# SCHEDULE 25

## Business Continuity

1. **Scope**

1.1 This schedule covers TfL's requirements in respect of:

(A) any circumstance or event which renders, or which TfL considers likely to render, it necessary or desirable for alternative, additional or replacement Hardware, Software, Systems, Premises, Personnel, processing, methods, processes or procedures as set out in the Business Continuity Plan instead of or as well as the Services, Service Systems, Services Data, Premises or Personnel (or any part of the Services, Service Systems, Services Data, Premises or Personnel) otherwise used to provide the Services in accordance with the provisions of this Agreement (a "**Business Continuity Event**"); or

(B) any circumstance or event which renders, or which TfL considers likely to render, the Services, Service Systems, Services Data, Premises or Personnel (or any part of the Services, Service Systems, Services Data, Premises or Personnel) unavailable, inaccessible, inoperable or in need of any other restoration, reinstallation, repair, removal, retrieval, re-entering, recovery or replacement (a "**Disaster Recovery Event**"),

whether resulting from an act or omission of the Service Provider or otherwise, including without limitation Hardware, Software or System failures, Service Failure, Viruses, changes in Law, fire, flood, water, wind, lightning and any other adverse weather conditions, explosions and any other catastrophe or Force Majeure Event. For the avoidance of doubt, a Disaster Recovery Event shall include the following:

(1) System Data loss and corruption;

(2) System Failure;

(3) Loss of power;

(4) Failure of any of the Service Systems Interfaces;

(5) Failure of the communication links between the Service System Element and any Connected Party; and

(6) Loss of the Premises and access to any Service System Element and any Connected Party.

1.2 The Service Provider acknowledges and agrees that Business Continuity in respect of the Services and Schemes is fully dependent upon the Business Continuity Plan, Business Continuity Infrastructure and Business Continuity Services and that it is necessary for the Service Provider to ensure Business Continuity and the provision of the Services in accordance with the provisions of this Agreement in all circumstances, events and scenarios including without limitation in respect of and following a Business Continuity Event or a Disaster Recovery Event.

1.3 Without limiting paragraph 1.2, the Service Provider shall:

(A) develop the Business Continuity Plan and the Business Continuity Test Schedule in accordance with the Implementation Plan (as part of the relevant Milestone);

(B) review and keep up to date the Business Continuity Plan and the Business Continuity Test Schedule and submit them to TfL for Approval on an ongoing basis during the Term;

(C) provide the Business Continuity Infrastructure and other actions or measures specified in the Business Continuity Plan to prevent or limit the effect of any Business Continuity Event or Disaster Recovery Event;

(D) continue to meet the Service Levels in accordance with Schedule 5 (Service Levels), in the event of a Business Continuity Event or Disaster Recovery Event;

(E) ensure that the Services, Service Systems, Services Data, Premises or Personnel (or any part of the Services, Service Systems, Services Data, Premises or Personnel) used to provide the Services in accordance with the provisions of this Agreement are resumed as soon as possible (and in any event within the time frames set out in the Business Continuity Plan) following a Business Continuity Event or Disaster Recovery Event (as applicable) in place of the Business Continuity Infrastructure or Business Continuity Services or any other alternative, additional or replacement Hardware, Software, Systems, Premises, Personnel, processing, methods, processes or procedures as set out in the Business Continuity Plan;

(F) review any Business Continuity Event and Disaster Recovery Event every day and inform TfL if it considers that it could cease implementation of the Business Continuity Plan, the Business Continuity Infrastructure or the Business Continuity Services and maintain Business Continuity. The Service Provider shall only cease to follow the Business Continuity Plan, use the Business Continuity Infrastructure or provide the Business Continuity Services (following a Business Continuity Event or a Disaster Recovery Event) if TfL has expressly agreed in writing that the Service Provider may do so;

(G) Test the Business Continuity Plan, the Business Continuity Services and Business Continuity Infrastructure;

(H) ensure that the Service Provider's management of its response to the Business Continuity Event and the associated activities of the Service Provider, TfL Other Service Providers and Third Parties, is conducted in accordance with ISO 27031;

(I) provide the Business Continuity Services and implement the applicable provisions of the Business Continuity Plan; and

(J) comply with its other obligations in this Schedule.

1.4 The Service Provider shall ensure that the Business Continuity Plan is implemented to the extent necessary in relation to any Change or Partial Termination.

## 2. Business Continuity Plan and Business Continuity Test Schedule

2.1 The Service Provider shall:

(A) ensure that a draft Business Continuity Plan and a draft Business Continuity Test Schedule are prepared and submitted to TfL not less than ten (10) Working Days prior to the relevant Milestone Date for Approval; and

(B) maintain the Business Continuity Plan and the Business Continuity Test Schedule on an ongoing basis during the Term.

2.2 The Service Provider shall in accordance with Clause 15.1.9 co-operate with the Other Service Providers as necessary to plan for the provision by the Other Service Providers of the appropriate business continuity services to the Service Provider and shall ensure that the relevant elements of the Other Service Providers' business continuity plans are taken into account by the Service Provider in the Business Continuity Plan and the Business Continuity Test Schedule.

2.3 The Service Provider shall ensure that its Sub-Contractors co-operate with Other Service Providers in a Business Continuity Event or Disaster Recovery Event.

2.4 The Service Provider shall review and resubmit the Business Continuity Plan and the Business Continuity Test Schedule to TfL for Approval:

(A) at least annually;

(B) if requested as part of any Change;

(C) after a Business Continuity Event and/or Disaster Recovery Event; and

(D) at such other intervals as may be required by TfL or the Service Provider.

2.5 Following TfL's Approval of a revised Business Continuity Plan and/or Business Continuity Test Schedule, the Service Provider shall (at no additional cost to TfL) promptly implement the latest Business Continuity Plan and the Business Continuity Test Schedule without prejudice to the Service Provider's obligations to comply with Good Industry Practice.

2.6 Any change to the Business Continuity Plan or the Business Continuity Test Schedule must be Approved by TfL prior to being effective.

2.7 The Service Provider shall ensure that the reviews examine (without limitation) the procedures and methodologies set out in the Business Continuity Plan and the Business Continuity Test Schedule and assess their suitability in light of any changes to the Services. Within twenty (20) Working Days of conclusion of such review, the Service Provider shall provide a report to TfL specifying:

(A) the findings of the review;

(B) any resulting changes to the risk profile of the Services and/or the Service System(s) (and the Service Provider shall update the Risk Register to reflect this); and

(C) the recommendations for addressing the new risk profile and any other findings of the review as it deems necessary.

2.8 TfL may from time to time issue a notice to the Service Provider requiring the Service Provider to amend the Business Continuity Plan or the Business Continuity Test Schedule. Upon receipt of such a notice from TfL, the Service Provider shall submit an amended version of the Business Continuity Plan or Business Continuity Test Schedule to TfL for Approval. TfL shall require the Service Provider to liaise, assist and co-operate with Other Service Providers (both when developing and when integrating the amendments to the Business Continuity Plan and the Business Continuity Test Schedule) to ensure consistency and inter-operability between the various business continuity and disaster recovery plans of the Service Provider and Other Service Providers, and to produce the updated Business Continuity Plan and Business Continuity Test Schedule on this basis. Any disputes arising pursuant to this paragraph shall be dealt with in accordance with the Dispute Resolution Procedure.

2.9 The Service Provider may request additional payment or changes to the Service Charges only in respect of material amendments to the Business Continuity Plan or the Business Continuity Test Schedule where such amendments arise as a result of a decision by TfL to change its requirements pursuant to paragraph 2.6 other than as a result of any act or omission of the Service Provider (or any Sub-Contractor) (such payments or changes to the Service Charges to be requested and implemented in accordance with the Change Control Request Procedure.

2.10 Without limitation to the generality of Clause 44 (Business Continuity), the Service Provider shall ensure that the Business Continuity Plan includes:

(A) an introduction describing the purpose and structure of the Business Continuity Plan and how to use the Business Continuity Plan;

(B) a master plan describing the overall strategy for ensuring Business Continuity (and for responding to a Business Continuity Event or Disaster Recovery Event) in respect of all Service Elements and all Service System(s) including without limitation the interrelationships and dependencies of each of the parts of the Business Continuity Plan relating to each of the Service Elements and Interfaces envisaged in paragraph 2.10(C);

(C) separate plans for each Service Element and all Service System Interfaces in order to ensure Business Continuity (and to respond to a Business Continuity Event or Disaster Recovery Event) in respect of the relevant Service Element and parts of the Service Systems including without limitation:

(1) a risk and issue assessment;

(2) Business Continuity planning and all actions or measures to prevent or limit the effect of any Business Continuity Event or Disaster Recovery Event such as hot, warm, cold or mobile backup sites, locations or Sub-Contractors;

(3) a description of all methods, processes and procedures and other actions and sequences to be followed for Business Continuity and to respond to a Business Continuity Event or Disaster Recovery Event (all such processes, procedures, actions and sequences to be at the sole cost and expense of the Service Provider) such as notifying TfL, Customers, Other Service Providers, Third Parties and Personnel, assignment of Personnel and tasks, using or recalling backups or

storage, recovering, re-entering or correcting Data, additional Personnel or other resources to be deployed, or additional, alternative or replacement Hardware, Software, Systems, Premises, processing, processes or procedures;

(4) all steps to be taken (all such steps to be at the sole cost and expense of the Service Provider) for the Services, Service Systems, Services Data, Premises or Personnel (or any part of the Services, Service Systems, Services Data, Premises or Personnel) to be provided as envisaged under this Agreement (such that the Service Provider can cease to follow the Business Continuity Plan in accordance with paragraph 1.3(F));

(5) management and review activities;

(6) the relevant parts of the Business Continuity Test Schedule;

(7) a description of how the relevant part of the Business Continuity Plan should be applied to not less than three (3) potential Business Continuity Event or Disaster Recovery Event scenarios to be specified by TfL at TfL's absolute discretion, including without limitation loss of access to Premises, sickness of Personnel and Data corruption (each a "**Scenario**"), the quantified impact to TfL of any loss of Service in the case of each Scenario and action maps for each different Scenario including the recovery priorities for each part of the Service;

(8) a description of the capability of the Services and/or Service Systems which shall be delivered under each Scenario as a proportion of the capability required under the provisions of the Agreement including without limitation the Service Levels;

(9) a description of the Hardware, Software, Systems and Premises that house and support the Business Continuity Services or relate to the Business Continuity Test Schedule (the "**Business Continuity Infrastructure**");

(10) provision for an extended Business Continuity Event or Disaster Recovery Event such as permanent loss of Premises; and

(11) separate detailed plans in respect of responding to a Business Continuity Event, on the one hand, and responding to a Disaster Recovery Event, on the other hand (and including without limitation all Hardware, Software and Systems for responding to a Disaster Recovery Event). The plan for responding to a Disaster Recovery Event shall include, but not be limited to:

a) an emergency response plan

b) a damage assessment plan

c) a salvage plan

d) a vital records plan

e) a crisis management and communications plan (including declaration of the Disaster Recovery Event and verification of recovery and restoration of the Service)

f) an accommodation and Services plan

g) Security Plan

h) a personnel plan

i) a finance and administration plan

j) a Service recovery priority

k) contacts

l) escalation procedures.

2.11 The Service Provider shall ensure that the Business Continuity Plan is designed in such a way to ensure that:

(A) the Business Continuity Plan does not depend on any Other Service Provider adjusting its Hardware, Software or Systems as a result of any Business Continuity Event or Disaster Recovery Event;

(B) in the event of a Business Continuity Event or Disaster Recovery Event the security of the Services and the Service Systems is not compromised in any way by the Business Continuity Event or Disaster Recovery Event;

(C) in the event of a Business Continuity Event or Disaster Recovery Event the Service Provider will still be able to make available datasets so that other Service Elements within the Services will be able to perform the Data synchronisations required in order to ensure consistent Data across the Services and Service Systems;

(D) it allows the Services to be provided by the Service Provider in accordance with the Service Levels and that the Business Continuity Plan mitigates the adverse impact of a Business Continuity Event or Disaster Recovery Event;

(E) the Business Continuity Plan is upgradeable and sufficiently flexible to support any changes to the business functionality and changes to the business processes facilitated and supported by the Services and/or the Service Systems in the future (including without limitation pursuant to Clause 18 (Technology Compatibility and Flexibility);

(F) the Service Provider is able to respond to, and comply with, the instructions or directions of any civil and/or military authority (including without limitation the fire, police or army services) attending any Premises affected by a Business Continuity Event or Disaster Recovery Event, without affecting the Service Provider's compliance with Schedule 14 (Security Policy) and the Security Plan; and

(G) it otherwise complies with the provisions of Clause 45 (Security) and the Security Plan and Schedule 14 (Security Policy).

## 3. **Testing**

3.1 Subject to paragraph 3.2, the Service Provider shall (at no cost to TfL) Test all aspects of the Business Continuity Plan (including without limitation the Business Continuity Services and the Business Continuity Infrastructure) in accordance with the Business Continuity Test Schedule and as a minimum:

(A) during Simulated Operation Testing and Ready for Service Assurance in accordance with Schedule 4 (Testing Regime);

(B) once in each twelve (12) month period taken from the Operational Commencement Date,

in each case at a time Approved in advance by TfL.

3.2 The Service Provider shall conduct the Testing envisaged under paragraph 3.1, in part or in full, more frequently than as set out in paragraph 3.1 if:

(A) TfL agrees to pay the Service Provider's reasonable costs in carrying out such Tests (subject to paragraph 3.3); or

(B) TfL reasonably believes that the Service Provider is not complying with its requirements under this schedule; or

(C) there is a loss of service or failure to meet all Service Levels due to an event that TfL reasonably believes to have been a Business Continuity Event or Disaster Recovery Event.

3.3 If TfL has requested the Service Provider to conduct Testing pursuant to paragraph 3.2(B), the Service Provider's reasonable costs (as notified in advance in writing and calculated at the rates specified in the Billing Model shall be borne by TfL unless the Tests fail as determined in accordance with the provisions of Schedule 4 (Testing Regime), in which case the costs and expenses (including without limitation TfL's and any Other Service Provider's or Third Party's costs and expenses) shall be borne by the Service Provider.

3.4 The Service Provider shall undertake and manage the Testing envisaged under this paragraph 3 in full consultation with TfL and any Other Service Provider or any Third Party nominated by TfL and will liaise with TfL in respect of the planning, performance and review of each Test.

3.5 The Service Provider shall participate in the Testing envisaged under this paragraph 3 with Other Service Providers, or any Third Party, at least once a year beginning on 25 June or such other day as may be specified by TfL from time to time.

3.6 The Service Provider shall perform post-Testing reviews and provide TfL with a formal report of the test results within five (5) Working Days of each Test. If Incidents are identified, the Service Provider shall use the Incident Management Process to manage, remedy, and report on each Incident.

3.7 The report required under paragraph 3.6 should include at a minimum:

(A) the details requested for a final Test Report in Schedule 4 (Testing Regime);

(B) a comparison of the results to the measures and purposes identified in the Business Continuity Plan;

(C) a report on the feedback from Test participants, Operational IT Users and other relevant stakeholders as to the adequacy of continuity for their respective areas; and

(D) a plan delivered no later than five (5) Working Days from Testing completion to rectify any failures identified.

## 4. Business Continuity Services and Business Continuity Infrastructure

4.1 The Service Provider shall ensure that the Business Continuity Services and the Business Continuity Infrastructure comply with the Security Policy and Clause 45 (Security).

4.2 The Service Provider shall ensure that appropriate Business Continuity Services and Business Continuity Infrastructure shall be provided by it or to it by its Sub-Contractors in accordance with the Business Continuity Plan and the requirements of this Schedule. The Service Provider shall ensure that the Sub-Contractors' business continuity plans and disaster recovery plans shall be integrated into and comply with the Business Continuity Plan and the Sub-Contractors' business continuity and disaster recovery infrastructure is integrated into the Business Continuity Infrastructure.

4.3 The Service Provider shall ensure that spares, maintenance equipment and Test equipment are available for use at the Premises in order to support and maintain provision of the Business Continuity Services and Business Continuity Infrastructure.

4.4 If the Premises are unavailable or inaccessible due to a Disaster Recovery Event, or a Business Continuity Event affecting any Services, the Service Provider shall ensure that all Services that would otherwise be provided from or via those Premises (including without limitation all support and maintenance envisaged under this Agreement and contact information and methods identified in the Communication Plan) continue to be provided through the Business Continuity Infrastructure independent of the Premises by redirecting the provision of such Services to the Business Continuity Premises.

4.5 The Service Provider shall ensure that for all Business Continuity Premises there is a named Business Continuity Premises manager who shall be responsible for executing the Business Continuity Services at each such set of Business Continuity Premises.

4.6 The Service Provider shall ensure that there is a named overall Business Continuity manager responsible for executing the Business Continuity Services and providing the Business Continuity Infrastructure and who shall act as a point of contact for TfL.

4.7 The Service Provider shall ensure that there is a named emergency management team which shall act as a point of contact for TfL and be available 24 hours a day, 7 days a week, 365 days a year including in the event of a Business Continuity Event or a Disaster Recovery Event.

4.8 The Service Provider shall ensure that the Service Systems, including but not limited to the Business Continuity Infrastructure, permit remote access, monitoring and control of elements of the Service Systems sited or situated at the Premises. The Service Provider shall ensure that these remote facilities are usable from the Business Continuity Premises to permit management and access to Data and ensure that there is no loss of Data should the Premises be unavailable or evacuated. The Service Provider shall ensure that where remote access is used enhanced encryption measures are used to protect system security in accordance with the Security Plan.

4.9 The Service Provider shall ensure that the Business Continuity Infrastructure is at all times equipped with versions of the Service Systems Software that are in the same release state to those used in the rest of the Service Systems.

## 5. TfL's Right to Inspect

Without prejudice to any other rights of TfL under Clause 36 (Audit and Inspection) or any other provisions of the Agreement, TfL may inspect any Premises (excluding Cloud Premises), Systems, Hardware or Software to identify any circumstances which caused or which TfL (in its absolute discretion) considers likely to cause the Business Continuity Plan to be invoked. The Service Provider shall make available all relevant information, Data, assistance, facilities, access and Personnel in relation to such inspection or circumstances.

## 6. General

6.1 The Service Provider shall ensure that the Business Continuity Plan complies, the Business Continuity Services comply and the Business Continuity Infrastructure complies, as a minimum, with Good Industry Practice and are consistent with the Service Providers Solution.

6.2 The Service Provider agrees that, in determining what constitutes Good Industry Practice, TfL may provide any information, data or documentation to any Third Party in order to assess Good Industry Practice or whether Good Industry Practice is being complied with pursuant to paragraph 6.1 and TfL may, subject to the Service Provider's right to dispute any Third Party assessment in accordance with Schedule 21 (Dispute Resolution), require the Service Provider to review and resubmit the Business Continuity Plan and the Business Continuity Test Schedule for Approval pursuant to paragraph 2.4 based upon that Third Party's assessment of Good Industry Practice.