SCHEDULE 4

Testing Regime

1. __Introduction__

1.1 This Schedule 4 sets out the procedures to be followed by the Service Provider in respect of testing:

(A) the System; and

(B) the Services.

1.2 The Service Provider shall Test all elements of the:

(A) the System; and

(B) the Services,

in accordance with the relevant Test Strategy, Test plans and Test specifications in order to demonstrate that they meet the requirements and comply with the design documents.

2. __Test Strategy__

2.1 The Service Provider shall in accordance with the Implementation Plan and this Schedule 4 develop a draft test strategy for the Testing in support of the System, and shall submit such draft test strategy to TfL for Approval (such Approved test strategy being the ("**Test Strategy**").

2.2 The Test Strategy shall include, but shall not be limited to, the following:

(A) the requirements, objectives and scope of all Testing;

(B) a description of the approach to Testing, including:

(1) a description of all testing methodologies to be employed;

(2) a rationale for the use of these testing methodologies in the context of the overall development methodologies and lifecycles to be employed;

(3) a description of how the scope and depth of the testing of the constituent parts of the System and Services under Test will be matched to the design and development complexity of those constituent parts; and

(4) a description of how consistency of testing will be achieved across the use of the testing methodologies employed to ensure adequate testing across all constituent parts of the System and Services under Test, including but not limited to, demonstrating end-to-end financial and evidential integrity;

(C) a description of how Testing will be grouped for organisational, management and reporting purposes into a more granular format (including, for example, test levels, phases, increments and test cycles) including, but not limited to:

(1)   a high level plan for the Testing of the System and Services under Test, including the scheduling of all Tests to be completed consistent with the Implementation Plan(s) and Schedule 3 (*Milestones and Deliverables*);

(2)   a description of dependencies between different elements of the high level plan, including dependencies between proposed test levels, phases, increments and cycles; and

(3)   the identification of which of those elements will be associated for planning and reporting purposes with the generation of Test Plans as envisaged under paragraph 3 (*Test Plans*) of this Schedule prior to their commencement and will conclude with the generation of Final Test Reports as envisaged under paragraph 5.6 of this Schedule, so as to ensure the resulting set of Test plans and Test reports cover all of the System and Services under Test;

(D)   a description of how the approach and structuring of the Testing will ensure that:

(1)   all the required aspects of the test coverage defined in Annex 1 (*Testing Methodology: Implementation Phase*) will be addressed; and

(2)   any aspects of the test coverage defined in Annex 1 (*Testing Methodology: Implementation Phase*) that the Service Provider believes are not required are identified;

(E)   for each Milestone, descriptions of the anticipated processes relating to Testing for achieving Acceptance of that Milestone including the performance of the Service Provider's obligations in respect of Test witnessing, Test reports, Incident management and the business process scenarios to be used in determining whether the test criteria have been met;

(F)   any dependencies affecting the Testing, including reliance on Third Parties;

(G)   any assumptions made by the Service Provider that may have an impact upon Testing;

(H)   the regular testing of all aspects of the Business Continuity Plan (including without limitation the Business Continuity services and the Business Continuity Infrastructure) in accordance with Schedule 25 (*Business Continuity*) as required by paragraph 3 (*Testing*) of Schedule 25 (*Business Continuity*);

(I)   any perceived risks to Testing together with the impact of such risks and proposed methods of mitigation;

(J)   an outline of the resource requirements, including personnel, personnel training, Test environments and Testing tools and how they will be used at each stage of the Testing;

(K)   the roles and responsibilities of all those involved with the Testing programme, including TfL Personnel or the Service Provider's Personnel and/or Third Parties personnel where applicable;

(L)   the full address of the location where all Testing is to be performed;

(M)   the sources and the mechanisms for specification, creation management and secure destruction of Test Data, in compliance with Privacy Legislation where applicable; and

(N)   the quality management tools and processes to be used in the Testing including:

(1)   the standards to be applied to Testing;

(2)   test design techniques to be employed during the Testing;

(3)   requirement traceability mechanisms;

(4)   the Incident management process;

(5)   Configuration Management;

(6)   Release Management;

(7)   Test results capture, logging and tracking;

(8)   Test progress reports; and

(9)   Final Test Reports.

3.   **Test Plans**

3.1   The Service Provider shall in accordance with paragraph 7 (*Timing Requirements*) and paragraph 3 (*Test Plans*) of this Schedule develop a Test plan or Test plans for all testing required in support of:

(A)   the development of the System which:

(1)   is consistent with the Test Strategy;

(2)   meets the relevant requirements set out in Annex 1 (*Testing Methodology: Implementation Phase*) to this Schedule 4;

(B)   each Change and the resolution of each Incident addressed by the Service Provider that might arise from time to time impacting on the live operation of the:

(1)   System; and

(2)   Services.

and shall submit each such Test plan to TfL for Assurance unless, in the case of Change and Incident Testing only, TfL have specifically agreed in advance in writing that such a Test plan need not be so submitted.

3.2   The Service Provider shall re-submit to TfL any Test plan which has been rejected by TfL with five (5) Business Days following the date that TfL issued its rejection of the relevant Test plan.

3.3   Each Test plan shall include, but shall not be limited to:

(A)   an overview of the specific Testing approach for the Release and applicable Testing covered by the Test plan;

(B)   the scope of the Testing for the version or Release covered, including without limitation a description of the Software, the System, constituent parts or functional areas of the System under test;

(C)   any specific Testing requirements or objectives for the Release and applicable Testing covered by the Test plan, including any Change Control Requests addressed;

(D)   a detailed process for Testing of Software versions and Releases covered by the Test plan, including but not limited to all required Regression Testing;

(E)   the identification and details of the Test environment(s) to be used in carrying out the Testing covered by the Test plan;

(F)   the detailed entry and exit criteria applicable to the Testing covered by the Test plan;

(G)   any specific dependencies, pre-requisites, assumptions and risks related to Testing any Software or System version or Release;

(H)   identification of the test scripts to be executed;

(I)   a detailed schedule for the Testing including the frequency of delivery of any and all required Test progress reports;

(J)   named roles and responsibilities for all those involved with Testing; and

(K)   a description of the Test Data to be used for Testing; and

(L)   a description of where the Test activities described in the Test plan represent a deviation from the earlier Test Strategy (subject always to the requirement that such deviation must be permitted in accordance with paragraph 6 (*Deviations from Testing Documents*) of this Schedule 4 together with the reasons and rationale for the deviation.

4.   **Test Specifications**

4.1   For each such Test plan required by paragraph 3.1 of this Schedule 4, the Service Provider shall in accordance with the paragraph 7 (*Timing Requirements*) of this Schedule 4 develop a Test specification or specifications for all Tests in each such Test plan which:

(A)   are consistent with the Test Strategy;

(B)   are consistent with the Test plan; and

(C)   are in accordance with the applicable Milestones and Milestone dates;

and shall submit each such Test specification to TfL for Assurance unless, in the case of Change and Incident Testing only, TfL have specifically indicated that such a Test specification need not be submitted for Assurance.

4.2   The Service Provider shall re-submit to TfL any Test specification(s) which has been rejected by TfL within five (5) Business Days following the date that TfL issued its rejection of the relevant Test specification.

4.3   Each Test specification shall include, but shall not be limited to:

(A)   the test criteria with traceability back to the relevant requirements, through the design documents and any other documents relevant to the Testing;

(B)   a set of test scenarios (including without limitation business process scenarios (where applicable)) and test cases designed to exercise all the test criteria identified within the Test specification, each with a reference to the test criteria covered by the test scenario;

(C)   a set of test scripts corresponding to the test scenarios and test cases describing the purpose of the Test, the Data requirements for the Test, any pre-requisites for the Test, the actions to be taken during the Test, and the expected results for each step or action of the Test against which success or failure of the Test shall be judged; and

(D)   a description of where the Test specification represents a deviation from the earlier Test plan (subject always to the requirement that such deviation must be permitted in accordance with paragraph 6 (*Deviations from Testing Documents*) of this Schedule 4 together with the reasons and rationale for the deviation.

5.   **Test Reporting**

5.1   During periods of Test execution covered by a Test plan as required by paragraph 3 (*Test Plans)* of this Schedule 4, the Service Provider shall submit Test progress reports to TfL for Assurance with the frequency detailed in that Test plan and in accordance with paragraph 5.5 to this Schedule 4.

5.2   On completion of any period of Test execution covered by a Test plan as required by paragraph 3 (*Test Plans)* of this Schedule 4, the Service Provider shall submit a Final Test Report to TfL for:

(A)   Acceptance where the test report is being submitted in respect of Milestone acceptance criteria; or

(B)   Assurance in relation to all other Final Test Reports;

in accordance with paragraph 5.6 of this Schedule 4 and paragraph 7 (*Timing Requirements*) of this Schedule 4.

5.3   The Service Provider agrees that, notwithstanding anything to the contrary in this Agreement, TfL may share Test progress reports and Final Test Reports in form or substance with any Third Party for any purpose in respect of this Agreement and/or the Services.

5.4   Unless otherwise agreed in advance by TfL in writing, Test progress reports and Final Test Reports shall not include references to Test Data which includes Personal Data.

Test Progress Reports

5.5   The Service Provider shall ensure that all Test progress reports are in the format set out in the relevant Test plan and include, as a minimum, the following information:

(A)   a detailed table which shall include an entry for each test script, with each such entry including:

(1)   the name of the test script;

(2)   a unique identifier for the test script sufficient to allow cross-referencing against other Test Documents;

(3)   the current status of test script;

(4)   the identity of any and all Incidents associated with the execution of that test script;

(5)   any observations associated with the execution of that test script; and

(6)   for a blocked test script, the dependencies and pre-requisites for future execution;

(B)   a detailed table setting out the status of any Incidents identified which shall include an entry for each Incident revealed during the performance of the relevant Testing, including Incidents which have been remedied by the Service Provider, with each such entry including as a minimum:

(1)   the name of the Incident;

(2)   a unique identifier for the Incident sufficient to allow cross-referencing against other Test Documents;

(3)   a concise description of the Incident;

(4)   the current status of the Incident;

(5)   the identity of the test script(s) associated with the Incident;

(6)   the Severity Level of the Incident;

(7)   dates relevant to the observation, investigation and resolution of the Incident; and;

(8)   the name of person responsible for progressing the investigation of the Incident;

(C)   a table detailing any proposed changes to the relevant Test plan(s) or Test specification(s);

(D)   a detailed graphical and narrative analysis of the progress of the relevant Testing; and

(E)   a summary of the narrative given pursuant to paragraph 5.5(D) above including a short narrative of progress since the last Test progress report and a description of progress anticipated by the next Test progress report.

Final Test Reports

5.6   The Service Provider shall ensure that all Final Test Reports are in the format set out in the relevant Test plan and, as a minimum, include:

(A)   any deviations from the Test Strategy or relevant Test plan or Test specification(s) (subject always to paragraph 3 (*Test Plans*) above);

(B)   the results of that Testing (to the extent that such results can be reported on);

(C)   if the testing failed in any way, the extent and cause of the failure;

(D)   the detail of any outstanding Incidents, including references to the Incident log and the associated Severity Level;

(E)   a description of any workarounds used during Testing, the relationship of such workarounds to specific Tests, Incidents observed or raised, and their impact including their use to progress the testing or any proposal for their operational use;

(F)   summary metrics on Incidents raised during the Testing;

(G)   Remedy Plan in respect of all outstanding Incidents and the removal of any associated workarounds; and

(H)   a description of any risks to the Implementation phase or operation of the System and/or Services raised during the Testing.

6.   **Deviations from Testing Documents**

6.1   Subject to TfL's Assurance rights, the Service Provider's Testing shall not deviate from previously Approved or Assured Testing Documents unless:

(A)   for deviations from the Approved Test Strategy:

(1)   an update to that Test Strategy reflecting such deviation has first been Approved by TfL; or

(2)   if agreed in advance by TfL in writing, the Service Provider fully details each such deviation (together with a written explanation detailing the reason for each such deviation) in the relevant Test plans(s) submitted to TfL for Assurance;

(B)   for deviations from an Assured Test plan:

        (1)   the Service Provider submits in advance to TfL for Assurance an update to that Test plan reflecting each such deviation; or

        (2)   if agreed in advance by TfL in writing, the Service Provider fully details each such deviation (together with a written explanation detailing the reason for each such deviation) in the relevant Test specification(s) submitted to TfL for Assurance; and

(C)   for deviations from an Assured Test specification:

        (1)   the Service Provider submits in advance to TfL for Assurance an update to that Test specification reflecting each such deviation; or

        (2)   if agreed in advance by TfL in writing, the relevant Final Test Report or Final Test Reports submitted by the Service Provider to TfL for:

                (a)   Acceptance where the Final Test Report is being submitted in respect of Milestone acceptance criteria; or

                (b)   Assurance in relation to all other Final Test Report;

fully details each such deviation (together with a written explanation detailing the reason for each such deviation).

7. **Timing Requirements**

7.1   The Service Provider shall:

(A)   give TfL at least ten (10) Business Days written notice of any Testing to be undertaken by the Service Provider;

(B)   deliver all relevant Test plans and Test specifications for Assurance, no less than ten (10) Business Days prior to the relevant Test;

(C)   complete and deliver any required Test progress reports in accordance with the relevant Test plan;

(D)   complete and deliver each Final Test Report in accordance with the relevant Test plan, the Implementation Plan and in any event at least five (5) Business Days prior to any Milestone date associated with successful completion of the relevant Test;

(E)   ensure that all relevant updates to the Incident log are completed no more than five (5) Business Days following completion of the relevant Testing; and

(F)   resolve all Incidents arising as a result of or identified during Testing at its own cost, in accordance with the provisions of paragraph 9 (*Incident Reporting*) of Schedule 10 (*Contract Management and Reporting*).

7.2   In regard to each period of Regular Business Continuity Testing the Service Provider shall, unless otherwise agreed in writing with TfL:

(A)   perform the testing in accordance with the agreed Business Continuity Test Schedule as required by in paragraph 2 (*Business Continuity Plan and Business Continuity Test Schedule*) of Schedule 25 (*Business Continuity*); and

(B)   deliver all relevant Test plans and Test specifications for Assurance, no less than ten (10) Business Days prior to the relevant Test;

(C)   complete and deliver any required Test progress reports in accordance with the relevant Test plan;

(D)   complete and deliver each Final Test Report in accordance with the relevant Test plan;

(E)   ensure that all relevant updates to the Incident log are completed no more than five (5) Business Days following completion of the relevant Testing; and

(F)   resolve all Incidents arising as a result of or identified during Testing at its own cost, in accordance with the provisions of paragraph 9 (*Incident Reporting*) of Schedule 10 (*Contract Management and Reporting*).

8.   **Test Witnessing**

8.1   TfL may, at its sole discretion, require its employees, agents or sub-contractors and any Third Party nominated by TfL, to witness any of the Testing carried out by the Service Provider or the Service Provider's Sub-Contractor(s) in relation to:

(A)   the development of the System;

(B)   the implementation of any Change that might arise from time to time; or

(C)   the resolution of any Incident that might arise from time to time;

and the Service Provider shall comply with such request.

8.2   In relation to all Test witnessing, the Service Provider shall:

(A)   provide such access, facilities, Information, Data, explanation, Documentation and assistance to TfL and any Third Party nominated by TfL in order for TfL (and/or that Third Party) to prepare for and participate in such Test witnessing as TfL may require;

(B)   follow TfL's reasonable instructions in relation to the form of Test witnessing and the way in which Test witnessing is to be carried out, including without limitation:

(1)   TfL witnessing the execution of the Testing being carried out by the Service Provider;

(2)   TfL witnessing a solution demonstration; and

(3)   TfL carrying out any Testing, including Testing by a TfL nominated Third Party, in conjunction with the Service Provider's Testing;

(C)   perform any specific sets of business process scenario Tests required by TfL;

(D)   demonstrate to TfL's reasonable satisfaction that adequate modifications and Testing have been performed leading to closure of any Incidents associated with the Test or the successful completion of the Test; and

(E)   ensure at all times that it provides a secure means of Test witnessing by TfL (or the relevant Third Party) pursuant to paragraph 8.2(A) of this Schedule which preserves the confidentiality and security of the Test Data and other information in connection with the Testing.

9.   **Use of Personal Data in Testing**

9.1   Subject to any contrary written instructions from TfL (as may be given from time to time), the Service Provider shall ensure that:

(A)   so far as practicable, all Test Data is manipulated, masked or scrambled so that it would no longer constitute Personal Data in a Third Party's hands; and

(B)   the use of Test Data which is Personal Data only occurs when essential to verify Testing integrity and then only in a secure Test environment, in accordance with good industry practice and guidance issued by the Information Commissioner from time to time.

9.2   Without prejudice to paragraph 9.1 of this Schedule 4, all Test Data shall:

(A)   be stored and held securely and otherwise in a manner that is compliant with any applicable Privacy Legislation, as shall all Data from which Test Data is derived;

(B)   in all but exceptional cases, have been processed to permanently and completely preserve the anonymity of the persons whose Data is contained therein in accordance with Privacy Legislation, best practice guidance that may be issued from time to time by the Information Commissioner, and/or other good industry practice, and Clauses 26 (*Loss of Software & Data Security*) and 37 (*Data Protection*) and using irreversible procedures and technology agreed by TfL in writing in advance of processing and use of such Data or Testing; and

(C)   be securely and promptly destroyed in accordance with relevant Privacy Legislation and good industry practice following completion of the relevant Tests for which such Test Data is being used unless it is required to be retained for any purpose compatible with the Data Protection Act. The Service Provider shall provide written confirmation to TfL that such Personal Data has been destroyed, as appropriate.

9.3   In the exceptional circumstances where the Service Provider believes that specific Testing requires the use of Test Data containing Personal Data such that the anonymity of the persons whose Data is contained therein is not completely established, then the Service Provider shall obtain the prior written approval of TfL for this use and in requesting such approval shall provide to TfL all information that TfL may require in relation thereto. The Service Provider acknowledges and agrees that TfL may at its absolute discretion decline such a request.

10.   **Disputes**

10.1   Any issues or disputes arising between the Parties in relation to Testing shall first be discussed by the Contract Manager and TfL's Contract Manager and, if not resolved within five (5) Business Days, shall be discussed and resolved in accordance with the Dispute Resolution Procedure.

ANNEX 1

Testing Methodology: Implementation Phase

1.   **Types of Testing**

1.1   During the Implementation phase the Service Provider shall carry out the following test and assurance activities:

   (A)   Functional Testing and Non-Functional Testing in a manner consistent with paragraph 3 (*Functional and Non-Functional Testing*) of this Annex;

   (B)   Systems Integration Testing in a manner consistent with paragraph 4 (*Systems Integration Testing*) of this Annex;

   (C)   Ready for Service Assurance in a manner consistent with paragraph 5 (*Ready For Service Assurance*) of this Annex; and

   (D)   Regression Testing in a manner consistent with paragraph 6 (*Regression Testing*) of this Annex.

2.   **Testing Documents**

2.1   The Service Provider shall be responsible for ensuring that all Testing is adequately documented.

2.2   The Service Provider shall structure the Test Documentation so that when taken together they collectively meet the requirements of this Schedule 4.

3.   **Functional & Non-Functional Testing**

3.1   The Service Provider shall ensure that Functional Testing and Non-Functional Testing shall take place to demonstrate that, when employing the Hardware to be used operationally in the System in its final location, the features, functions and facilities associated with the System or constituent parts of thereof (including but not limited to all Interfaces) behave in accordance with the relevant:

   (A)   requirements;

   (B)   design documents; and

   (C)   Test specifications.

   Functional Testing

3.2   The Service Provider shall ensure that any and all constituent parts of the System (including but not limited to all Interfaces) have been subject to Functional Testing which shall be conducted using a Test environment representative of the Hardware to be used operationally in the System, to a degree appropriate to the method and complexity of the development and configuration of the System, as set out in the Test Strategy.

3.3   The Service Provider shall ensure that Functional Testing of the System:

(A)   uses Data representative of operational conditions for the Testing;

(B)   demonstrates end-to-end Data and process flows across the System meet the Specification;

(C)   demonstrates Data and process integrity across the System, including across any and all interfaces between constituent parts of the System, works in accordance with the Specification;

(D)   verifies that Data and input validation works in accordance with the design documents;

(E)   demonstrates that Data display formatting works in accordance with the design documents;

(F)   demonstrates that screen/report layout are in accordance with the design documents;

(G)   demonstrates that process and screen navigation and the management of context Data meets the Specification and works in accordance with the design documents;

(H)   demonstrates continuity of processing across the System in accordance with the design documents;

(I)   includes negative and positive Tests for all functionality implemented within the System;

(J)   verifies through defined Tests that potentially damaging transactions cannot be performed;

(K)   demonstrates that Incidents are handled and reported correctly;

(L)   demonstrates that maximum, minimum, null and zero (0) Data values across the System and its Interfaces are correctly handled;

(M)   demonstrates that Data contention and Data locking are correctly handled;

(N)   demonstrates that transactional integrity and Data integrity and Data replication work correctly;

(O)   verifies that all Management Information is correctly recorded, stored and reported on; and

(P)   verifies that all systems, security, access and audit trail logs are appropriately and correctly updated.

Non-Functional Testing

3.4   The Service Provider shall perform Non-Functional Testing of the System:

(A)   employing the Hardware to be used operationally in the System in its final location unless exceptionally the use of a Test environment distinct from the Hardware to be used operationally in the System is agreed with TfL and documented in the Test Strategy; and

(B)   shall ensure that any Non-Functional Testing performed on a Test environment distinct from the Hardware to be used operationally in the System remains valid through the use of appropriate Regression Tests.

3.1   The Non-Functional Testing shall be designed to demonstrate that:

(A)   all Software and Hardware used in the System have been built correctly in terms of installation, configuration and connectivity in accordance with the design documents and System Build Documentation, including;

(1)   the performance of audits to ensure that all Hardware specified by the System Build Documentation as being used in the System is present and functional;

(2)   the performance of Tests to ensure that all Software specified by the System Build Documentation as being used in the System is present and functional;

(3)   the performance of configuration Tests in relation to all Software and Hardware in the System to ensure that it is configured in accordance with the System build Documentation;

(4)   the demonstration of complete network connectivity between the System and the Other Service Providers via the Interface specified in Appendix 13 (*Interface Catalogue*), employing Test environments representative of the system(s) of each Other Service Provider; and

(B)   the resilience of the System, including through;

(1)   the performance of fail-over Tests of all relevant Infrastructure;

(2)   the performance of load balancing Tests (where relevant);

(3)   Testing of the Business Continuity Plan, Business Continuity Infrastructure, Business Continuity services and other Business Continuity and back-up continuity procedures (in each case including as required in accordance with Schedule 25 (*Business Continuity*)), recovery work areas and overflow resources and Premises is complete, including without limitation the Testing of these aspects to confirm that they comply with the Security Policy as confirmed by an external independent BS7799 audit, and in each case has been Approved by TfL;

(C)   the System conform to the Security Policy;

(D)   the System is safe from external penetration and the Non-Functional Testing shall include independent external penetration Tests to demonstrate the security of the System from intrusion via networks external to those of the Service Provider, to be arranged by Service Provider:

(1)   at the cost of the Service Provider;

(2)   with the full participation of the Service Provider;

(3)   to occur;

(a) in advance the Operational Commencement Date or any processing of non-anonomised Personal Data by the System (whichever is the sooner); and

(b) additionally and without limitation, promptly upon written request from TfL from time to time;

(E)   the Software and Hardware comprising the System integrates correctly with each other and that the Interfaces of the System as documented in Appendix 13 (*Interface Catalogue*) to Schedule 2 (*Statement of Requirements*) comply with the relevant Interface specifications and any Third Party specifications prior to the commencement of Systems Integration Testing. Such integration Testing shall include;

(1)   demonstrating full end-to-end integration of the System;

(2)   technical integration Tests across the Interfaces between the System and the Other Service Providers via the Interface specified in Appendix 13 (*Interface Catalogue*) to Schedule 2 (*Statement of Requirements*), employing Test environments representative of the system(s) of each Other Service Provider, where necessary, to:

(a) demonstrate compliance with the relevant Interface specifications; and

(b) ensure all Interface failure conditions, exception conditions and recovery mechanisms are working effectively;

(F)   the System has the capacity to run without Incident for an extended period, and such Non-Functional Testing shall include demonstrating periods of extended and continuous operation to provide assurance to TfL of the reliability and maintainability of the System, including a period of continuous operation;

(1)   exercising all Software and Hardware comprising the System;

(2)   ensuring that the period of continuous running is of sufficient length to cover all material business activities.

(G)   the System can reliably:

(1)   run at the required load,

(2)   process the normal and maximum expected volumes of events or transactions, as set out in Appendix 3 (*Volumetrics*) to Schedule 2 (*Statement of Requirements*) and the design documents, and

(3)   achieve the required Performance Indicators and Service Levels and while maintaining accuracy and effective operational performance,

through the use of sufficient stored Data volumes on the Hardware to be used operationally in the System in its final location;

(H)   Data is correctly stored by the System;

(I)   all graphical user interfaces are easily comprehensible and usable by their target user base, including, where relevant, TfL Personnel;

(J)   the System complies with all Applicable Laws, including without limitation all Privacy Legislation, FOI Legislation, monitoring and interception of communication and similar laws from time to time in force to the extent applicable; and

(K)   the System as built provides accurate Management Information, and such Non-Functional Testing shall include that MIS and Interfaces in relation to TfL's systems perform to the reasonable satisfaction of TfL.

4.   **Systems Integration Testing**

4.1   The Service Provider shall ensure that System Integration Testing shall take place to ensure that the System will fully integrate and fully inter-operate with all systems to which they interface, directly or indirectly, including to each Other Service Provider via the Interface specified in Appendix 13 (*Interface Catalogue*) to Schedule 2 (*Statement of Requirements*).

4.2   Such System Integration Testing shall employ end-to-end Tests across the System, all other systems to which the System interfaces, and the Interfaces between them, designed to demonstrate that they behave in accordance with the relevant:

(A)   requirements;

(B)   design documents; and

(C)   Test specifications;

and shall be designed to identify where conflicts exist between the Specification, design and implementation of the System and other systems to which they interface with regard to delivering the Services.

4.3   The Service Provider shall ensure that Systems Integration Testing of the System is conducted employing Test environments representative of the Hardware to be used operationally in the System and at a location to be determined by TfL.

4.4   The Service Provider shall ensure that Systems Integration Testing includes, without limitation:

(A)   the demonstration of the full end-to-end integration of the System with all other Systems to which they interface by executing Tests based on end-to-end business processes and Data flows across all of those Systems against the business process definitions set out in the design documents and the Specification, so as to demonstrate compliance with the requirements;

(B)   Data constructed to cover normal and exception conditions, including but not limited to boundary values, null values and maximum length values, passed between the System and all other systems to which they interface;

(C)   Test of all Interface failure conditions and recovery from failure for all Interfaces between the System and all other systems to which they interface;

(D)   load and stress Testing performed with and across the System and all other systems to which they interface, including without limitation the MIS, to demonstrate that the System interoperating with the other systems can:

(1)   run at the required load,

(2)   process the normal and maximum expected volumes of events or transactions, as set out in Appendix 3 (*Volumetrics*) to Schedule 2 (*Statement of Requirements*) and the design documents, and

(3)   achieve the required Performance Indicators and Service Levels and while maintaining accuracy and effective operational performance;

(E)   Tests are performed to ensure and assure compliance with the Security Policy and other obligations set out in this Agreement; and

(F)   all Management Information is correctly accumulated from the System, stored and reported.

(G)   Tests are performed to demonstrate that Evidence Packs, Unattended Outstation Evidence Packs and Video Files are accessible by the correct Other Service Providers and that no Other Service Provider will have access to Evidence Packs, Unattended Outstation Evidence Packs and Video Files that they are not entitled to receive;

(H)   Tests performed to demonstrate the correct processing of heartbeat messages sent between the CCTV Instation CAM server and the System;

(I)   Tests are performed to demonstrate that the System is capable of integrating with all supported types of hardware Codecs and digital Cameras;

(J)   Tests are performed to demonstrate that the System supports the request, achievement, execution and relinquishment of the required degree of control of each of the types of hardware Codecs and digital Cameras;

(K)   Tests are performed to demonstrate that the System supports the receipt and recording of Video Files from each of the types of hardware Codecs and digital Cameras; and

(L)   Tests are performed to demonstrate the System integrates fully with the PES Mobile Application.

5.   **Ready For Service Assurance**

5.1   The Service Provider shall carry out Ready for Service Assurance to ensure that all Test related activities required prior to the Operational Commencement Date have been completed, including without limitation ensuring:

(A)   full completion of all Testing, including confirmation that:

(1)   Testing of the Security Policy has been undertaken and is complete;

(2)   independent external penetration has been undertaken by a company approved in writing by TfL in advance and is complete;

(3)   Testing of all MIS reporting has been undertaken and is complete; and

(4)   Testing of the Business Continuity Plan, Business Continuity Infrastructure, Business Continuity services and other Business Continuity and back-up continuity procedures has been undertaken and is complete, in each case including as required in accordance with Schedule 25 (*Business Continuity*);

(B)   the Test Strategy has been Approved;

(C)   that it has been demonstrated to TfL's reasonable satisfaction that the Evidential Integrity requirements for the Services have been met;

(D)   that it has been demonstrated to TfL's reasonable satisfaction that all audit mechanisms and trails are operational and adequate including without limitation by way of an external independent BS7799 audit (to be carried out by the National Computing Centre or such other suitably qualified Third Party as the Parties may agree in writing, the cost of which shall be borne by the Service Provider) and that the Service Provider shall at its own cost and expense promptly rectify any failing areas identified during the course of any such audit; and

(E)   that it has been demonstrated to TfL's reasonable satisfaction that the Service Provider's Data Retention mechanisms comply and continue to comply with Privacy Legislation, the Data Retention processes and procedures, and all TfL policies.

6.   **Regression Testing**

6.1   The Service Provider shall perform Regression Testing as necessary to demonstrate that any Software changes have no adverse impact on the System, the Interfaces or the Other Service Providers.

ANNEX 2

Testing of Changes and Incidents

1.   **Types of Testing**

1.1   The Service Provider shall in regard to any Change or the resolution of Incidents that might arise from time to time regarding the System or the Services and impacting on the System and/or the Services in live operation, carry out the following test and assurance activities:

(A)   Confirmation Testing in a manner consistent with paragraph 3 (*Confirmation Testing*) of this Annex;

(B)   Regression Testing in a manner consistent with paragraph 4 (*Regression Testing*) of this Annex; and

(C)   Acceptance Testing in a manner consistent with paragraph 5 (*Acceptance Testing*) of this Annex;

to a degree appropriate to the scope, complexity and criticality of such Change or Incident.

2.   **Testing Documents**

2.1   The Service Provider shall be responsible for ensuring that all Testing is adequately documented.

2.1   The Service Provider shall structure the Test Documentation so that when taken together they collectively meet the requirements of this Schedule 4.

3.   **Confirmation Testing**

3.1   The Service Provider shall carry out Confirmation Testing in relation to each Change or corrected Incident, targeted appropriately to the scope, complexity and criticality of the Change implemented or the correction made to confirm the correct implementation of the Change or correction.

3.2   The Service Provider shall ensure that the Confirmation Testing in relation to each Change or corrected Incident includes sufficient

(A)   functional testing (including as required: component testing, component integration testing, and system testing across the System and addressing where appropriate boundary value and negative testing); and

(B)   non-functional testing (including as required: performance testing and recoverability testing);

to ensure the System continues to operate in accordance with the relevant:

(1)   requirements;

(2)   design documents; and

(3)   Test specifications.

3.3   Where the nature of a Change or correction made in respect of the Incident is such as to potentially impact on the integration of the System with any systems to which the System interfaces, directly or indirectly, the Service Provide shall ensure that the Confirmation Testing includes sufficient Systems Integration Testing in accordance with paragraph 4 (*Systems Integration Testing*) of Annex 1 (*Testing Methodology: Implementation Phase*) to ensure that the System will continue to fully integrate and fully inter-operate with all systems to which they interface in accordance with the relevant:

(A)   requirements;

(B)   design documents; and

(C)   Test specifications.

4.   **Regression Testing**

4.1   The Service Provide shall carry out Regression Testing in relation to each Change or corrected Incident on the basis of analysis of the impact of the changes made to the System to demonstrate that the Change or corrected Incident has not affected the components of the System not subject to such Change or corrected Incident, including but not limited to end-to-end evidential integrity, in accordance with the design documents and the relevant Test specification;

5.   **Acceptance Testing**

5.1   The Service Provide shall carry out Acceptance Testing in relation to each Change or corrected Incident, including Tests of business process scenarios (including such business processes as reasonably specified by TfL) demonstrating the operation of all affected aspects of the Services, to demonstrate to TfL that the Change or Incident:

(A)   is in accordance with the design documents and the relevant Test specification;

(B)   is consistent with the agreed Change Control Request pursuant to Schedule 9 (*Change Control Request Procedure*);

(C)   is in accordance with the Security Plan;

(D)   complies with Privacy Legislation, the Data Retention processes and procedures, and all other policies and procedures of TfL which may be amended, replaced, or introduced during the Term;

(E)   is consistent with the Service Levels;

(F)   is implemented in accordance with good industry practice; and

(G)   complies with and does not prejudice the Business Continuity Plan, Business Continuity Infrastructure, Business Continuity services and other Business Continuity (in each case including as required in accordance with Schedule 25 (*Business Continuity*)) and back-up continuity procedures, recovery work areas and overflow resources and Premises, including without limitation Testing these aspects against the Security Plan in respect of that Change or corrected Incident (unless otherwise agreed in writing between the Parties).

5.2   For each Change or Incident the Service Provider shall, unless explicitly declined by TfL, agree with TfL the content of a demonstration of the updated Services in relation to:

(A)   the resolution of the relevant Incident, or

(B)   the implementation of the relevant Change,

including as required the demonstration of process scenarios (including such business processes as reasonably specified by TfL), the demonstration to be carried out prior to, and as a prerequisite of, the introduction into service of the relevant Change or Incident and in support of TfL's Assurance of the relevant Final Test Report.

6.   **Release Documentation**

6.1   The Service Provider shall where relevant prepare and provide to TfL Release Notes describing any new or amended functionality in functional user terms, any outstanding Incidents and any operational workarounds required due to those Incidents.