as well as to support essential business processes.

- The degree of protection of specific organizational records should be in accordance with their corresponding classification based on the organisation's classification scheme. (See IS Classification Policy)
- Records should be categorised into record types, e.g. accounting records, database records, transaction logs, audit logs and operational procedures, each with details of retention periods and type of allowable storage media, e.g. paper, microfiche, magnetic or optical.
- Any related cryptographic keys and programs associated with encrypted archives or digital signatures, should also be stored to enable decryption of the records for the length of time the records are retained.
- Consideration should be given to the possibility of deterioration of media used for storage of records.
- Storage and handling procedures should be implemented in accordance with manufacturer's recommendations.
- When electronic storage media is chosen, procedures to ensure the ability to access data (both media and format readability) throughout the

retention period should be established to safeguard against loss due to future technology change.

- Data storage systems should be chosen such that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.
- The system of storage and handling should ensure identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organization.

To meet these record safeguarding objectives, the following steps should be taken within an organization:

- Guidelines should be issued on the retention, storage, handling and disposal of records and information. (See IS Disposal of Confidential Waste policy)
- A retention schedule should be drawn up identifying records and the period of time for which they should be retained.
- An inventory of sources of key information should be maintained.
- Controls must be applied to all records regardless of whether they are paper based or electronically stored.
- Records must be stored and retrieved in a manner that supports their use in a court of law.

6.1.4 Data protection and privacy of personal information

Privacy and protection of personally identifiable information should be ensured as required in relevant legislation and regulation where applicable. Presently this is the Data Protection Act 2018. The following controls must be applied to ensure compliance with this:

- A data policy for privacy and protection of personally identifiable information should be developed and implemented (See Data Protection Policy).
- This policy should be communicated to all persons involved in the processing of personally identifiable information.
- Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information must be achieved by appropriate management structure and control.
- TfGM will appoint a person responsible, an Information Manager, who should provide guidance to managers, users and service providers on

their individual responsibilities and the specific procedures that should be followed.

- Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations.
  Appropriate technical and organizational measures to protect personally identifiable information should be implemented.

6.1.5 Regulation of cryptographic controls

Cryptographic controls should be used in compliance with all relevant national agreements, laws, legislation and regulations. Currently the Regulation of Investigatory Powers (RIP) Act, 2000, provides for access to encryption keys or a decrypted version of the data when required by the state.

The following items should be considered for compliance with the relevant agreements, laws and regulations:

- restrictions on import or export of computer hardware and software for performing cryptographic functions
- restrictions on import or export of computer hardware and software which is designed to have cryptographic functions added to it;
- restrictions on the usage of encryption;
- mandatory or discretionary methods of access by the countries' authorities to information encrypted by hardware or software to provide confidentiality of content.
- Legal advice should be sought to ensure compliance with relevant legislation and regulations.
- Before encrypted information or cryptographic controls are moved across jurisdictional borders, legal advice should also be taken.

6.2 Information security reviews

TfGM will carry out Information Security Reviews to ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

6.2.1 Independent review of information security

The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) should be reviewed independently at planned intervals or when significant changes occur.

- Management should initiate the independent review. Such an independent review is necessary to ensure the continuing suitability, adequacy and effectiveness of the organization’s approach to managing information security.
- The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives.
- Such a review should be carried out by individuals independent of the area under review, e.g. the internal audit function, an independent manager or an external party organization specializing in such reviews.
- Individuals carrying out these reviews should have the appropriate skills and experience.
- The results of the independent review should be recorded and reported to the management who initiated the review. These records should be maintained.
- If the independent review identifies that the organization’s approach and implementation to managing information security is inadequate, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies, (see Management direction for information security) management should consider corrective actions.

6.2.2 Compliance with security policies and standards

Managers should regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.

- Managers should identify how to review that information security requirements defined in policies, standards and other applicable regulations are met.
- Automatic measurement and reporting tools should be considered for efficient regular review.
- If any non-compliance is found as a result of the review, managers should:
  a) Identify the causes of the non-compliance;
  b) Evaluate the need for actions to achieve compliance;
  c) Implement appropriate corrective action;
  d) Review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.
- Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained.

- Managers should report the results to the persons carrying out independent reviews (see 6.2.1) when an independent review takes place in the area of their responsibility.

6.2.3 Technical compliance review

Information systems should be regularly reviewed for compliance with the organization's information security policies and standards.

- Technical compliance should be reviewed preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed.
- If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable.
- Any technical compliance review should only be carried out by competent, authorized persons or under the supervision of such persons.
- Technical compliance reviews involve the examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance review requires specialist technical expertise.
- Compliance reviews also cover, for example, penetration testing and vulnerability assessments, which might be carried out by independent experts specifically contracted for this purpose. This can be useful in detecting vulnerabilities in the system and for inspecting how effective the controls are in preventing unauthorized access due to these vulnerabilities.
- Penetration testing and vulnerability assessments provide a snapshot of a system in a specific state at a specific time. The snapshot is limited to those portions of the system actually tested during the penetration attempt(s).
- Penetration testing and vulnerability assessments should not be used as a substitute for risk assessment.

7 Enforcement

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

Change control record: complete each time there is a change

Policy/Procedure:				
Version	Change	Reason for change	Date	Name
1.0	Date and Version	Annual Review	31/03/2015	C Burke
2.0	Date and Version	Annual Review	31/03/2016	C Burke
3.0	Date and Version	Annual Review	31/03/2017	C. Burke
4.0	Date and Version	Annual Review	31/03/2018	C. Styler
5.0	Updated, Date and Version	Annual Review and change of data protection law	31/03/2018	C. Styler