LONDON CYCLE HIRE SCHEME AGREEMENT

Schedule 14 – Security Policy

SCHEDULE 14

Security Policy

This Schedule 14 describes the Service Provider's obligations in respect of the preparation and maintenance of and compliance with the Security Policy and Security Plan.

The Security Policy and Security Plan set out the Service Provider's obligations in respect of ensuring the security of the Terminals, Service Systems and the Services.

The Security Policy covers the security requirements for all Service Systems used in the London Cycle Hire Scheme, including Terminals and Services Website, and includes, as appropriate, physical security where compliance is necessary to the meet specific requirements of certain standards such as PCI DSS.

The Service Provider's obligations in respect of physical security of LCHS Assets are set out in the Statement of Requirements.

Security Principles

1.1 The Service Provider agrees that security and Data confidentiality in connection with the Terminals and Services Website, Service Systems and the Services are of key importance and fundamental to the evidential and financial security requirements necessary to administer and operate the London Cycle Hire Scheme and to retain public confidence.

1.2 The Service Provider shall, and shall procure that its Sub-Contractors shall, at all times ensure that the Terminals, Service Systems and Services:

avoid the security threats to the Terminals, Service Systems and Services in accordance with the Statement of Requirements; and

comply with the requirements of the latest version of PCI DSS, including application for (if applicable) and maintenance of PCI DSS accreditation and certification;

comply with:

BS IS0/IEC 27001:2005 (formerly BS 7799-2:2002) (*Specification for Information Security Management*); and

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

each as amended or replaced;

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

ensure that:

the Security Policy and Security Plan are Approved, in accordance with Schedule 3 (*Milestones and Deliverables*); and

Testing of the Security Plan is carried out in accordance with:

Schedule 4 (*Testing Regime*);

Schedule 3 (*Milestones and Deliverables*) during the Implementation Phase; and

paragraph 6 *(Testing of the Security Plan during the Operational Phase)* of this Schedule 14;

without limiting paragraph 1.2(E) above and any other provision of this Agreement, regularly and at least once per twelve (12) Month period and prior to the Operational Commencement Date, conduct a formal review of and update to the Security Plan at no extra cost to TfL including compliance with the standards defined in paragraph 3 *(Information to be included in the Security Plan for each Service Element)* below as amended from time to time;

keep all Data, Information, Premises, Terminals and Service Systems used by the Service Provider (and/or its Sub-Contractors) in connection with the Service Systems and Services secure and protected against all loss, damage, corruption, unavailability and unauthorised use, access or disclosure in accordance with standards not to fall below those

set out in this Schedule 14; and

dictated by Good Industry Practice;

ensure that the Security Plan allows TTL Confidential Information and all Personal Data to be protected in accordance with the provisions of this Agreement;

comply with all or part of the Information Security Policy set out at Schedule 34 (*TfL Group Policies*) and related TfL Group Policies and procedures in relation to the Service Systems and Services 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 TTL's satisfaction that the Service Provider will have to incur materially increased costs as a result of complying with its obligation under this paragraph 1.2(I) in relation to any changes to the Information Security Policy set out at Schedule 34 (*TfL Group Policies*) and related TfL Group policies and procedures as were in place as at the Effective Date, the Service Provider shall be permitted to pass on such costs to TTL in accordance with the Change Control Request Procedure;

fully support and assist TTL Personnel with all of the security initiatives of the TfL Group from time to time, to the extent the same have been communicated by TTL in writing to the Service Provider and subject to any Changes to such security initiatives after the Effective Date, such Changes being implemented as a Mandatory Change;

promptly comply with the reasonable instructions of TTL Personnel relating to all policies, procedures and initiatives specified in paragraphs 1.2(I) and 1.2 (J) above;

immediately notify TTL of any actual or threatened breach in connection with the security of the Terminals, Service Systems and the Services;

ensure that appropriate background security checks of all Service Provider Personnel are performed before such Service Provider Personnel are permitted to access any of the Terminals and Service Systems used in connection with the Services; and

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

Security Plan Provision

1.3 The Initial Security Plan shall be set out in Annex A (*Initial Security Plan*) to this Schedule 14.

1.4 The Initial Security Plan shall be:

refined, expanded and amended by the Service Provider; and

delivered to TTL for Approval and Approved as a condition of achievement of Milestone 1 (*End of Planning*) as set out in Schedule 3 (*Milestones and Deliverables*),

the document so Approved shall be the "**Security Plan**".

1.5 Unless and until the Security Plan has been Approved in accordance with paragraph 1.4 above, the Service Provider shall comply with the Initial Security Plan.

1.6 The Security Plan shall:

include specific detail related to the Terminals, Service Systems and Services for which the Service Provider is responsible; and

reference and comply with the Security Policy.

1.7 If, and to the extent that any existing security policies and procedures in force at any of the premises used to provide the Services (including the Premises and Business Continuity Premises) do not comply with the provisions of the Security Policy, the Service Provider shall amend such security policies and procedures so as to conform with the Security Policy.

1.8 The Service Provider shall ensure that the Security Plan deals as a minimum with:

the security requirements set out in:

this Schedule 14; and

the Statement of Requirements; and

such other provisions that the Service Provider deems necessary or TTL may reasonably request from time to time.

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

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

all security measures to be implemented and maintained by the Service Provider (and its Sub-Contractors) in relation to all aspects of the Terminals, Service Systems and Services;

the same structure as BS IS0/IEC 27001:2005 (formerly BS 7799-2:2002) (*Specification for Information Security Management*) or any replacement, substitute or superseding standard;

a demonstration that BS IS0/IEC 27001:2005 ("steps 1 to 6 of Figure 1 - Establishing a Management Framework") (formerly BS 7799-2:2002) (*Specification for Information Security Management*) have or will be completed by the Service Provider by the Operational Commencement Date;

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

the parameters of reviews and updates referred to in paragraph 3.1(D) above by the Service Provider, including:

all new or changed threats to the Terminals, Service Systems and Services and relevant countermeasures;

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

responses to any Security Incident that occurred in relation to the Terminals, Service Systems and Services; and

any security measure in relation to the Terminals and, Service Systems and Services, which fail to meet Good Industry Practice.

Severity Levels

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

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

immediately:

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

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

comply with its obligations under Clause 47 (*Security Policy*) in connection with each Security Incident; and

without limitation to the other provisions of this Agreement, follow TTL's instructions in relation to the:

identification and resolution of each Security Incident;

Terminals, Service Systems and Services (including the classification of a Severity Level in respect of the Security Incident); and

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

1.11 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 TTL may instruct), unless the Service Provider can demonstrate to TTL's satisfaction that a classification of Severity 3 or lower would be more appropriate.

Security Rectification Plans relating to Security Incidents

1.12 The Service Provider shall ensure that each Security Rectification Plan required under Clause 47 (*Security Policy*) includes:

details of all outstanding Security Incidents;

the Severity Level ascribed to each Security Incident;

any workarounds for the Security Incident; and

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

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

Testing of the Security Plan during the Operational Phase

1.14 The Service Provider shall, in relation to the Security Plan and at no additional cost to TTL conduct the following Tests no less frequently than every twelve (12) Months from the Operational Commencement Date:

System Level Tests, which shall Test each component of the:

Security Plan; and

Service Systems,

and the capabilities and procedures undertaken by the Service Provider's technical and operational Service Provider Personnel;

Total Service Tests, which shall Test the Service Provider's compliance with the Security Policy; and

to demonstrate that the Service Provider is complying with the Security Policy.

1.15 The Service Provider shall conduct the first System Level Test and Total Service Test no less than four (4) Months following the Operational Commencement Date and as detailed in the Security Plan.

1.16 Subject to TTL's prior written consent, the Service Provider may conduct the Tests described above, at its own cost and expense, more frequently than is specified in

paragraph 6.1 above, if the Service Provider, acting in accordance with Good Industry Practice, deems it necessary.

1.17 TTL shall be entitled to require the Service Provider to conduct the Tests described above (in whole or part), more frequently than as set out in paragraph 6.1 above, in the event that either:

TTL agrees to pay the Service Provider's reasonable costs in carrying out such Tests; or

subject to paragraph 6.4 below, TTL reasonably believes that the Service Provider is not complying with its obligations under this Schedule 14.

1.18 If TTL has requested the Service Provider to conduct Testing pursuant to paragraph 6.2 above, the Service Provider's reasonable costs (as notified in advance in writing and calculated at the rates specified in Annex G (*Principles to Apply to the Pricing of Changes to this Agreement*) to Schedule 9 (*Change Control Request Procedure*)) shall be borne by TTL, unless the Tests fail as determined in accordance with the provisions of Schedule 4 (*Testing Regime*), in which case the costs and expenses (including TTL's and any Interested Party's, Other Service Provider's, the Insurance Provider's and/or Third Party's costs and expenses) shall be borne by the Service Provider.

1.19 The Service Provider shall:

produce Test Plans and Test Specifications for each Test required by paragraph 6.1(A) above; and

make copies of such Test Plans and Test Specifications available to TTL upon request,

provide TTL with ten (10) Working Days' notice of its intention to carry out the Tests;

entitle TTL, at its sole discretion, to require TTL Personnel to participate in Test Witnessing of Tests performed in accordance with this Schedule 14; and

provide TTL with a copy of the results of each Test performed in accordance with this Schedule 14.

1.20 Where Tests require downtime of the whole or part of the Service Systems and/or Services, the date and timing of such Tests shall be subject to prior agreement with TTL. Any downtime approved by TTL in writing and in advance of such Tests being performed shall be excluded from any measurement of Service Levels for the purposes of Schedule 5 (*Service Level Agreement*) in respect of the relevant Performance Indicators affected by such Tests.

1.21 The Service Provider shall:

undertake and manage all Testing required in accordance with the Schedule 14 in full consultation with TTL and any Interested Party, Other Service Provider, the Insurance Provider and/or any Third Party nominated by TTL; and

liaise with TTL in respect of the planning, performance and review of each Test.

1.22 Any participation by TTL in relation to the Testing of the Security Plan will be without prejudice to and will not be deemed in any way to:

restrict the steps required to be taken by the Service Provider pursuant to this Schedule 14; or

be acceptance or Approval by TTL that the Security Plan is adequate.

1.23 If any aspect of the Tests referred to in paragraph 6.1 above fail to meet the criteria in the Security Policy, the Service Provider shall take such action, at its own expense, as is necessary, and repeat such Tests until all the relevant criteria are met.

ANNEX A

Initial Security Plan

[Information Redacted]