



Information Security Policy

Issue date: 16 December 2009

Effective: 1 January 2010

This supersedes any previous policy.

Purpose

1. The objective of this policy is to ensure that all the Information Transport for London (TfL) holds in order to deliver its services and operations is managed with appropriate regard for Information Security, so as to:
 - (a) Protect its integrity, availability, and confidentiality;
 - (b) Minimise the potential consequences of information security breaches by preventing their occurrence in the first instance, or where necessary, containing and reducing their impact; and
 - (c) Ensure that personal data is afforded the protection required by the Data Protection Act 1998.
2. This policy applies to all Information held by TfL in any form or medium, electronic, paper or otherwise, including all data held on, or processed by, TfL systems.
3. External service providers must adhere to the principles of this policy; compliance will be monitored through contractual arrangements and audits.

Definitions

4. Information: any information, data or records, irrespective of format, which are generated or used by a business system or process. Examples include electronic communications, emails, video or digital recordings, hard copy (paper) files, images, graphics, maps, plans, technical drawings, programs, software and all other types of data.
5. Information Governance: a business unit within General Counsel.
6. Information Management (IM): a business unit within Finance.
7. Information Owners: senior managers, who are responsible for managing the acquisition, creation, maintenance and disposal of TfL's Information and Information Systems within their assigned area of control.
8. Information Risk: that part of TfL's overall risk portfolio which relates to the, integrity, availability and confidentiality of Information within the TfL Group.

9. Information Security: the ability to protect the integrity, availability, and confidentiality of Information held by TfL and to protect Information from unauthorised use, modification, accidental or intentional damage or destruction.
10. Information Security Breach: an Information Security Incident where it is confirmed that a stated organisational policy or legal requirement regarding Information Security has been contravened.
11. Information Security Incident: a single or a series of unwanted or unexpected Information Security events that have a significant probability of compromising business operations and threatening information security.
12. Information System: Information in all media, hardware, software and supporting networks and the processes and human resources that support its acquisition, storage and communication.
13. Internal Audit: a business unit within General Counsel.
14. TfL Personnel: includes all TfL employees as well as all temporary staff, contractors, consultants and any third parties with whom special arrangements (such as confidentiality and non-disclosure agreements) have been made.
14. Transport for London (TfL): the statutory corporation and its operating subsidiaries.

Organisational scope

15. This policy applies to TfL and to any commercial organisations or service providers (including agencies or consultancy companies) contracted to carry out work for TfL.

Policy statement

14. TfL depends on Information and Information Systems to support and develop its key business objectives, including the provision of public transport services and the implementation of the Mayor of London's Transport Strategy. TfL will adopt appropriate technical and organisational arrangements in accordance with this policy to protect the resilience, integrity, availability and confidentiality of the Information it holds (including personal data relating to both customers and employees) and the systems in which the Information resides.
15. This policy has been developed with reference to the following best practice standards and guidance:
 - (a) Information Security Standard ISO/IEC 27001 and associated Code of Practice for Information Security ISO/IEC 27002:2005.
 - (b) Her Majesty's Government (HMG) Security Policy Framework.
 - (c) Cross Government Mandatory Minimum Measures for Data Handling.
 - (d) Government Protective Marking Scheme (GPMS).
 - (e) Payment Card Industry Data Security Standard (PCI DSS).

Policy content

16. TfL's policy is to ensure that:
- (a) Information Security is considered as a fundamental and integral part of all TfL operations.
 - (b) Statutory requirements to safeguard the security of Information are met and the accuracy, completeness and segregation of personal data are assured.
 - (c) Information is accessible to authorised users when they need it and is assigned an appropriate security classification.
 - (d) ICT systems, networks and other key infrastructure components are protected from harm and the integrity of Information is maintained and protected from attack and unauthorised access or alteration.
 - (e) Information Risk will be considered and afforded a priority in decisions within TfL in the same way as financial and operational risk. This will be reflected in corporate and local risk registers. Information Risk will be managed by a process of identifying, controlling, minimising and/or eliminating risks that may affect TfL's information or information systems.
 - (f) Business continuity plans, including disaster recovery plans, are implemented to support business needs and appropriate Information Security training is given to TfL Personnel.
 - (g) All Information Security Breaches, actual or suspected, are reported and investigated and a culture exists where improving Information Security procedures is encouraged.
 - (h) All necessary measures are taken in order to comply with the Payment Card Industry Data Security Standards (PCI DSS), which are mandatory for organisations processing payment card transactions.

Responsibility for Information Security

17. Each TfL employee is responsible for actively supporting this policy and must ensure that their use of TfL's Information or Information Systems is in accordance with it. Employees must seek advice in the event of uncertainty in relation to this issue.
18. All Cost Centre and Project managers are directly responsible for the security of Information within their business areas.
19. Information Owners are responsible for ensuring that TfL Personnel within their area of control are aware of this policy and are adequately trained in Information Security.
20. Information Owners are responsible for the assessment and reporting of Information Risk within each business unit.
21. Information Owners will define and document relevant statutory and contractual requirements for Information Systems.

22. Information Owners will implement appropriate procedures to ensure compliance with legal restrictions on the use of material in respect of which there may be intellectual property rights including copyright, design rights and trademarks.
23. Information Owners, with support from TfL Personnel who lead on business continuity planning within the relevant business area, will manage and co-ordinate strategies for resilience, including business recovery following information loss or corruption or unauthorised disclosure or access.
24. TfL Personnel who lead on business continuity planning within their business area are responsible for co-ordinating the creation and maintenance of business continuity plans for all departments across TfL, which take account of the requirements of this policy where appropriate.
25. Information Governance, Internal Audit and IM are responsible for managing actual or suspected Information Security Incidents and Breaches and recommending additional or improved security measures to prevent their reoccurrence.
26. Information Governance is responsible for the interpretation of this policy, for monitoring compliance with the policy and for providing advice and guidance on its implementation.
27. IM are responsible for advising the business on the technical measures required to implement this policy and for their implementation on TfL's Information Systems and for ensuring that appropriate technical measures are in place to protect the security of electronic Information.

Procedures/Guidelines/Processes

28. All Information held by TfL must be managed in accordance with TfL's Privacy and Data Protection Policy, Information and Records Management Policy and Information Access Policy.
29. Appropriate Information Security procedures and TfL Standards will be implemented in support of this policy. These will include Standards and procedures as listed in the Annex to this Policy.
30. TfL will have in place an Information Security Classification Standard for protectively marking Information. Security classifications will be applied to all of TfL's Information on creation or receipt, irrespective of format or medium, and Information classified according to this Standard must be transmitted, stored and disposed of as required by the classification Standard and its accompanying instructions.
31. TfL personnel handling Information which has been protectively marked in accordance with HMG's Security Policy Framework (SPF) will adhere to the requirements of the SPF.
32. Actual or suspected Information Security Incidents involving personal or sensitive personal data (as defined by the Data Protection Act 1998) must be reported to Information Governance in order for the incident to be managed in accordance with the Incident Management Procedure for the Loss or Unauthorised Disclosure of Personal Data.

33. Internal Audit will perform a periodic audit of the security processes, procedures and practices of TfL and its service providers to monitor compliance with this policy.

Approval and amendments

34. This policy was approved by the Commissioner on 18 November 2009.
35. This policy was approved by the Audit Committee on 16 December 2009.
36. Following an organisational restructure, a number of minor amendments to this Policy were made on 2 May 2012.
37. This policy will be subject to periodic review as considered appropriate by General Counsel.

Policy owner

38. TfL's General Counsel is the designated owner of this policy.

Annex: Information Security Standards and procedures

Standards and procedures covering the following topics will be implemented in support of the Information Security Policy:

- Physical security of data centres, communications rooms and sensitive zones.
- Incident management.
- Business continuity.
- CMDB (IT asset register).
- Security vetting for sensitive roles within Information Management (IM).
- IT user registration.
- Back-up.
- Cryptographic controls.
- Third party connections.
- Change management.
- Development and test areas.
- Access controls.
- System requirements analysis.
- Mobile computing and remote working.
- Input data validation.
- Integrity of software and information.
- Acceptable use and user responsibilities.
- Information handling.