Schedule 14

Security

1. Scope

1.1 This Schedule 14 sets out the Service Provider's obligations in respect of:

(A) TfL's security requirements relating to the Services and Service System(s); and

(B) the development, updating and testing of the Security Policy and Security Plan.

2. Security Policy

2.1 The Service Provider shall ensure that the Security Policy is initially Approved in accordance with the Implementation Plan and shall subsequently, at its own cost and in accordance with the Requirements:

(A) refine, expand and amend the Security Policy:

(1) in accordance with the Implementation Plan (and, in any event, prior to the Operational Commencement Date); and

(2) within ten (10) Working Days, or such other period as may be expressly agreed in writing by the Parties following the implementation of a Change so as to incorporate the effects of that Change in the Security Policy; and

(B) promptly prepare a written review of the Security Plan (as the same may be amended from time to time in accordance with paragraph 2.1(A)(2)) upon request from TfL from time to time and in any event at least once in every twelve (12) Month period following the Operational Commencement Date,

and in each case, the Service Provider shall submit a copy of those documents (as applicable) to TfL for Approval.

2.2 The Service Provider shall ensure that the Security Policy shall:

(A) include specific detail related to the Services and Service System(s);

(B) reference and comply with, and be consistent with, this Schedule 14;

(C) reference and comply with the security requirements set out in Schedule 2 (*Statement of Requirements*);

(D) comply with all relevant TfL Policies in relation to the security of the Service System(s) and Services; and

(E) comply with such other requirements that TfL may reasonably request from time to time.

2.3 The Service Provider shall ensure that the Document Library at all times contains the up-to-date Security Policy.

3. **Security Plan**

3.1 The Service Provider shall ensure that the Security Plan is:

(A) **i**nitially Approved in accordance with the Project Plan; and

(B) **s**ubsequently refined, expanded and amended by the Service Provider and Approved by TfL:

(1) in accordance with the Implementation Plan (and, in any event, prior to the Operational Commencement Date); and

(2) formally reviewed every twelve (12) Months from the Operational Commencement Date.

3.2 The Security Plan shall set out the processes and Security Operating Procedures that the Service Provider will implement at the Premises and otherwise in relation to the Services and Service System(s) to ensure compliance with the Security Policy.

3.3 If and to the extent that any existing security policies and procedures in force at any of the Premises or that otherwise apply in relation to the Services or Service System(s) do not comply with the Security Policy, the Service Provider shall amend such security policies and procedures so as to conform with the Security Policy and set these out in the Security Plan (at no cost to TfL).

3.4 The Service Provider shall ensure that the Security Plan shall be consistent with this Schedule and with the Security Policy.

3.5 The Service Provider shall ensure that the Security Plan at all times includes:

(A) fully documented security processes as necessary and relevant for secure operation of the Services (such process to be set out as an appendix in the Security Plan);

(B) fully documented security operating procedures as necessary and relevant for secure operation of the Services(such process to be set out as an appendix in the Security Plan);

(C) all security measures to be implemented and maintained by the Service Provider (and its Sub-Contractors) in relation to all aspects of the Service System(s) and Services including the code of connection (and any similar requirements) of any relevant Vehicle Data Service;

(D) uses the same structure as BS IS0/IEC 27001:2005 (*Specification for Information Security Management*) or any replacement, substitute or superseding standard (provided that TfL must first consent in writing to such replacement, substitute or superseding standard);

(E) a demonstration that steps 1 to 6 of Figure 1 - Establishing a Management Framework in BS IS0/IEC 27001:2005 (*Specification for Information Security*

Management), or the corresponding section in any replacement or superseding standard, have or will be completed by the Service Provider by the Operational Commencement Date;

(F) a demonstration that the current requirements of the Payment Card Industry Data Security Standard as may be amended or replaced from time to time ('PCI DSS') are being met;

(G) a demonstration that the current requirements of the Data Protection Act as may be amended or replaced from time to time are being met;

(H) an obligation on the Service Provider and its Sub-Contractors to use industry standard disk-wipe software and other mechanisms as laid out in Schedule 34 (TfL Policies) ("TfL's Secure Erasure and Disposal Policy – IM-S-PO-035") to render unusable all media that are no longer operational. This includes optical disks, floppy disks, hard disk drives, solid state storage, paper and tapes;

(I) an obligation on the Service Provider to ensure that the procedure used to comply with paragraph 3.5(F) is documented and tested and to produce certificates of destruction upon request by TfL;

(J) without limitation to any other provision of this Agreement, the date or periods for reviews of, and updates to, the Security Plan;

(K) an acknowledgment that it complies with all relevant policies set out at Schedule 34 (TfL Policies) in relation to the security of the Service System(s) and Services; and

(L) the parameters of reviews and updates referred to in paragraph 3.5(J) above by the Service Provider, including:

(1) all new or changed threats to the Services or Service System(s) and relevant countermeasures;

(2) emerging Good Industry Practice in relation to physical and logical security;

(3) responses to any Security Incident that occurred in relation to the Services, Service System(s) and Services; and

(4) identification and enhancement of any security measure in relation to the Service System(s) or Services which fail to meet Good Industry Practice.

3.6 The Service Provider shall ensure that the Document Library at all times contains the up-to-date Security Plan.

4. **Security Principles**

4.1 The Service Provider acknowledges and agrees that security and Data and Information confidentiality in connection with the Services and the Service System(s) are of key importance and fundamental to the evidential and financial

security requirements necessary to administer and operate the Services and to retain public confidence.

4.2 The Service Provider shall, and shall procure that its Sub-Contractors shall, at all times ensure that the Services and the Service System(s):

(A) avoid the security threats to the Services, Service System(s) and Services in accordance with the Statement of Requirements;

(B) fully comply with:

(1) the Data Protection Act,

(2) BS ISO/IEC 27002:2005 (previously named ISO/IEC 17799:2005) (Code of Practice for Information Security Management);

(3) the current, at any given moment in time, requirements of PCI DSS; and

(4) all relevant policies set out at Schedule 34 (TfL Policies) in relation to the security of the Service System(s) and Services,

each as amended or replaced from time to time;

(C) are certified as meeting ISO/IEC 27001:2005 and shall maintain such certification throughout the Term, and;

(1) the scope of such certification must specifically include all elements that comprise or support the Services;

(2) proof of current and up to date certification to ISO/IEC 27001:2005 must be provided to TfL upon request, within fourteen (14) days of the request being made;

(3) full details of the certification scope will be made available to TfL upon request, within fourteen (14) days of the request being made; and

(4) full details of the relevant ISO/IEC 27001:2005 "Statement of Applicability" will be made available to TfL upon request, within fourteen (14) days of the request being made;

(D) comply with the relevant components of ITSEC, as amended and updated by Common Criteria for Information Technology Security Evaluation or ISO/IEC 15408 standards.

4.3 The Service Provider shall keep all Data, Information, Premises, and Service System(s) secure and protected against all loss, damage, corruption, unavailability and unauthorised use, access or disclosure in accordance with standards not to fall below those standards:

(A) set out in this Schedule 14;

(B) set out in the Security Policy;

(C) set out in Clause 49 (Information Governance);

(D) as set out in the General Statement of Requirements and TfL's Information Security Classification Standard as amended or replaced from time to time; and

(E) consistent with Good Industry Practice, for example as set out in CESG Data Handling Final Report – June 2008.

4.4 TfL may from time to time specify the appropriate security classification at which the Service Provider shall protect and keep secure all Data, Information, Premises, and Service System(s) and the Service Provider shall design and implement the controls, processes and procedures required to comply with such security classification. To the extent that the security classification specified by TfL requires any changes to the Requirements, the impact of such changes shall be considered and implemented in accordance with the Change Control Request Procedure.

4.5 The Service Provider shall design and implement the controls, processes and procedures required to comply with any relevant Vehicle Data Service's security requirements and shall ensure (at its own cost) that the associated controls, processes and procedures are assessed by a qualified Clas consultant in accordance with the guidance given at www.cesg.gov.uk/publications/documents/is1_risk_assessment.pdf and shall provide such Clas consultant report to TfL on or before the date specified for the delivery of such report in the Implementation Plan.

4.6 Prior to the Milestone Date for Milestone T1 (''Ready to Commence TE Service Proving''), the Service Provider shall submit a summary of the design of all security controls, processes and procedures, together with the assessment obtained from a Clas consultant pursuant to paragraph 4.5, to TfL for Assurance and, once Assured, shall implement and comply with such security controls, processes and procedures.

4.7 The Service Provider shall immediately notify TfL of any actual or threatened breach in connection with the security of the Services, Service System(s) and the Services.

4.8 The Service Provider shall ensure that appropriate background security checks of all Service Provider Personnel are performed before such Service Provider Personnel are permitted to access the Services or the Service System(s).

4.9 The Service Provider shall be liable for any breaches of the access permissions allocated to the Service Provider or its Personnel for access to the Service System(s).

4.10 The Service Provider shall ensure that Hardware used in the provision of any of the Services is not reused or is only reused in accordance with the Security Plan.

4.11 The Service Provider's obligations in respect of physical security of Assets are set out in Schedule 2 (*Statement of Requirements*).

4.12 The Service Provider shall design and build, and apply any changes to, a Service System(s) in such a way that the impact of exposure of Personal Data, data relating to the Service or its configuration that could pose a security risk and data supplied by government agencies, to unauthorised parties is minimised (to the extent reasonably possible) including by ensuring partitioning/segmentation of data occurs to the extent necessary to prevent retrieval of large volumes of aggregated data in

order to reduce the data handling requirements that would be imposed by any government agency.

5. **Notification and reporting of Security Incidents**

5.1 The Service Provider shall, and shall procure that its Sub-Contractors shall:

(A) promptly identify all Security Incidents;

(B) immediately:

(1) classify each Security Incident according to the Severity Levels (if appropriate); and

(2) record each Security Incident and corresponding Severity Level in the Incident Log;

(C) where a Security Incident involves Personal Data, notify TfL as soon as possible and in any event in accordance with the timeframes set out in Schedule 5 (*Service Level Agreement*); and

(D) without limitation to the other provisions of this Agreement, follow TfL's instructions in relation to the:

(1) identification and resolution of each Security Incident; and

(2) recording of Incidents, Errors and Service Issues on the Incident Log, as applicable.

5.2 Without limitation to the other provisions of this Agreement, the Service Provider agrees that each Security Incident will be classified as Severity 1 or Severity 2 (as TfL may instruct), unless the Service Provider can demonstrate to TfL's satisfaction that a classification of Severity 3 or lower would be more appropriate.

5.3 If a Security Incident occurs:

(A) the Service Provider shall as soon as possible (at no cost to TfL) correct, make good, reinstate, replace and fix all deficiencies, loss and/or damage to the Service System(s) and/or Services in connection with a Security Incident, and/or perform or re-perform Tests or alternative tests relating to the security of the Service System(s) and/or Services, as appropriate, including within timeframes specified by TfL from time to time, to demonstrate to TfL's satisfaction that the relevant parts of the Service System(s) and Services provide the features, functions, and facilities and meet the performance criteria specified in the Requirements and this Agreement including in connection with the Service Provider implementing any Security rectification plan pursuant to section 5.3(B);

(B) the Service Provider shall immediately and at the Service Provider's cost prepare a security rectification plan including full details of the steps to be taken by the Service Provider to perform its obligations under section 5.3(A) and shall, without limiting section 5.3(A), submit a copy of that security rectification plan to TfL for its Approval and, subject to such Approval, the

Service Provider shall fully implement and comply with that security rectification plan;

(C) the Service Provider shall promptly escalate the matter to such level of seniority within the Service Provider's Personnel as TfL may require; and/or

(D) TfL may exercise its rights under Clause 59 (Enhanced Co-operation) and Clause 60 (*Step-In*).

6. Testing of the Security Plan

The Service Provider shall, in relation to the Security Plan and at no additional cost to TfL conduct Tests to assure compliance with the Security Plan and with TfL's Security Policy, the security provisions in this Agreement and this Schedule 14. Testing should be conducted in accordance with Schedule 4 (Testing Regime) and make the results available to TfL upon request. Such security tests must be conducted, as a minimum, every twelve (12) Months from the Operational Commencement Date and shall also include security penetration testing of the System(s) and the associated technical infrastructure. For services that are accessible from the internet or other such public network then security penetration tests must also be carried out from the internet or the public network.

7. Auditing

7.1 In addition to the auditing requirements of PCI DSS, the Service Provider shall at least once within each twelve (12) month period from the Operational Commencement Date, engage an appropriately skilled Third Party to conduct a formal audit of the Service System(s) and Services against the then current versions of the following:

(A) the Security Plan;

(B) the controls, processes and procedures put in place or required pursuant to this Agreement;

(C) the Data Protection Act (using BS10012 or another standard as agreed with TfL); and

(D) BS IS0/IEC 27001:2005 / BS ISO/IEC 27002:2005.

8. Specific Requirements

8.1 In addition to its obligations in this Schedule, the Service Provider shall comply with the following specific requirements:

(A) **Service System(s) - Anti-Malware Scanning and Protection**

(1) The Service Provider shall provide all Service Provider Personnel with induction and ongoing training in the processes and procedures used to protect the Service System(s) from Viruses, worms, spyware and other potentially destructive devices, and how to manage the impact of such

attacks in accordance with the Incident Management Process.

(2) The Service Provider shall ensure that all procedure manuals related to anti-malware protection are readily available to all relevant Personnel.

(B) **Risk Management**

(1) The Service Provider shall submit a proposal for a risk management methodology to TfL for Approval and, once Approved, shall implement such methodology prior to the Planned Operational Commencement Date.

(2) The Service Provider shall provide TfL with full details relating to identified risks, risk scoring and risk treatment plans upon request, within fourteen (14) days of the request being made.

(C) **Security and Audit Logs**

(1) The Service Provider shall ensure that an audit trail of all Users accessing Evidential Records (including Penalty Notices) is maintained, including Users with read-only access.

(2) The Service Provider shall ensure that the Service System(s) maintains a record of User access to all Personal Data, including Correspondence and voice recordings of calls with Customers.

(3) The Service Provider shall maintain a log of all retrievals of data from the Vehicle Data Service records through the Service System(s) Interfaces.

(4) The Service Provider shall maintain a log of all User logon attempts, successful and failed, to all Service System(s) applications and any other elements of the Service System(s) requiring authentication.

(5) The Service Provider shall maintain a log of all User Account creations, deletions, IT system group memberships, User and group privilege changes against each of the system resources.

(6) The Service Provider shall implement recording mechanisms**,** to identify individual Users and their actions when cases of misuse and fraud are being investigated. The Service Provider shall ensure that recording mechanisms are protected against manipulation and disruption by Users and malicious computer processes.

(7) The Service Provider shall implement a process which will verify and validate all files transferred onto and from the Service System(s). This process will include controls which ensure that only authorised files are transferred by using principles of segregation of duties (so that no person is given responsibility for more than one related function, for example, a person creating content to be uploaded into the Service System(s) must not be able to load such content themselves and a different person will be responsible for the verification, validation and upload functions).

(8) The Service Provider shall implement a mechanism to strictly control

and limit the application programs that can be executed. Only programs necessary for the correct operation of the Service System(s) shall be permitted to execute. The Service Provider shall formally record these permitted programs, along with version numbers and justifications for executing any such programs and must log all attempted violations, such log to record (without limitation);

(i) the name of the user attempting to execute an unauthorised program;

(ii) the date and time of the incident; and

(iii) the IP address of the system.

Any such violation attempt must be recorded as a Security Incident and investigated to identify the root cause.

(9) The Service Provider shall provide any system audit log data (being any log data that is collected by the Service Provider during the delivery of the Services) to TfL on request, in a human readable electronic format. Acceptable formats are Comma Separated Value or Microsoft Excel.

(10) The Service Provider shall ensure that all system audit log files are retained in accordance with Schedule 2 (*General Statement of Requirements*), Appendix 24 (*Data Retention*).

(D) **Security Management**

(1) The Service Provider shall propose a member of the Service Provider Personnel as Security Manager to TfL for Approval (and, when Approved, shall appoint such person).

(2) The Service Provider shall ensure that the Security Manager shall provide a security management service to develop, monitor, enforce, maintain and enhance all aspects of the Security Plan throughout the Term.

(3) The Service Provider shall provide security reports detailing any security breaches to TfL in accordance with the Incident Management Process and the associated Requirements in Schedule 2 Statement of Requirements (General);

(4) The Service Provider shall provide a detailed report to TfL within forty eight (48) hours of the resolution of a Security Incident. This report shall detail:

(a) the nature of the Security Incident;

(b) the causes and consequences of the Security Incident;

(c) the actions taken to handle the Incident and timeframes applicable to resolution of the Security Incident; and

(d) actions to prevent recurrence of the Security Incident.

(E) Evidential Records

(1) The Service Provider shall ensure that the Detection Event Evidential Records received from the Detection and Event Infrastructure are transferred to a Permanent Evidence Store without alteration in a secure manner, so that the confidentiality and integrity of the records is assured, unauthorised personnel cannot view or access the records and the records will not be altered in any way.

(2) The Service Provider shall ensure that the permanent evidence store utilises Write Once Read Many technology so that the master record cannot be deleted.

(3) The Service provider shall ensure that access to the Permanent Evidence Store is strictly controlled and only provided to specifically authorised personnel. The Service Provider will maintain a register of authorised personnel. This register must be validated at ninety (90) day intervals.

(4) The Service Provider shall ensure that a logged audit trail is maintained for all access to the Permanent Evidence Store.