LONDON CYCLE HIRE SCHEME AGREEMENT

Schedule 2 – Common Statement of Requirement Lot 2

London Cycle Hire Scheme

Schedule 2

Common Statement of Requirements

Lot 2

INFORMATION COMPLIANCE

1.1 General

1.1.1 The Service Provider shall comply with all obligations in relation to:

a) Data Protection Legislation; and

b) Freedom of Information Legislation,

including those obligations set out in Schedule 15 (*Information Compliance*) and in accordance with schedule 5: Service Level Agreement.

1.1.2 The Service Provider shall provide the Data Protection Notice and/or the terms and conditions relating to the use of the Services Website and/or the London Cycle Hire Scheme to any Customer on request.

1.1.3 The Service Provider shall ensure that there are adequate controls on any manual notes of Personal Data, including financial Data. Such controls shall include measures to protect the manual Data against misuse or loss. By way of illustration, such notes might be made during a manual fallback procedure due to a System Failure.

1.1.4 The Service Provider shall ensure that there is at all times a nominated member of the Service Provider Personnel responsible for ensuring the Service Provider's compliance with its obligations under Data Protection Legislation and FOI Legislation, and in accordance with:

a) this Statement of Requirements;

b) Appendix 1 (*Information Compliance Processes*);

c) Clause 50 (*Information Compliance*);

d) Schedule 15(*Information Compliance*); and

e) Schedule 5 (*Service Level Agreement*).

1.1.5 The Service Provider shall implement a procedure, agreed with TTL in advance, for dealing with Complaints concerning the collection, storage and disclosure of Personal Data. Such Complaints procedure shall allow unsatisfied Customers to make appeals against the outcome of the original Complaint.

1.1.6 The Service Provider shall ensure that all forms of Data (paper and electronic) used to collect Personal Data are written to comply with the Data Protection Legislation.

1.1.7 The Service Provider shall update such forms at no additional charge to TTL, upon request by TTL and as required to comply with the requirements of the Data Protection Legislation.

1.1.8 The Service Provider shall ensure all forms of Data (electronic and paper) clearly indicate (for example, by use of an asterisk) which Data items are mandatory and must be provided. All mandatory items must be agreed with TTL.

1.1.9 The Service Provider shall use a Data Protection Notice (for illustration, the notice in current use is included in Appendix 1: (*Information Compliance Processes*) supplied by TTL and to be updated by the Service Provider at no additional charge to TTL on request by TTL.

1.1.10 The Service Provider shall ensure it has adequate Service Provider Personnel resources in place to oversee and carry out its obligations under this Agreement in relation to Data Protection Legislation and FOI Legislation.

1.2 Freedom of Information Requests

1.2.1 TTL will direct the Service Provider how to respond to the Information Request.

1.2.2 The Service Provider shall gather any relevant Data surrounding the Information Request in the required format (e.g. Data table, graphical representation, copy of Document etc.).

1.2.3 The Service Provider shall implement a procedure (to be agreed with TTL) to deal with FOI requests where the Customer is unable to put their request in writing.

1.3 Complaints

1.3.1 The Service Provider shall escalate, in the first instance, all Complaints relating to infringements of Data Protection Legislation, civil liberties, equality and human rights to authorised TTL Personnel.

1.3.2 The Service Provider shall escalate, in the first instance, all complaints of the nature referred to in paragraph 1.3.1 above against any Other Service Provider or Sub-Contractor to the authorised TTL Personnel.

1.4 Subject Access Requests

1.4.1 The Service Provider shall implement a procedure, to be approved by TTL in advance, for processing SARs in accordance with Data Protection Legislation. The Service Provider shall ensure that all Sub-Contractors also comply with such procedures.

1.4.2 Where the Service Provider (or any Sub-Contractor) is sending a response directly to the individual who has made a SAR, the Service Provider shall ensure that the response is provided to the individual within forty (40) calendar days of such request having been received (wherever the request was initially received).

1.4.3 The Service Provider, if required to provide Information to TTL for a SAR, shall provide the Information within the timescales specified by TTL, and if no timescale is specified, within ten (10) Working Days of the Service Provider’s receipt of the request from TTL.

1.4.4 The Service Provider shall provide statistics to TTL or nominated Third Parties on SARs in accordance with Schedule 15 (*Information Compliance*) and Schedule 5 (*Service Level Agreement*).

1.4.5 Where the Service Provider (or any Sub-Contractor) is required to supply Information to TTL or an Other Service Provider to enable them to respond to a SAR, the Service Provider shall or shall procure that the relevant Sub-Contractor shall supply the Information required within such time and in such form as reasonably requested by TTL or the Other Service Provider. Where no period of time is specified in the request, the Service Provider shall supply the Information within ten (10) Working Days from the date the request is made to the Service Provider or the Sub-Contractor (as appropriate) or such longer period as TTL at its sole discretion may agree.

1.5 Data Protection Audit

1.5.1 The Service Provider shall produce and maintain a Data Protection audit plan to be agreed by TTL, which shall include:

a) timescales for preparation and conduct of the annual Data Protection audit;
b) the Data Protection audit strategy and planned outputs;
c) details of the independent Third Party undertaking the Data Protection audit;
d) the Service Provider Personnel responsible for fulfilment of the Data Protection audit plan; and
e) the Service Provider Personnel responsible for the management of the independent Third Party undertaking the Data Protection audit.

1.5.2 The Service Provider shall implement a comprehensive Data Protection audit, to be undertaken by an independent Third Party approved by TTL, covering all Data Processing undertaken by the Service Provider. The Data Protection audit will be completed at no cost to TTL.

1.5.3 The Service Provider shall conduct the Data Protection audit annually (or at a frequency agreed with TTL) and report the findings to TTL.

1.5.4 The Service Provider shall act on the findings from any Data Protection audits to ensure (within timescales agreed by TTL) that the Service Provider's Processing, storage, disclosure and destruction of Personal Data are conducted in accordance with:

a) the Data Protection Legislation;
b) the provisions of Clause 50 (*Information Compliance*);
c) Schedule 15 (*Information Compliance*); and
d) Schedule 5 (*Service Level Agreement*).

2 FINANCE

2.1 General

2.1.1 The Service Provider shall support the accounting Service System to:

a) accurately record all financial transactions; and
b) satisfy the requirements of Schedule 32 (*Revenue Collection and Payment*).

2.1.2 The Service Provider shall ensure that Service Provider Personnel responsible for managing the finance function are fully qualified accountants holding a recognised UK accounting qualification and are fully trained to a level sufficient to enable them to perform their duties competently.

2.1.3 The Service Provider shall ensure sufficient segregation of duties within the finance team and will operate internal independent reviews and supervision as is necessary to safeguard the integrity of the financial processes.

2.1.4 The Service Provider shall maintain a direct Interface to the designated Merchant Acquirer in order to process debit card/credit card transactions.

2.1.5 The Service Provider shall record separately from gross income any charges made by the Merchant Acquirer.

2.2 Standards

2.2.1 The Service Provider shall ensure full compliance with:

a) UK Generally Accepted Accounting Principles (UK GAAP); and
b) International Accounting standards (IAS),

as recognised and applied by TTL in recognition of all financial transactions.

2.2.2 The Service Provider shall comply with PCI DSS, as amended from time to time.

2.2.3 The Service Provider shall maintain proper books and records of all individual financial transactions, LCHS Assets and liabilities.

2.2.4 The Service Provider shall supply a copy of such books and records to TTL upon request.

2.2.5 The Service Provider's working practices shall conform to the Investors in People standard.

2.2.6 The Service Provider shall ensure that the completeness and integrity of all financial processes are maintained at all times on all accounting Service Systems.

2.2.7 The Service Provider shall implement accounting policies that are agreed with TTL.

2.2.8 The Service Provider shall have processes in place to ensure timely recovery of fees for failed debit card/credit card and any other form of receipt.

2.2.9 The Service Provider shall ensure all payments received are banked on the day of receipt when the payment is received before midday, and on the next Working Day in all other circumstances.

2.2.10 The Service Provider shall maintain sufficient records to provide a full audit trail (as defined by TTL) to meet the requirements of:

a) Clause 42 (*Audit and Inspection*);
b) external auditors of the TfL Group;
c) internal auditors of the TfL Group; and
d) the contract management and monitoring reporting requirements.

2.2.11 The Service Provider shall provide updates to TTL's general ledger on a periodic basis (as per TTL's reporting cycle) and shall adopt the same four (4) Weekly financial period end dates as TTL.

2.2.12 The Service Provider shall reconcile all receipts and provide TTL with a Weekly reconciliation report.

2.2.13 The Service Provider shall be responsible for obtaining payment via debit cards/credit cards by using TTL's card Merchant Acquirer.

2.3 Control

2.3.1 The Service Provider shall ensure that security procedures, which have been approved by TTL, are in place to safeguard all books and records relating to TTL and are in accordance with:

a) Good Industry Practice; and
b) Schedule 14 (*Security Policy*).

2.3.2 The Service Provider shall maintain a log for all detected fraudulent activities/attempted fraudulent activities carried out on a Customer Record and a Service System and inform TTL of such instances.

2.3.3 The Service Provider shall perform ad hoc checks and reconciliations as requested by TTL to prove the completeness and integrity of Data entered into the Service Provider’s accounting Service System.

2.3.4 The Service Provider shall operate control accounts and reconciliation procedures across all such accounts.

2.3.5 The Service Provider shall provide written details of all proposed adjustments due to reconciliation differences to TTL one (1) Week before period end.

2.3.6 The Service Provider shall ensure that procedures are applied to prevent and detect actual or attempted fraud both from within and external to the Service Provider. These procedures shall be Approved by TTL.

2.3.7 For the purposes of debit card/credit card fraud and other investigations, the Service Provider shall provide all required and requested Data and statements directly to the Metropolitan Police Authority (or appropriate relevant authority).

2.3.8 The Service Provider shall ensure that appropriate procedures, which have been approved by TTL, are in place to ensure sufficient segregation of duties between the finance team, the internal independent review and supervision as is necessary to safeguard the integrity of the financial processes.

2.3.9 The Service Provider shall identify and investigate irregular payment patterns, specifically relating to Refunds and shall notify TTL of such events.

2.3.10 The Service Provider shall maintain and update the detected fraudulent activities/attempted fraudulent activities log ensuring that all newly detected fraudulent/attempted fraudulent activities are recorded as soon as they occur.

2.3.11 The Service Provider shall refer to and consider the information in the corresponding detected fraudulent activities/attempted fraudulent activities log when processing charge-backs and Refunds for an Account.

2.3.12 The Service Provider shall provide annual internal fraud detection and prevention training to all Service Provider’s Personnel involved with processing payments.

2.3.13 The Service Provider shall comply with the terms and conditions of the TfL Merchant Acquirer Agreement, including all reasonable opportunities presented to safeguard against fraudulent transactions

2.3.14 The Service Provider shall obtain authorisation from TTL before making Refund payments that are above the Refund threshold as specified by TTL and detailed in Appendix 4 (*Returns Policy*).

2.4 Accounts Receivable

2.4.1 The Service Provider shall accurately record all Revenue receipts for the London Cycle Hire Scheme as accounts receivable in the accounting Service System.

2.4.2 The Service Provider shall ensure that, where batch processing is undertaken, there are sufficient and adequate controls, such as the use of batch totals and segregation of duties (e.g. segregating banking from reconciliation processes), applied to ensure the completeness and accuracy of input.

2.4.3 The Service Provider shall use the facility to trace dishonoured charge-backs and Declined Payments (disputed card payments) received to the source transaction(s).

2.4.4 The Service Provider use processes for the identification and recovery of underpayments.

2.4.5 The Service Provider shall provide methods of debt recovery in the event of dishonoured charge-backs.

2.4.6 The Service Provider shall be liable for any charge-backs and Declined Payments, where the card issuer does not provide requested monies, resulting from the Service Provider’s failure to comply with the terms and conditions of TfL’s Merchant Acquirer Agreement.

2.4.7 The Service Provider shall provide a summary report of debtors after each accounting period and once the general ledger and debtor accounts have been reconciled.

2.5 Accounts Payable

2.5.1 The Service Provider shall ensure that all payments including payments of Refunds to Customers are recorded accurately as accounts payable in the accounting Service System.

2.5.2 The Service Provider shall implement processes to ensure that the accounting Service System correctly identifies and records all transactions in line with UK GAAP for each transaction, including:

a) full Refunds;
b) partial Refunds;
c) Refunds covering a future period;
d) Refunds of deferred income; and
e) good-will payments.

2.5.3 The Service Provider shall implement processes to ensure that the policies and controls relating to the accounts payable and Payments shall include all transactions.

2.5.4 The Service Provider shall process all Refunds up to agreed limits as advised by TTL in accordance with Appendix 4: (*Returns Policy*).

2.5.5 The Service Provider shall ensure that any Refunds are only made for:

a) overpayments or duplicate payments resulting from an error of the Service Provider;
b) overpayments above the threshold, which have been agreed with TTL;
c) Refunds in line with Appendix 4 (*Returns Policy*); and
d) Incorrect charge amounts due to Bicycle or Docking Point failure.

2.6 Reporting

2.6.1 The Service Provider shall provide financial reports and journals relating to each period in an electronic format to TTL by the end of Working Day one (1) of the subsequent period detailing each transaction, including:

a)	income and expenditure (profit and loss accounts)	– periodic basis;
b)	income analysis	– periodic basis;
c)	receipts and payments	– Weekly;
d)	income reconciliation	– periodic basis;
e)	balance sheet and trial balance	– periodic basis;
f)	bank reconciliations	– Weekly and periodic basis;
g)	bank adjustments	– Weekly and periodic basis;
h)	aged debtors	– periodic basis;
i)	failed receipts report	– Weekly and periodic basis;
j)	receipts and payments	– periodic basis;
k)	deferred income	– periodic basis;
l)	overpayments	- periodic basis; and
m)	unidentified receipts	- periodic basis.

2.6.2 The Service Provider shall ensure that all reports are securely transferred to TTL, for example via ODETTE file transfer protocol.

3 STANDARDS, WORKING PRACTICES & PRINCIPLES

3.1 General

3.1.1 The Service Provider shall employ programme management and Development Methodologies which either follow:

a) an industry standard; or
b) are well documented and can be demonstrated to follow Good Industry Practice.

3.1.2 The Service Provider shall adhere to the standards and working practices of internationally recognised organisations as referenced in Table 1 *(Organisations)* and Table 2 *(Standards)* below, or, where such standards and working practices have been amended and/or superseded, by the latest revisions or superseding standards and working practices, or any standard which is generally recognised as being equivalent to it.

Table 1 – Organisations

BSI	British Standards Institution
NEMA	National Electrical Manufacturers Association
EIA	Electronic Industries Alliance
ISO	International Organisation for Standardisation
IET	Institution of Engineering and Technology
TfL	Transport for London
HSE	Health and Safety Executive

Table 2 – Standards

BS ISO/IEC 270 02:2005	Code of Practice for Information Security Management
BS7671	The IET Wiring Regulations
BS ISO/IEC 26514:2008	Guidelines for the documentation of computer-based application systems

BS EN ISO 9000-3	Guidelines for the application of ISO 9001:2000 to the development, supply, installation and maintenance of computer software
BS EN 60950-1:2006	Specification for safety of information technology equipment, including electrical business equipment
BS EN 60529	Specification for degrees of protection provided by enclosures (IP codes)
BS EN 60073	Basic and safety principles for man-machine interface, marking and identification. Coding principles for indication devices and actuators
BS ISO/IEC 6592	Guidelines for the documentation of computer-based application systems
EN 55022	Electro Magnetic Compatibility
BS EN 60617	Graphical symbols for diagrams
BS EN 60950	Specification for safety of information technology equipment, including electrical business equipment
TR 2130C	Environmental tests for Motorway Communications equipment
IEC Publication 68	Environmental Testing
BS IS0/IEC 2700 1:2005	Specification for Information Security Management
BS ISO/IEC 270 02:2005	Code of Practice for Information Security Management
POSIX	Information Technology. Portable Operating System Interface (POSIX). Shell and Utilities

CDM 2007	The Construction (Design and Management) Regulations 2007

3.2 Version Control

3.2.1 The Service Provider shall use a Version Control Process and Version Control System Approved by TTL.

3.2.2 The Service Provider shall store and maintain all files necessary to build the Service Systems, (or any part thereof) any sub-component of the Service Systems, within the Version Control System. This shall include:

a) the Design Documents;
b) Source Code;
c) Configuration Files;
d) Build Files;
e) Application Libraries; and
f) the development Environment.

4 QUALITY ASSURANCE, RISK MANAGEMENT AND CHANGE CONTROL

4.1 General

4.1.1 The Service Provider shall nominate a Quality Controller to be Approved by TTL.

4.1.2 The Service Provider shall nominate and enforce a Quality Assurance methodology to be Approved by TTL.

4.1.3 The Service Provider shall nominate and enforce a risk management methodology to be Approved by TTL.

4.1.4 The Service Provider shall develop a Quality Plan, in accordance with Schedule 3 (*Milestones and Deliverables*), that:

a) ensures that all aspects of the Services are the subject of quality management systems; and
b) is consistent with ISO 9001:2005 or any standard which is generally recognised as being equivalent to it.

4.1.5 The Service Provider shall obtain TTL's Approval of the Quality Plan prior to implementing it.

4.1.6 The Service Provider shall provide the Services in compliance with the Quality Plan.

4.1.7 The Service Provider shall agree and implement any Changes to the Quality Plan in accordance with the Change Control Request Procedure.

4.1.8 TTL may carry out audits of the Service Provider’s quality management systems (including the Quality Plan and any quality manuals and procedures) from time to time. TTL shall also reserve the right to audit the Service Provider’s design or operational capability together with but not limited to all associated Documentation.

5 TESTING

5.1 General

5.1.1 The Service Provider shall carry conduct Testing in accordance with:

a) Schedule 4 (*Testing Regime*);
b) Good Industry Practice; and
c) Data Protection Legislation.

5.1.2 The Service Provider shall ensure that all Data used during Testing is stored, processed and deleted securely in accordance with appendix 1: *(Information Compliance Processes)*.

5.2 Test Environments

5.2.1 The Service Provider shall provide suitable test Environments for development and Testing of the Service Systems during the Operational Phase.

5.2.2 The Service Provider shall provide a test system and links to the Service Systems, together with associated test/acceptance functions.

5.2.3 The Service Provider shall ensure that at least one (1) of the test Environments is representative of the operational Environment so that realistic Tests of performance and functionality can be performed during the Operational Phase.

6 SECURITY

6.1 Security Policy and Management

6.1.1 The Service Provider shall provide and implement a Security Plan in accordance with:

a) Schedule 14 (*Security Policy*); and
b) prevailing industry recognised security standards.

6.1.2 The Service Provider shall commission, at no cost to TTL, an independent external security audit at least once per year to review and check compliance with the Security Policy. The external auditor shall be agreed with TTL prior to such audit, which shall include the execution of independent external penetration Testing and report generation.

6.1.3 The Service Provider shall nominate a Security Manager to be Approved by TTL.

6.1.4 The Security Manager shall provide a security management service to monitor, enforce, maintain and enhance all aspects of the Security Policy.

6.1.5 The Service Provider shall allocate appropriately qualified resources to enforce the Security Policy.

6.1.6 The Service Provider shall provide security reports detailing any security breaches to TTL at periodic intervals to be agreed with and on request by TTL.

6.1.7 The Service Provider shall ensure that the Service System provides within forty eight (48) hours of the resolution of a Security Incident, a detailed report to TTL, which includes details of:

a) the Security Incident;
b) the causes and consequences of the Security Incident;
c) the actions taken to handle the Security Incident and timeframes applicable to resolution of the Security Incident; and
d) actions to prevent recurrence of the Security Incident.

6.1.8 The Service Provider shall ensure that all networks provided by the Service Provider are secure and protected from unauthorised access.

6.1.9 The Service Provider shall ensure that all transfers of Data are secure including but not limited to those using removable media.

6.2 Facilities and Building Security

6.2.1 The Service Provider shall ensure that User access into secure areas shall be automatically recorded and logged. The Service Provider shall retain the logs in accordance with Appendix 2 (*Data Retention*).

6.2.2 The Service Provider shall deny physical access to its Service Systems to individuals without appropriate and specific authorisation, to be agreed with TTL.

6.2.3 The Service Provider shall ensure that the layout and furnishings of secure areas minimise opportunities for concealment of items or persons.

6.2.4 The Service Provider shall ensure that all networks provided by the Service Provider are secure and protected from unauthorised access.

6.2.5 The Service Provider shall make any relevant security checks of potential Service Provider Personnel prior to the commencement of employment in any part of the Services. The depth of such checks shall reflect the roles and responsibilities to which Personnel will be assigned and shall be agreed with TTL.

6.2.6 The Service Provider shall provide training for all Service Provider Personnel providing any aspects of the Services in security processes and procedures at their induction and shall provide on-going training to ensure that all of its Service Provider Personnel are fully aware of security requirements and are able to put these into practice.

6.3 Anti-Virus Scanning and Protection

6.3.1 The Service Provider shall maintain the latest versions of leading industry protection Software to address risks of Virus', firewalls or unauthorised usage of the Service Systems.

6.3.2 The Service Provider shall ensure that protection Software updates are implemented on at least a daily basis to ensure the maximum possible protection is provided for Data stored on behalf of TTL.

6.4 Security Clearance

6.4.1 The Service Provider shall develop, maintain and apply security clearance processes and procedures for Service Provider Personnel and Third Parties attending the premises in accordance with Good Industry Practice.

6.4.2 The Service Provider shall apply security clearance procedures to all Service Provider Personnel and other visiting personnel

6.5 Access to Systems and Data

6.5.1 The Service Provider shall ensure that the identity of all Users is securely authenticated before using any Service System.

6.5.2 The Service Provider shall ensure that access to and use of all Service Systems is subject to appropriate authorisation in accordance with Schedule 14 (*Security Policy*) and Good Industry Practice.

6.5.3 The Service Provider shall ensure that the Services Systems prevent unauthorised Users and Service Provider Personnel from making changes to configurations and Parameters.

6.5.4 The Service Provider shall ensure that all of the Service Systems restrict Internet access; for its Service Provider Personnel employed in the provision of the Services and at the Premises used for the provision of the Services, except where required for the provision of the Services and/or on an individual basis.

6.5.5 Where the Service Provider engages in services with clients other than TTL, the Service Provider shall take all relevant steps to ensure that there is no accidental or malicious interference with the Services.

6.5.6 The Service Provider shall allocate permissions to its Service Provider Personnel at its own risk.

6.5.7 The Service Provider shall immediately disable a User's logon and access rights when a User ceases to be a member of the Service Provider Personnel or TTL Personnel.

6.5.8 The Service Provider shall provide on-site read-only access to all Data to nominated TTL Personnel or authorised agents.

6.5.9 In accordance with Appendix 2 (*Data Protection*), the Service Provider shall securely delete Data at the expiry of its retention period by the following means such that the Data cannot be accessed by any User, intruder or member of the public:

a) Data held on paper shall be securely shredded;
b) Data held on fixed hard disks shall be deleted using tested deletion scripts; and
c) Data held on any removable medium such as optical disks, floppy disks and tapes shall be securely destroyed such that the Data cannot be accessed by any reasonable means.

6.5.10 The Service Provider shall carry out a security audit on all of its Service Systems in accordance with Good Industry Practice.

6.5.11 Where fixed disks holding Data are to be retired or re-used, the Service Provider shall re-format the disks such that the Data cannot be accessed by any reasonable means.

6.5.12 In the event that a member of its Service Provider Personnel is dismissed, the Service Provider shall ensure that all security devices and access cards are taken from the individual immediately.

6.6 Audit Trails

6.6.1 The Service Provider shall maintain a System Log and User Audit Log for all transactions and all other actions completed on the Service Systems with details of the individual User or Service System process responsible for the transaction or action, including:

a) access to or mutation of specific subsets of the Data;
b) User authentication requests; and
c) execution of specific Service Systems.

6.6.2 The Service Provider shall provide all System Logs and User Audit Logs to support the list as described in requirement 6.6.1 above to TTL in an electronic format upon request.

6.6.3 The Service Provider shall maintain an audit trail of all messages sent and received between the Central System and Docking Stations, including messages relating to:
a) Hire of Bicycles including Bicycle Release and Dock of Bicycles;
b) payment transactions;
c) configuration Parameters;
d) Incidents reported; and
e) SmartCard identification.

7 INCIDENT MANAGEMENT AND RESOLUTION

7.1 General

7.1.1 The Service Provider shall use an escalation process for Incident Management provided by the Implementation Service Provider.

7.1.2 The Service Provider shall be responsible for the resolution of all Incidents.

7.1.3 All Incidents relating to the Services shall be recorded in the Incident Log by the Service Provider within five (5) minutes of being raised.

7.1.4 The Service Provider shall be responsible for working with Interested Parties, Other Service Providers and Third Parties, in accordance with Clause 16 (*Co-operation with TTL, Interested Parties and Other Service Providers and Third Parties*), to resolve Incidents where the failure may lie outside the scope of the Services or where a failure may impact an Other Service Provider's or a Third Party's operations.

7.1.5 The Service Provider shall define and implement escalation procedures for resolution of Incidents where these are, or are suspected to be, related to the TTL Systems and Third Party Systems or the Interfaces to them.

7.1.6 The Service System shall provide a Weekly Incident report to TTL prior to the meeting of the Contract Management Board, which shall include:
a) a description of all Incidents arising in the previous Week, together with their classification and their Severity Level in the case of Service Issues, Errors and Security Incidents;
b) a status report on all open Incidents; and

c) a description of the resolution of all Incidents closed during the previous Week.

7.1.7 Where an Incident is considered by the Service Provider to result from a failure outside the scope of the Services, the Service Provider shall provide supporting evidence upon making the claim, to the satisfaction of TTL, to the party considered responsible and to TTL. Until such agreement is reached, the responsibility of the Incident shall remain with the Service Provider.

7.1.8 The Service Provider shall bear the cost of any work undertaken by a Third Party in order to resolve an Incident within the scope of the Services where the Service Provider has failed to perform this work itself.

7.1.9 The Service Provider shall provide and document the processes, mechanisms and tools to be used to manage all Incidents, including the interactions with TTL in Incident resolution, as set out in Schedule 10 (*Contract Management and Reporting*).

7.1.10 The Service Provider shall document, maintain and apply procedures for management and resolution of Incidents including the reporting of Incidents by Third Parties and liaison with Interested Parties, Other Service Providers, Sub-Contractors and other Third Parties. The Service Provider shall provide these procedures to TTL for Approval.

7.1.11 The Service Provider will nominate an Incident Resolution & Problem Manager for Incidents in relation to the Services.

7.1.12 The Service Provider shall log the corrective actions taken to resolve Incidents in the Incident Log.

7.1.13 The Service Provider shall raise any Incidents resulting in a loss of Services as Severity 1.

7.1.14 The Service Provider shall raise any Incidents resulting from loss of redundancy within the Service Systems as Severity 2.

7.1.15 The Service Provider shall resolve, rectify and close Errors, Service Issues and Security Incidents within the following timescales according to their Severity Level:

a) Severity 1 – four (4) hours;
b) Severity 2 – twenty four (24) hours;
c) Severity 3 – ten (10) days;
d) Severity 4 – next scheduled Software Release in the case of Errors or as agreed with TTL in the case of Service Issues; and
e) Severity 5 – next convenient Software Release in the case of Errors or as agreed with TTL in the case of Service Issues.

7.1.16 The Service Provider shall only close an Incident when:

a) in the case of Errors, corrective action has been completed and tested according to the agreed maintenance procedures and the agreed Test Strategy, and released into production systems;

b) in the case of Service Issues, the Service Issue has been resolved to TTL's satisfaction or it is agreed with TTL that no corrective action is required; or

c) the resolution of the Incident is agreed by TTL to be a Change and recorded in the Change Log.

7.1.17 An Incident is considered to be resolved and closed when corrective action has been completed, Tested and the Incident properly recorded as closed in the Incident Log by the Service Provider with the express written agreement of TTL. This agreement may be given retrospectively. The time taken to resolve and close each Incident is from the earliest of the time of:

a) Detection of such Incident by the Service Provider or any of its Sub-Contractors or any Service Provider Personnel, as the case may be;

b) notification of such Incident being provided to the Service Provider or any of its Sub-Contractors or any Service Provider Personnel, as the case may be; or

c) any of the applications or Services becoming unavailable as a result of such Incident; to the time when the Incident is resolved and closed.

7.1.18 The Service Provider shall analyse the Incident Log to identify common recurring Service Issues, Errors, Security Incidents and Performance Indicator Incidents and take action to prevent their re-occurrence.

7.1.19 Where appropriate, the Service Provider shall schedule preventative maintenance to address such Errors, Service Issues, Security Incidents and Performance Indicator Incidents as part of the regular maintenance plan.

7.1.20 The Service Provider shall progress Incidents classified as Changes in accordance with the Change Control Request Procedure and shall close these Incidents in the Incident Log.

7.1.21 The Service Provider shall classify Errors, Service Issues and Security Incidents by the severity of the impact of the Error, Service Issue or Security Incident on provision of the Services. Severity Levels for Errors, Service Issues and Security Incidents are given in Schedule 1 (*Definitions*).

7.1.22 The Service Provider shall report any Severity 1 or Severity 2 Incidents to TTL within ten (10) minutes of the time at which the Incident occurs via the agreed Communication Plan.

7.1.23 The Service Provider shall re-evaluate any Incident jointly with TTL at TTL's request. In the event of dispute over the classification of an Incident or the assignment of a Severity Level, it shall be referred to the next meeting of the Contract Management Board. If agreement cannot be reached at the Contract Management Board meeting, then the Service Provider shall follow TTL's instructions on the classification of the Incident and/or assignment of a Severity Level.

7.1.24 Where the Service Provider is unable to resolve an Incident within the resolution time periods specified for its Severity Level, the Service Provider shall inform TTL in writing and propose the actions to be taken to resolve the Incident.

8 DOCUMENTATION

8.1 General

8.1.1 The Service Provider shall provide, for review by TTL, all Documentation described in:

a) Schedule 3 (*Milestones and Deliverables*);
b) Schedule 4 (*Testing Regime*); and
c) all other Documentation requested by TTL.

8.1.2 The Service Provider shall agree a schedule for the provision of all Documentation for review by TTL. The schedule shall:

a) include adequate review time and assume no less than two (2) revisions of each Document; and
b) avoid the simultaneous release of Documents to achieve a practical review workload.

8.1.3 The Service Provider shall maintain and store all Documentation under Version Control according to Good Industry Practice.

8.1.4 The Service Provider shall address any review actions or comments raised by TTL Personnel within a reasonable timescale to be agreed with TTL unless explicitly stated in this Agreement. Where agreement by both Parties to Documentation is required, TTL reserves the right to withhold its agreement in the event that review actions or comments are not addressed to TTL's satisfaction.

8.1.5 Subject to paragraph 8.1.6 below, the Service Provider shall provide Documentation to TTL in both electronic and paper format, as requested by TTL.

8.1.6 The Service Provider shall provide electronic copies of Documentation in either:

a) Microsoft Office (Word, Visio, Excel or PowerPoint); or
b) PDF format,

as requested by TTL.

8.2 Operational Documentation

8.2.1 The Service Provider shall provide Operational Processes and Procedures Documentation for all tasks to be undertaken by the Service Provider or its Sub-Contractors or agents from the Operational Commencement Date. This shall, subject to any other items listed in this Agreement or referenced herein, comprise:

a) procedures for operation of the Services, LCHS Assets and Service Systems; and
b) procedures for maintenance and support of the Services, LCHS Assets and Service Systems.

These Documents shall make reference to the Systems Documentation as required and shall been sent to TTL for Approval in accordance with Schedule 3 (*Milestones and Deliverables*).

9 REPORTING, PERFORMANCE MANAGEMENT AND AUDIT

9.1 General

9.1.1 The Service Provider shall:

a) monitor the London Cycle Hire Scheme's operational performance;
b) produce Operational Reports as specified below; and
c) produce Performance Indicator reporting to TTL as specified in Schedule 5 (*Service Level Agreement*).

9.1.2 The Service Provider shall provide to Performance Indicator Reports on a Monthly basis (where performance is measured on a daily basis these reports must be delivered to TTL Monthly and must include a daily breakdown).

9.1.3 The Service Provider shall provide Ad Hoc Reports to TTL.

9.1.4 The Service Provider shall ensure that all Reports are securely transferred via file transfer protocol.

9.1.5 The Service Provider shall provide to TTL regular Operational Reports in a format to be agreed with TTL, including the information required by Schedule 5 (*Service Level Agreement*) and the following:

a) Contact Centre report (ongoing Operational Report delivered Weekly with a daily breakdown) including:

I. total number of calls offered;
II. total number of calls handled;
III. total Number calls answered in less than thirty (30) seconds;
IV. total number of calls abandoned;
V. total number of calls abandoned in equal to or less than twenty (20) seconds;
VI. average queue time of calls (in seconds); and
VII. average talk time of calls (in seconds).

b) Enquiries and Complaints (ongoing Operational Report delivered Weekly with a daily breakdown) including:

I. total number of Enquiries received (broken down by contact channel and Enquiry category);
II. total number of Complaints received (broken down by channel and Complaint category);
III. total number of disputes per Week;
IV. total number of disputes found in the Customers favour;
V. the length of time each dispute took to resolve;

c) Registrations (ongoing Operational Report delivered Weekly with a daily breakdown)

I. total number of Customers registered on each Subscription category;
II. total number of Registrations per contact channel;
III. total number of Registrations rejected and reason for rejection; and
IV. total number of Registration closed or suspended and the reason for the closure or suspension.

d) Subscriptions (ongoing Operational Report delivered Weekly with a daily breakdown)

I. total number of Subscriptions (broken down by contact channel and Subscription category);
II. total in each Subscription status for example number that are new, approved, active, expired, renewals;
III. total number of Non-Registered Customers purchasing Subscriptions at the Terminal (broken down by Subscription category); and
IV. total number of Customers purchasing two (2) or more Subscriptions per day.

e) Bicycle Hired (ongoing Operational Report delivered Weekly with a daily breakdown)

I. total number of Bicycles Hired;
II. average duration of Bicycle journeys;
III. average number of times each Bicycle is Hired;

IV. average number of Bicycles Hired by each Customer

V. average number of Bicycles Hired at each Priority 1 Docking Station during Peak Hours;

VI. average number of Bicycles Hired at each Priority 2 Docking Station during Peak Hours;

VII. average number of Bicycles Hired at each Priority 1 Docking Station during Off-Peak Hours;

VIII. average number of Bicycles Hired at each Priority 2 Docking Station during Off-Peak Hours;

IX. average number of Bicycle Docks at each Priority 1 Docking Station during Peak Hours;

X. average number of Bicycle Docks at each Priority 2 Docking Station during Peak Hours;

XI. average number of Bicycle Docks at each Priority 1 Docking Station during Off-Peak Hours;

XII. average number of Bicycle Docks at each Priority 2 Docking Station during Off-Peak Hours;

XIII. total number of Bicycles Hired by Customers using SmartCards;

XIV. total number of Bicycles reported as stolen per day;

XV. most frequent Bicycle Hire routes (determined by Docking Station where Bicycles are Hired and then subsequently Dock);

XVI. total number of collision/accidents reported by Customers; and

XVII. total number of Customers that Hire more the one (1) Bicycle simultaneously against one (1) Payment Card.

f) Charges and Payments (ongoing Operational Report delivered Weekly with a daily breakdown unless otherwise stated)

I. total amount of Bicycle Hire charges received;

II. total number of Customers who exceed their Threshold Value;

III. total number of Customers who incur late return fees;

IV. total amount of late return fees received;

V. total amount of rejected Payments against Credit/Debit cards or direct debits that is not collectable per Month;

VI. total number of Customers who pay by each Payment method per Month;

VII. total amount of Refunds given and the reason for the Refund;

VIII. total number of statements printed at Terminals; and

IX. total number of Bicycle return receipts printed at Terminals.

g) Bicycle availability (ongoing Operational Report delivered Weekly with a daily breakdown)

I. Total number of Bicycles available for use by Customers at XX:XX am each calendar day;
II. total number of replacement Bicycles held in stock;
III. total number of Bicycles missing or stolen;
IV. total number of missing Bicycles returned;
V. total number of Bicycles Damaged;
VI. total number of Bicycles repaired at Docking Stations;
VII. total number of Bicycles taken out of service for repair; and
VIII. total number of replacement Bicycles taken out of stock and made available for Customer Hire.

h) average life of each Bicycle.

i) Docking Station and Bicycle vandalism (ongoing Operational Report delivered Weekly with a daily breakdown) including:
I. total number of occasions when a Terminal has be vandalised (including a detailed description of the type of graffiti found);
II. total number of occasions when a Bicycle has be vandalised (including a detailed description of the type of graffiti found); and
III. total number of occasions when a Docking Point has be vandalised (including a detailed description of the type of graffiti found).

j) Installation of Docking Stations during the Operational Phase (ongoing Operational Report delivered Weekly with a daily breakdown)
I. number and location of all Docking stations installed;
II. number and location of all Docking stations tested;
III. number and location of all Docking stations installed and signed off by TTL;
IV. number and location of Docking Stations in progress of being installed;
V. number and location of Docking Stations being tested;
VI. number and location of Docking Station installations awaiting sign off by TTL; and
VII. number and location of Docking Stations where installation is not started, with estimated start date.

9.1.6 The Service Provider shall ensure that the Operational Reports can be delivered in a format (to be agreed by TTL) whereby TTL have the ability to extract the raw Data from the report and present the Data in another format within other TTL reports.

9.1.7 The Service Provider shall ensure that frequency and format of Operational Reports and Performance Indicator Reports can be changed by ensuring that such reports are Parameterised.

9.1.8 The Service Provider shall provide functional specifications for each of the agreed Operational Reports. These specifications shall be Approved by TTL and include:

a) the source of the Data;
b) the script used to obtain the Data;
c) any exclusion of Data;
d) the transformation applied to the Data;
e) the presentation of the Data;
f) the process and tools used to generate the report; and
g) any input Parameters to the report and report frequency if generated automatically.

9.1.9 The Service Provider shall provide the Ad Hoc Reports and Data in a format specified by TTL at the time of the request.

9.1.10 The Service Provider shall provide to TTL all Ad Hoc Reports and Data within forty-eight (48) hours of the date and time of each request.

9.1.11 TTL reserves the right to request a copy of all operational Data held by the Service Provider in either an electronic or paper format.

9.2 Performance Indicator Reporting

9.2.1 The Service Provider shall provide all Performance Indicator Reports and associated raw Data, in a format to be agreed with TTL, on a Parameterised Monthly basis for the previous Month’s performance at a time and date to be agreed with TTL.

9.2.2 The Service Provider shall ensure that the raw Data used to measure and compile all Performance Indicators is made available to TTL at the time of providing the Performance Indicator Report.

9.2.3 The Service Provider shall provide functional specifications for each of the agreed Performance Indicator Reports. These specifications shall be Approved by TTL and include:

a) the source of the Data;
b) the script used to obtain the Data;
c) any exclusion of Data;
d) the transformation applied to the Data;
e) the presentation of the Data;
f) the process and tools used to generate the report; and
g) any input Parameters to the report and report frequency if generated automatically.

9.3 Audit

9.3.1 The Service Provider shall upon request by TTL, allow TTL full access to conduct an audit in accordance with Clause 42 (*Audit and Inspection*), including the following areas:

a) the method of report production and any Data transformations;
b) queries and conditions used for Data extraction; and
c) reconciliation of source to target Data.

9.3.2 The Service Provider shall provide full co-operation with the audit including access to all relevant Documentation and Service Provider Personnel.

9.3.3 The Service Provider shall ensure that it implements and provides details of any audit methodology which it applies to monitor and control all business processes.

9.3.4 The Service Provider shall allow the monitoring and controlling methodology to be subject to continued review throughout the Term.

10 MANAGEMENT SERVICES

10.1 General

The Service Provider shall provide Management Services in accordance with Schedule 20 (*Management Service*).