SCHEDULE 14

Security Policy

1. Security Principles

1.1 The Service Provider agrees that security and Data confidentiality in connection with the Services and the Service Systems are of key importance and are fundamental to the evidential requirements necessary to administer and enforce the Schemes and to retain public confidence in road charging schemes.

1.2 The Service Provider shall ensure that the Services and Service Systems at all times provide a level of security which:

(A) is in accordance with the London Congestion Charging Evidential Handbook and Good Industry Practice (including but not limited to HOSDB guidelines, Department for Transport evidential standards and Mayoral-endorsed evidential standards, to the extent the same have been communicated to the Service Provider or it has otherwise been made aware, or should have been made aware of them, provided that if the Service Provider can demonstrate to TfL's satisfaction that it will have to incur materially increased costs as a result of complying with its obligation under this paragraph 1.2(A) in relation to any changes to Mayoral-endorsed evidential standards as were in place as at the Effective Date, the Service Provider shall be permitted to pass on such costs to TfL in accordance with the Change Control Request Procedure). For the avoidance of doubt, where there is conflict between the London Congestion Charging Evidential Handbook and the HOSDB guidelines, Department for Transport evidential standards and Mayoral-endorsed evidential standards, the Service Provider will comply with the London Congestion Charging Evidential Handbook; and

(B) meets specific security threats to the Services and the Service Systems in accordance with the Specification.

1.3 The Service Provider shall, in relation to the Services and Service Systems:

(A) at all times comply with BS7799/IS0/IEC 27001:2005, BSISO/IEC17799:2005 and BS6079-3:2002 (or replacements) and ensure that each Sub-Contractor does so;

(B) at all times comply with all ITSEC standards and ensure that each Sub-Contractor does so;

(C) ensure that Testing is carried out in relation to the Security Plan and that the Security Plan is Approved in accordance with schedule 3 (Milestones and Deliverables);

(D) without limiting any other provision of this Agreement, regularly and at least once per six (6) month period, conduct updates and audits in connection with the Security Plan;

(E) at all times keep all Data, Information, Premises and Systems used by the Service Provider (and/or a Sub-Contractor) in connection with the Services and the Service Systems secure and protected against all loss, damage, corruption and unauthorised use, access or disclosure in accordance with standards not to fall below those dictated by Good Industry Practice; and

(F) at all times ensure that the Security Plan allows TfL Confidential Information and Personal Data to be protected in accordance with the provisions of this Agreement.

1.4 The Service Provider shall at all times:

(A) comply with TfL's IT and security policies and procedures in relation to the Services and Service Systems, from time to time in effect, to the extent the same have been communicated to the Service Provider or it has otherwise been made aware of them, provided that if the Service Provider can demonstrate to TfL's satisfaction that it will have to incur materially increased costs as a result of complying with its obligation under this paragraph 1.4(A) in relation to any changes to TfL's IT and security policies and procedures as were in place as at the Effective Date and such costs would not have been incurred as a result of the Service Provider complying with paragraph 1.2(A), the Service Provider shall be permitted to pass on such costs to TfL in accordance with the Change Control Request Procedure;

(B) fully support and co-operate with all of the security initiatives of TfL from time to time, to the extent the same have been communicated by TfL in writing to the Service Provider and subject to any changes to such assistance required as a result of changes to such initiatives after the Effective Date being implemented as a Mandatory Change;

(C) promptly comply with the reasonable instructions of TfL relating to all policies, procedures and initiatives specified in paragraphs 1.4(A) and 1.4(B) of this schedule;

(D) immediately notify TfL of any actual or threatened breach in connection with the security of the Services and the Service Systems;

(E) ensure that appropriate security checks of all Personnel are performed before they are permitted to access any of the Hardware, Software or Systems used in connection with the Services (including but not limited to the Service Systems); and

(F) ensure that Hardware is not reused or is only reused in accordance with the Security Plan.

2. **Security Plan Provision**

2.1 The Initial Security Plan is set out in Annex A to this schedule.

2.2 The Initial Security Plan shall be refined and expanded by the Service Provider and delivered to TfL for Approval and Approved as a condition of achievement of the

Milestones as set out in schedule 3 (Milestones and Deliverables). The document so Approved shall be the "**Security Plan**".

2.3 Unless and until the Security Plan has been Approved in accordance with paragraph 2.2, the Service Provider shall comply with the Initial Security Plan.

2.4 The Security Plan shall include specific detail related to each of the Service Elements for which the Service Provider is responsible and shall reference and comply with any security policies in force at the Premises used to provide each of the Service Elements for which the Service Provider is responsible, including this Security Policy.

2.5 If and to the extent that any existing security policies and procedures in force at the Premises used to provide the Services do not comply with the provisions of this Security Policy, such policies and procedures shall be amended so as to conform to the Security Policy.

2.6 The Service Provider shall ensure that the Security Plan deals as a minimum with the security requirements set out in this schedule and the Statement of Requirements, together with such other provisions as the Service Provider deems necessary or TfL may reasonably request from time to time, including, but not limited to, the security measures and procedures in force during both the Implementation Phase and the Operational Phase.

3. Information to be included in the Security Plan for each Service Element

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

(A) all security measures to be implemented and maintained by the Service Provider (and, where Sub-Contractors are used by the Service Provider, by those Sub-Contractors) in relation to all aspects of the Services and the Service Systems;

(B) a demonstration that the Security Plan ensures a level of security sufficient for the purposes of assuring Evidential Integrity in accordance with the London Congestion Charging Evidential Handbook;

(C) the same structure as BS IS0/IEC 27001:2005 (in ISO/IEC 17799 as at the Effective Date) or any replacement, substitute or superseding standard, with cross-referencing to other schedules of this Agreement;

(D) a demonstration that BS IS0/IEC 27001:2005 ("steps 1 to 6 of Figure 1 - Establishing a Management Framework") have or will be completed by the Service Provider by the Operational Commencement Date;

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

(F) the parameters of reviews and updates referred to in (E) above by the Service Provider including:

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

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

(3) responses to any Security Incident that occurred in relation to the Services or the Service Systems; and

(4) any security measure in relation to the Services and Service Systems which fails to meet Good Industry Practice.

4. Severity Levels

4.1 The Service Provider shall:

(A) promptly identify all Security Incidents relating to, or otherwise having an impact on, the Services and Service Systems;

(B) immediately classify such Security Incident according to the Severity Levels (if appropriate);

(C) immediately record each Security Incident and corresponding Severity Level in the Incident Log (and shall use best endeavours to ensure that all Sub-Contractors do so as soon as possible);

(D) comply with its obligations under clause 57 (Security) in connection with each Security Incident; and

(E) without limitation to the other provisions of this Agreement, follow TfL's instructions in relation to the identification and resolution of each Security Incident in relation to the Services and the Service Systems (including the classification of a Severity Level in respect of the Security Incident) and the recording of Incidents, Errors and Service Issues on the Incident Log, as applicable.

4.2 Without limitation to the other provisions of this Agreement, the Service Provider agrees that each Security Incident will be classified as a Severity 1 or a 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. Security Rectification Plans relating to Security Incidents

5.1 The Service Provider shall ensure that each Security Rectification Plan required under clause 57 (Security) includes:

(A) details of all outstanding Security Incidents;

(B) the Severity Level ascribed to each Security Incident;

(C) any workarounds for the Security Incident; and

(D) the dates for correction of, and Testing in connection with the correction of, each Security Incident.

5.2 The Service Provider shall follow any reasonable instructions of TfL in connection with a Security Rectification Plan including promptly incorporating amendments to the Security Rectification Plan suggested by TfL.

ANNEX A

INITIAL SECURITY PLAN

[Information Redacted]