SCHEDULE 7

BUSINESS CONTINUITY AND DISASTER RECOVERY

PURPOSE OF THIS SCHEDULE

## This schedule sets out the Authority’s requirements for ensuring continuity of the Services in circumstances of Service disruption or failure and for restoring the Services through disaster recovery procedures. It also includes the requirement on the Supplier to develop, review, test, change, and maintain the Business Continuity Plan and the Disaster Recovery Plan.

## The Business Continuity Plan and Disaster Recovery Plan shall:

### detail the processes and arrangements which the Supplier shall follow to ensure continuity of business processes and operations following any failure or disruption of any element of the Services and to ensure restoration of the Services in the event of a Supplier Business Continuity Event or a Disaster; and

### recognise the requirement for the Supplier and its Sub‑Contractors to follow Best Industry Practice in respect of the adoption of organisational business continuity plans.

# **DEVELOPMENT OF THE BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN**

## The Business Continuity Plan and Disaster Recovery Plan shall unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of paragraphs 3, 4 and 5 of this schedule.

## The Supplier shall provide the Business Continuity Plan and Disaster Recovery Plan to the Authority by the Milestone 1A in the Implementation Plan.

PART A ‑ GENERAL PRINCIPLES AND REQUIREMENTS

## The Business Continuity Plan and Disaster Recovery Plan shall:

### address how the Supplier shall meet the requirements of the Specification in respect of business continuity and disaster recovery;

### provide details of how the invocation of any element of the Business Continuity Plan and Disaster Recovery Plan may impact upon the operation of the Services;

### contain an obligation upon the Supplier to liaise with the Authority and (at the Authority’s request) any third party with respect to issues concerning disaster recovery where applicable;

### contain a communication strategy including details of an Incident and problem management service and advice and help desk facility;

### contain a risk analysis, including:

#### failure or disruption scenarios and assessments and estimates of frequency of occurrence;

#### identification of accepted residual risks not further mitigated, including failure of central internet components or any Force Majeure Event;

#### identification of any single points of failure that may arise as part of the delivery of the Services, and processes for managing the risks arising therefrom;

#### identification of risks arising from the interaction of the Services with the services provided by a third party; and

#### a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions;

### provide for documentation of processes, including business processes and procedures;

### set out key contact details (including roles and responsibilities) for the Supplier (and any Sub‑Contractors) and for the Authority;

### identify the procedures for reverting to "normal service". ;

### set out method(s) of recovering or updating data collected during a failure or disruption to ensure that there is no data loss and to preserve data integrity;

### provide for the provision of technical advice and assistance to key contacts at the Authority as notified by the Authority from time to time to inform decisions in support of the Authority’s business continuity plan and disaster recovery plans; and

### set out how the business continuity and disaster recovery elements link to each other.

## The Business Continuity Plan and Disaster Recovery Plan shall be designed so as to ensure that:

### the Services are provided in accordance with the agreement at all times during and after the invocation of the Business Continuity Plan and Disaster Recovery Plan;

### the adverse impact of any Disaster, Supplier Business Continuity Event, service failure, or disruption on the operations of the Scheme is minimal as far as reasonably possible;

### it follows in general the relevant provisions of ISO/IEC 27002, BS ISO/IEC 27001, ISO/IEC 20000; and

### there is a process for the management of disaster recovery testing and business continuity testing detailed in the Disaster Recovery Plan and Business Continuity Plan, respectively.

## The Business Continuity Plan and Disaster Recovery Plan must be upgradeable and sufficiently flexible to support any changes to the Services or to the business processes and business operations facilitated by them.

## The Supplier shall not be entitled to any relief from its obligations under the Service Levels or to any increase in the Charges to the extent that a Disaster and/or Supplier Business Continuity Event occurs as a consequence of any breach by the Supplier of this agreement.

## The Supplier shall comply with the maximum RTO and RPO, as set out in the following table:

|  |  |  |
| --- | --- | --- |
| Services | Maximum recovery times (RTO) | Maximum data loss (RPO) |
| The impacted element of the Services  | [●] | [●] |

### **[*Note to Bidders: The confirmed maximum RTO/RPO shall be taken from the bidder response*]**

## For the purposes of paragraph 3.5, "**RTO**" shall mean the period of time and service level within which a process which is provided to the Authority or which otherwise supports the Services shall be restored following a Supplier Business Continuity Event and/or Disaster and "**RPO**" shall mean the maximum tolerable period during which data is lost from an IT service in the event of a Supplier Business Continuity Event and/or Disaster.

PART B: DISASTER RECOVERY ‑ PRINCIPLES AND CONTENTS

## The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the operation of the Services (as far as reasonably practicable).

## The Disaster Recovery Plan shall only be invoked upon the occurrence of a Disaster.

## The Disaster Recovery Plan shall include the following:

### the Disaster Recovery System architecture;

### details of the procedures and processes to be put in place by the Supplier and any Sub‑Contractor in relation to the Disaster Recovery System and the provision of the Disaster Recovery Services and any testing of the same including but not limited to the following:

#### disaster recovery audits;

#### backup methodology and details of the Supplier's approach to data back‑up and data verification;

#### identification of agreed (between the Supplier and the Authority) disaster scenarios;

#### risk analysis and residual risk acceptance;

#### documentation of processes and procedures;

#### planning in respect of any specific components that are included within the Services, including any data networks and communication links;

#### invocation rules;

#### Services recovery procedures; and

#### steps to be taken upon Services resumption to address any prevailing effect of failure or disruption to the Services;

### any applicable Service Levels with respect to the provision of Disaster Recovery Services;

### details of how the Supplier shall ensure compliance with security Standards ensuring that compliance is maintained for any period during which the Disaster Recovery Plan is invoked;

### access controls (to any disaster recovery sites used by the Supplier or any Sub‑Contractor in relation to its obligations pursuant to this schedule); and

### annual testing and management arrangements.

PART B – BUSINESS CONTINUITY ELEMENT – PRINCIPLES AND CONTENTS

## The parties acknowledge that the Authority may be materially impacted by any significant failure in or disruption to the operations of the Supplier or any Sub-Contractor, however caused ("**Supplier Business Continuity Event**") and that it is in the interests of both parties to ensure that the Supplier and its Sub-Contractor all have comprehensive business continuity plans in place to eliminate or significantly reduce any effect upon the Services or upon the Authority and the Users of any Supplier Business Continuity Event which may occur.

## The Supplier shall ensure that the Business Continuity Plan is sufficiently robust to ensure that the provision of the Services will be maintained or recovered within the defined continuity or recovery strategy set out in the Business Continuity Plan in the event that a Supplier Business Continuity Event occurs affecting any aspect of the Supplier's operations relating or contributing to the provision of the Services.

## The Business Continuity Plan shall set out the arrangements that are to be invoked should there be any Supplier Business Continuity Event, including:

### the alternative processes, (including business processes), options and responsibilities that may be adopted in the event of a failure in or disruption to such operations; and

### the steps to be taken by the Supplier upon resumption of the Services in order to address any prevailing effect of the failure or disruption including a root cause analysis of the failure or disruption.

## The Business Continuity Plan shall address the various possible levels of failures of or disruptions to the Services and the services to be provided and the steps to be taken to remedy to the different levels of failure and disruption. The Business Continuity Plan shall also clearly set out the conditions and/or circumstances under which the Disaster Recovery Plan is invoked.

REVIEW AND AMENDMENT OF THE BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

## The Supplier shall review the Business Continuity Plan and Disaster Recovery Plan (and the risk analysis on which it is based):

### on a regular basis and as a minimum once every sixcalendar months;

### within three calendar months of the Business Continuity Plan and Disaster Recovery Plan (or any part) having been invoked pursuant to this schedule; and

### where the Authority requests any additional reviews (over and above those provided for in paragraphs 6.1.1 and 6.1.2 of this schedule) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Authority’s written requirements. The costs of both parties for any such additional reviews will be met by the Authority.

## Each review of the Business Continuity Plan and Disaster Recovery Plan pursuant to paragraph 6.1 shall be a review of the procedures and methodologies set out in the Business Continuity Plan and Disaster Recovery Plan and shall assess their suitability having regard to any Changes that have taken place since the later of the original approval of the Business Continuity Plan and Disaster Recovery Plan or the last review of the Business Continuity Plan and Disaster Recovery Plan and shall also have regard to any occurrence of any event since that date (or the likelihood of any such event taking place in the foreseeable future) which may increase the likelihood of the need to invoke the Business Continuity Plan and/or Disaster Recovery Plan. The review shall be completed by the Supplier within the period set out in the Business Continuity Plan and Disaster Recovery Plan or if no such period is set out in the Business Continuity Plan and/or Disaster Recovery Plan, the period as the Authority shall require, and the Supplier shall reasonably agree with. The Supplier shall, within 20 Working Days of the conclusion of each such review of the Business Continuity Plan and Disaster Recovery Plan, provide to the Authority a report (**Review Report**) setting out:

### the findings of the review;

### any changes in the risk profile associated with the Services; and

### the Supplier's proposals for addressing any changes in the risk profile and its proposals for amendments to the Business Continuity Plan and/or Disaster Recovery Plan following the review detailing the impact (if any and to the extent that the Supplier can reasonably be expected to be aware of the same) that the implementation of such proposals may have on any services or systems provided by the Authority, such proposals to be subject to the Authority’s approval.

## The Supplier shall as soon as reasonably practicable after receiving the Authority’s approval of the Supplier's proposals (having regard to the significance of any risks highlighted in the Review Report) effect any change in its practices or procedures necessary so as to give effect to the Supplier's proposals. Any such change shall be at the Supplier's expense unless it can be reasonably shown that the changes are required because of a material change to the risk profile of the Services.

TESTING OF THE BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN

## The Supplier shall test the Business Continuity Plan and Disaster Recovery Plan on a regular basis (and in any event not less than once in every Contract Year). Subject to paragraph 7.2, the Authority may require the Supplier to conduct additional tests of some or all aspects of the Business Continuity Plan and/or Disaster Recovery Plan at any time where the Authority considers it necessary, including where there has been any change to the Services or on the occurrence of any event which may increase the likelihood of the need to implement the Business Continuity Plan and/or Disaster Recovery Plan.

## If the Authority requires an additional test of the Business Continuity Plan and/or Disaster Recovery Plan it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Authority’s requirements and the relevant provisions of the Business Continuity Plan and/or Disaster Recovery Plan. The Supplier's costs of the additional test shall be borne by the Authority, unless the Business Continuity Plan and Disaster Recovery Plan fails the additional test in which case the Supplier’s costs of that failed test shall be borne by the Supplier.

## The Supplier shall undertake and manage testing of the Business Continuity Plan and Disaster Recovery Plan in full consultation with the Authority, and shall liaise with the Authority in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Authority in this regard. Each test shall be carried out under the supervision of the Authority or its nominee.

## The Supplier shall ensure that any use by it or any Sub‑Contractor of "live" data in such testing is first approved by the Authority. Copies of live test data used in any such testing shall be (if required by the Authority) destroyed or returned to the Authority on completion of the test.

## For the avoidance of doubt, the carrying out of a test of the Disaster Recovery Plan and/or Business Continuity Plan (including a test of the Disaster Recovery Plan and/or Business Continuity Plan procedures) shall not relieve the Supplier of any of its obligations under this schedule or otherwise.

## The Supplier shall, within 20 Working Days, of the conclusion of each test, provide to the Authority a report setting out:

### the outcome of the test;

### any failures in the Business Continuity Plan and/or Disaster Recovery Plan (including the procedures) revealed by the test; and

### the Supplier’s proposals for remedying any such failures.

## Following each test, the Supplier shall promptly implement any actions and all measures requested by the Authority, (including requests for the re-testing of the Business Continuity Plan and/or Disaster Recovery Plan) to remedy any failures in the Business Continuity Plan and/or Disaster Recovery Plan and such remedial activity and re-testing shall be completed by the Supplier, at no additional cost to the Authority, by the date reasonably required by the Authority and set out in such request.

INVOCATION OF THE BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN

The Supplier shall invoke the Business Continuity Plan and Disaster Recovery Plan in accordance with its provisions (and shall inform the Authority promptly of such invocation).