AGENDA ITEM 12

TRANSPORT FOR LONDON

AUDIT COMMITTEE

SUBJECT: DRAFT INFORMATION SECURITY POLICY

DATE: 16 DECEMBER 2009

1 PURPOSE AND DECISION REQUIRED

1.1 A draft Information Security Policy for Transport for London (TfL) has been prepared in order to provide a policy basis for the secure management of all of TfL's information and to improve TfL's capability to protect the integrity, availability and confidentiality of information.

1.2 The Committee is asked to approve the draft policy.

2 BACKGROUND

2.1 TfL collects and processes large volumes of information relating to its operations and TfL has an obligation to ensure the security of the information it holds. An Information Security Policy has been developed in order to ensure that a consistent approach is adopted towards the management of information security and to demonstrate compliance with best practice on this issue. The draft Information Security Policy is attached at Appendix 1.

2.2 The management of information security has become an increasingly high profile responsibility, with significant compliance and reputational risks associated with incidents involving the loss of personal data. From April 2010 the Information Commissioner will have the power to impose financial penalties (likely to be up to £0.5 million) on organisations responsible for serious breaches of the Data Protection Act which are likely to cause substantial damage or distress, if the organisation failed to take reasonable preventative steps to avoid the breach. Custodial sentences will be introduced from April 2010 for individuals convicted of the offence of knowingly or recklessly obtaining or disclosing personal data without the consent of the data controller.

3 INFORMATION SECURITY

3.1 The draft policy sets a framework within which TfL will manage all information, whether electronic, on paper, or otherwise, in a way that provides protection from unauthorised use, disclosure, modification and accidental or intentional damage or destruction.

3.2 The draft policy sets out the responsibility of individual employees and managers and 'information owners' who rely on information and information systems for the delivery of a TfL service or process. In addition, Your IM will develop and implement a series of standards and procedures to provide assurance that information stored and transmitted electronically is adequately protected. The policy also requires information risks to be managed through

TfL’s existing risk management framework.

3.3 The policy will be supported by the introduction of a scheme to apply security classifications to TfL’s information. This will enable the identification of information which requires particular protection and ensure that it is handled according to standards prescribed by the scheme. The level of classification (‘Not Protectively Marked’, ‘TfL Restricted’ or TfL Confidential’) will be based on an assessment, using standard criteria, of the impact that would be caused in the event the information was disclosed or accessed without approval.

3.4 The draft policy has been prepared by the Information Access and Compliance Team (IACT) within General Counsel. A range of stakeholders across TfL, including the Chief Information Officer and officers with responsibility for security, information handling, fraud investigation, risk management and Your IM strategy, have been consulted on earlier drafts.

3.5 Once approved, the policy will be communicated through a programme of awareness-raising and training co-ordinated by IACT. Implementation of its requirements will be the responsibility of individual employees and managers, ‘information owners’ and Your IM.

4 RISK MANAGEMENT

4.1 The policy will have implications for the range of risks reported through TfL’s risk management framework and should increase the visibility of the risks associated with information security, and their mitigating actions.

5 RECOMMENDATION

5.1 The Audit Committee is asked to APPROVE the draft Information Security Policy.

6 CONTACT

6.1 Contact: Ellen Howard, Director of Corporate Governance
Email: Ellenhoward@tfl.gov.uk
Phone: 020 7126 4221

Appendix 1

Information Security Policy

Issue date: xx xxxx 2009
Effective: xx xxxx 2009

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:

   1.1 protect its integrity, availability, and confidentiality;

   1.2 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

   1.3 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 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.

6. Information Risk: that part of TfL's overall risk portfolio which relates to the, integrity, availability and confidentiality of information within the TfL Group.

7. 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.

8. 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.

9. 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.

10. Information System: information in all media, hardware, software and supporting networks and the processes and human resources that support its acquisition, storage and communication.

11. 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.

12. Transport for London (TfL): the statutory corporation and its operating subsidiaries.

Organisational scope

13. 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 information 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:

    15.1 Information Security Standard ISO/IEC 27001 and associated Code of Practice for Information Security ISO/IEC 27002:2005.

    15.2 Her Majesty's Government (HMG) Security Policy Framework.

    15.3 Cross Government Mandatory Minimum Measures for Data Handling.

    15.4 Government Protective Marking Scheme (GPMS).

    15.5 Payment Card Industry Data Security Standard (PCI DSS).

Policy content

16. TfL’s policy is to ensure that:

    16.1 Information Security is considered as a fundamental and integral part of all TfL operations.

    16.2. Statutory requirements to safeguard the security of information are met and the accuracy, completeness and segregation of personal data are assured.

    16.3 Information is accessible to authorised users when they need it and is assigned an appropriate security classification.

    16.4 IT 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.

    16.5 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.

    16.6 Business continuity plans, including disaster recovery plans, are implemented to support business needs and appropriate Information Security training is given to TfL Personnel.

    16.7 All Information Security Breaches, actual or suspected, are reported and investigated and a culture exists where improving Information Security procedures is encouraged.

    16.8 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's Business Continuity Teams, will manage and co-ordinate strategies for resilience, including business recovery following information loss or corruption or unauthorised disclosure or access.

24. TfL's Business Continuity Teams 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. The Information Access & Compliance Team (IACT), Fraud & Security and IM Operational Security are responsible for managing actual or suspected information security incidents and breaches and recommending additional or improved security measures to prevent the reoccurrence of such incidents and breaches.

26. IACT is responsible for the interpretation of this policy, for monitoring compliance with the policy and for providing advice and guidance on its implementation.

27. Your IM are responsible for advising TfL 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 TfL's information on creation or receipt, irrespective of format or medium, and information classified according to this scheme must be transmitted, stored and disposed of as required by the classification scheme 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 IACT 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. TfL 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 [.....................] on [……].

35. This policy will be subject to periodic review as considered appropriate by General Counsel.

Policy owner

36. 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 (IM asset register).
- Security vetting for sensitive roles within IM.
- IM 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.