Ministry of JUSTICE

Hosting

Schedule 8.6: Business Continuity

TABLE OF CONTENTS

1. PURPOSE OF THIS SCHEDULE

1.1 This schedule 8.6 (Business Continuity) sets out the requirements for the Hosting Supplier with respect to ITSCM for the Hosting Supplier's internal business functions, operations and services. This shall include, but not be limited to: developing, reviewing, testing, changing and maintaining the Hosting ITSCM Plan, Hosting ITSC Plan(s) and Hosting Disaster Recovery Plan. Schedule 2.1 (Service Requirements) sets out the Hosting Supplier's obligations with respect to ITSCM for the FITS Services.

1.2 The Hosting ITSCM Plan shall detail the processes and arrangements which the Hosting Supplier shall implement following an ITSC Event and shall be comprised of three parts:

1.2.1 part A - general principles and requirements;

1.2.2 part B - Hosting ITSC Plan(s); and

1.2.3 part C - Hosting Disaster Recovery Plan(s), to be invoked by the Hosting Supplier following a Critical Incident.

2. DEVELOPMENT AND MANAGEMENT OF THE HOSTING ITSCM PLAN

2.1 The Hosting Supplier shall work and co-operate with the Authority, and Suppliers with respect to ITSCM.

2.2 The Hosting Supplier shall develop the Hosting ITSCM Plan in conjunction with the provisions of paragraph 12.4 (IT Service Continuity Management) of schedule 2.1 (Service Requirements).

2.3 The Hosting ITSCM Plan shall, unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of this schedule 8.6 (Business Continuity).

2.4 The Hosting ITSCM Plan will be provided to the Authority for Approval within ninety (90) Working Days of the Effective Date.

2.5 The Hosting Supplier shall demonstrate Configuration Management of the Hosting ITSCM Plan to the Authority and make the Hosting ITSCM Plan available to the Authority within three (3) Working Days of request.

3. PART A - HOSTING ITSCM PLAN

3.1 The Hosting ITSCM Plan shall:

3.1.1 describe the dependencies between the Hosting ITSC Plan(s) and Hosting Disaster Recovery Plan(s);

3.1.2 provide details of how the invocation of any element of the Hosting ITSCM Plan may impact upon the provision of the FITS Services;

3.1.3 detail how the Hosting ITSCM Plan links and interoperates with any of the Authority's Business Continuity and Hosting Disaster Recovery Plan(s);

3.1.4 detail how the Hosting ITSCM Plan links and interoperates with any of the Other Suppliers' ITSC Plans and the Hosting Disaster Recovery Plan(s), where applicable;

3.1.5 contain a communication plan including the specific communication channels with the Authority;

3.1.6 detail the Hosting Supplier's processes and procedures, including, but not limited to, Incident Management and Problem Management, in the event that an ITSC Plan is invoked;

3.1.7 contain a Risk Analysis, including, but not limited to:

3.1.7.1 ITSC Event scenarios and assessments, and estimates of frequency of occurrence;

3.1.7.2 identification, impact analysis and risk management of any single point of failure within the Hosting Supplier's internal business functions, operations and services that may impact the End to End Services; and

3.1.7.3 identification, impact analysis and risk management of anticipated ITSC Events that may impact the End to End Services;

3.1.8 identify and document the processes and procedures for restoring the services to normal operations.

3.1.9 demonstrate how the Hosting Services shall be provided as set out in schedule 2.1 (Service Requirements) and schedule 2.2 (Service Performance Management) in the event of an ITSC Event;

3.1.10 be consistent with current industry standards and best practices; and

3.1.11 set out the processes and procedures for reviewing, testing, changing and maintaining the Hosting ITSCM Plan.

3.2 Upon the occurrence of a Critical Incident where the Hosting Supplier invokes the Hosting ITSCM Plan the Hosting Supplier shall inform the Authority before it is invoked or as soon as practicable thereafter.

4. PART B – HOSTING ITSC PLANS

4.1 The Hosting ITSC Plan shall set out the arrangements that are to be invoked to ensure continuity of the Hosting Supplier's internal business functions, operations and services. The Hosting ITSC Plan shall include, but not be limited to:

4.1.1 alternative processes, (including business processes), options and responsibilities that shall be adopted in the event an ITSC Event affects the Hosting Services; and

4.1.2 the steps to be taken by the Hosting Supplier upon resumption of the Hosting Services in order to address any prevailing effect or impact of the ITSC Event, including a root cause analysis and remediation plans.

4.2 The Hosting ITSC Plan shall set out the conditions under which the Hosting Disaster Recovery Plan is invoked.

4.3 The Hosting Supplier shall provide the processes and procedures for reviewing, testing, changing and maintaining the Hosting ITSC Plan.

4.4 The Hosting ITSC Plan will be provided with the Hosting ITSCM Plan to the Authority.

4.5 The Hosting Supplier shall demonstrate Configuration Management of the Hosting ITSC Plan to the Authority and make the Hosting ITSC Plan available to the Authority within three (3) Working Days of request.

4.6 Upon the occurrence of a Critical Incident where the Hosting Supplier invokes the Hosting ITSC Plan the Hosting Supplier shall inform the Authority before it is invoked or as soon as practicable thereafter.

5. PART C – HOSTING DISASTER RECOVERY PLAN

5.1 The Hosting Supplier shall design the Hosting Disaster Recovery Plan which ensures that upon the occurrence of a Critical Incident:

5.1.1 the impacts on Hosting Supplier's business functions, operations and services are minimised; and

5.1.2 the impacts on the Authority, the Hosting Services and the FITS Services are minimised.

5.2 The Hosting Supplier shall inform the Authority as soon as practicable after invoking the Hosting Disaster Recovery Plan.

5.3 The Hosting Disaster Recovery Plan shall include, but not be limited to:

5.3.1 details of all processes and procedures to be put in place by the Hosting Supplier in relation to the provision of the Hosting Disaster Recovery and any testing of the same including but not limited to the following:

5.3.1.1 data centre and the Hosting Disaster Recovery site audits;

5.3.1.2 the methodology and details of the Hosting Supplier's approach to data availability and integrity;

5.3.1.3 identification of potential Critical Incidents;

5.3.1.4 Risk Analysis;

5.3.1.5 documentation of the processes and procedures;

5.3.1.6 hardware configuration details;

5.3.1.7 network planning including details of all relevant data networks and communication links;

5.3.1.8 rules governing the invocation of the Hosting Disaster Recovery Plan; and

5.3.1.9 the steps to be taken by the Hosting Supplier upon resumption of the services in order to address any prevailing effect or impact of the ITSC Event, including a root cause analysis and remediation plans.

5.4 Details of how the Hosting Supplier shall ensure compliance with Information Security Management standards as laid out in schedule 2.3 (Standards) and schedule 2.5 (Security Management Plan), where applicable, ensuring that compliance is maintained for any period during which the Hosting Disaster Recovery Plan is invoked.

5.5 The Hosting Supplier shall provide the processes and procedures for reviewing, testing, changing and maintaining the Hosting Disaster Recovery Plan.

5.6 The Hosting Disaster Recovery Plan will be provided with the Hosting ITSCM Plan to the Authority.

5.7 The Hosting Supplier shall demonstrate Configuration Management of the Hosting Disaster Recovery Plan to the Authority and make the Hosting Disaster Recovery Plan available to the Authority within three (3) Working Days of request.

6. REVIEW AND AMENDMENT OF THE HOSTING ITSCM PLAN, HOSTING ITSC PLAN(S) AND THE HOSTING DISASTER RECOVERY PLAN

6.1 The Hosting Supplier shall provide the processes and procedures for reviewing, testing, changing and maintaining the Hosting ITSCM Plan, Hosting ITSC Plans and the Hosting Disaster Recovery Plan.

6.2 The Hosting Supplier shall review and amend accordingly its Hosting ITSCM Plan, Hosting ITSC Plans and Business Continuity and the Hosting Disaster Recovery Plan:

6.2.1 on a regular basis and as a minimum annually;

6.2.2 within one calendar month of the Hosting ITSCM Plan, Hosting ITSC Plans and the Hosting Disaster Recovery Plan (or any part) having been invoked; and

6.2.3 following an annual review of the Authority's Business Continuity and the Hosting Disaster Recovery Plan or an ITSC impact assessment.

6.3 Any review by the Hosting Supplier of the Hosting ITSCM Plan, Hosting ITSC Plans and the Hosting Disaster Recovery Plan shall assess the suitability of the procedures and methodologies set out in the Hosting ITSCM Plan, Hosting ITSC Plans and the Hosting Disaster Recovery Plan. Each review shall take into account any changes to the Hosting Supplier’s business functions, operations, FITS Services and Hosting Services.

6.4 Any review shall be completed by the Hosting Supplier within the period specified in the Hosting ITSCM Plan or the processes and procedures for reviewing, testing, changing and maintaining the Hosting ITSCM Plan, Hosting ITSC Plan or the Hosting Disaster Recovery

Plan. The Hosting Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the Hosting ITSCM Plan, Hosting ITSC Plan or the Hosting Disaster Recovery Plan, provide to the Authority a report setting out:

6.4.1 the findings of the review;

6.4.2 any changes in the risk profile associated with the FITS Services and/or Hosting Services; and

6.4.3 the Hosting Supplier's proposals for addressing any changes in the risk profile and its proposals for amendments to the Hosting ITSCM Plan, Hosting ITSC Plan or the Hosting Disaster Recovery Plan following the review. It shall also detail the impact that the implementation of such proposals may have on any services or systems provided by any other party.

7. TESTING OF THE HOSTING ITSCM PLAN

7.1 The Hosting Supplier shall test the Hosting ITSCM Plan (excluding the Hosting Disaster Recovery Plan) on a regular basis, and in any event not less than once in every twelve (12) month period. The Authority or the SIAM Supplier may require the Hosting Supplier to conduct additional tests of some or all elements of the Hosting ITSCM Plan including where there has been any change to the Hosting Services, or on the occurrence of any event which may increase the likelihood of the need to implement the Hosting ITSCM Plan.

7.2 If the Authority or the SIAM Supplier requires an additional test of the Hosting ITSCM Plan it shall give the Hosting Supplier written notice and the Hosting Supplier shall conduct the test in accordance with the Authority's requirements or the SIAM Supplier's instructions and the relevant provisions of the Hosting ITSCM Plan.

7.3 The Hosting Supplier's costs of any additional test shall be borne by the Authority, unless the Hosting Supplier's test of the Hosting ITSCM Plan fails, in which case the Hosting Supplier shall retest the Hosting ITSCM Plan until successful completion at its own cost.

7.4 Following each test, the Hosting Supplier shall, within twenty (20) Working Days, send to the Authority for Approval a written report summarising the results of the test. This shall include, but not be limited to:

7.4.1 the outcome of the test;

7.4.2 any failures in the Hosting ITSCM Plan revealed by the test; and

7.4.3 the Hosting Supplier's proposals for remedying any such failures.

7.5 The Hosting Supplier shall implement any actions or remedial measures which the Authority has Approved.

7.6 The Hosting Supplier shall undertake and manage testing of the Hosting ITSCM Plan in 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 Authority's requirements in this regard.

7.7 Testing of the Hosting Disaster Recovery Plan will be carried out on an individual per Business Application basis and at the same time as an AMS Disaster Recovery Plan test for that Business Application.

7.8 The Authority shall provide a quarterly rolling plan of Business Applications it intends to be the subject of Disaster Recovery Plan testing. The Authority will provide at least three (3) month's written notice via the Change Control Procedure of a requirement to undertake a Disaster Recovery Plan test.

7.9 In each twelve (12) month period, the Hosting Supplier shall undertake one (1) Disaster Recovery Plan test for one (1) Business Application at no additional cost to the Authority. The Authority must submit a request via the Change Control Procedure confirming which Business Application it requires a Disaster Recovery Plan test for at no additional cost. Such Business Application may fall under any one of the categories listed at paragraph 7.11.

7.10 If the Authority requires additional Disaster Recovery Plan testing to that provided in paragraph 7.9, it will raise a Change Request via the Change Control Procedure and the activity will be chargeable in accordance with the Disaster Recovery Plan testing catalogue pricing in Schedule 7.5 (Financial Model).

7.11 The Business Applications in scope for a Disaster Recovery Plan test shall be limited to:

REDACTED

7.12 The following shall apply in respect of any Disaster Recovery Plan testing:

7.12.1 each of the above Business Applications shall not be subject to more than one Disaster Recovery Plan test in a twelve (12) month period;

7.12.2 only one Business Application Disaster Recovery Plan test will be undertaken at any one time unless otherwise agreed by the parties;

7.12.3 when scheduling a Disaster Recovery Plan test, the parties will seek to avoid scheduling these during the months of August and December, subject to the Authority's business need;

7.12.4 Disaster Recovery Plan testing shall not be undertaken for Business Applications that have been migrated out of the REDACTED Data Centre Facility; and

7.12.5 in the event the Authority requires a scheduled Disaster Recovery Plan test to be cancelled, it shall provide written notice at least 4 (four) Working Days in advance of the scheduled Disaster Recovery Plan test. Where the Authority does not provide notice in accordance with this paragraph 7.12.5, the Charges for such test that was scheduled to take place shall still be payable by the Authority.

7.13 REDACTED.

End of schedule