SCHEDULE 8.6

BUSINESS CONTINUITY AND DISASTER RECOVERY

SCHEDULE 8.6

BUSINESS CONTINUITY AND DISASTER RECOVERY

1 NOT USED

2 BCDRP

2.1 Within forty (40) Working Days from the Effective Date the Supplier shall prepare and deliver to the Authority for the Authority's written approval a plan, which shall detail the processes and arrangements that the Supplier shall follow to:

(a) ensure continuity of the business processes and operations supported by the Services following any failure or disruption of any element of the Services; and

(b) the recovery of the Services in the event of a Disaster.

2.2 The BCDRP shall:

(a) be divided into three (3) parts:

(i) Part A which shall set out general principles applicable to the BCDRP;

(ii) Part B which shall relate to business continuity (the **"Business Continuity Plan"**); and

(iii) Part C which shall relate to disaster recovery (the **"Disaster Recovery Plan"**).

(b) unless otherwise required by the Authority in writing, be based upon and be consistent with the provisions of Paragraphs 3, 4 and 5.

2.3 Following receipt of the draft BCDRP from the Supplier, the Authority shall:

(a) review and comment on the draft BCDRP as soon as reasonably practicable; and

(b) notify the Supplier in writing that it approves or rejects the draft BCDRP no later than twenty (20) Working Days after the date on which the draft BCDRP is first delivered to the Authority.

2.4 If the Authority rejects the draft BCDRP:

(a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and

(b) the Supplier shall then revise the draft BCDRP (taking reasonable account of the Authority's comments) and shall re-submit a revised draft BCDRP to the Authority for the Authority's approval within twenty (20) Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 2.3 and this Paragraph 2.4 shall apply again to any resubmitted

draft BCDRP, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

3 PART A OF THE BCDRP AND GENERAL PRINCIPLES AND REQUIREMENTS

3.1 Part A of the BCDRP shall:

(a) set out the Supplier's BCM Policy which it will apply in its delivery of the Services;

(b) set out how the business continuity and disaster recovery elements of the Plan link to each other;

(c) provide details of how the invocation of any element of the BCDRP may impact upon the operation of the Services and any services provided to the Authority by a Related Service Provider;

(d) contain an obligation upon the Supplier to liaise with the Authority and (at the Authority's request) any Related Service Provider with respect to issues concerning business continuity and disaster recovery where applicable;

(e) detail how the BCDRP links and interoperates with any overarching and/or connected disaster recovery or business continuity plan of the Authority and any of its other Related Service Providers in each case as notified to the Supplier by the Authority from time to time;

(f) contain a communication strategy including details of an incident and problem management service and advice and help desk facility which can be accessed via multi-channels (including but without limitation a web-site (with FAQs), e-mail, phone and fax) for both portable and desk top configurations, where required by the Authority;

(g) contain strategy options for the continued delivery of Services and activities under this Agreement to the Service Levels required in the event of incidents and business disruption including options in relation to:

(i) supplier personnel;

(ii) sites;

(iii) technology;

(iv) information and data; and

(v) supplies;

(h) contain a risk analysis including:

(i) failure or disruption scenarios and assessments and estimates of frequency of occurrence;

(ii) identification of any single points of failure within the Services and processes for managing the risks arising therefrom;

(iii) threat and risk analysis of the delivery of the overall Agreement and the Services delivered under this Agreement;

(iv) identification of risks arising from the interaction of the Services with the services provided by a Related Service Provider; and

(v) a business impact analysis (detailing the impact on business processes and operations) of different anticipated failures or disruptions; and identifying the Supplier's critical activities, Recovery Time Objectives and Maximum Tolerable Periods of disruption that will enable the Authority's Service Requirements to be met;

(i) provide for documentation of processes, including business processes, and procedures;

(j) set out key contact details (including roles and responsibilities) for the Supplier (and any Sub-contractors) and for the Authority;

(k) provide clear evidence that appropriate BCM Programme Management arrangements are in place throughout the Term and that key contacts and personnel assigned to BCM responsibilities under this Agreement are competent to perform the tasks to which they have been allocated, which may include evidence of membership of recognised Business Continuity organisations (such as the Business Continuity Institute);

(l) identify the procedures for reverting to "normal service";

(m) set out method(s) of recovering or updating data collected (or which ought to have been collected) during a failure or disruption to ensure that there is no more than the accepted amount of data loss and to preserve data integrity;

(n) identify the responsibilities (if any) that the Authority has agreed it will assume in the event of the invocation of the BCDRP; and

(o) 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 plans.

3.2 The BCDRP shall be designed so as to ensure that:

(a) the Services are provided in accordance with this Agreement at all times during and after the invocation of the BCDRP;

(b) the adverse impact of any Disaster, service failure, or disruption on the operations of the Authority is minimal as far as reasonably possible and the BCDRP provides the Authority with sufficient assurance that such events will be managed by the Supplier effectively;

(c) it complies with the relevant provisions of ISO/IEC 27002 and all other industry standards from time to time in force;

(d) there is a process for the management of disaster recovery testing detailed in the BCDRP;

(e) it is aligned to the Authority's standards for IT recovery;

(f) it is developed in accordance with the Authority's Business Continuity Framework; and

(g) it is developed in accordance with good industry practice and recognised industry standard guidelines.

3.3 The BCDRP shall be upgradeable and sufficiently flexible to support any changes to the Services or to the business processes facilitated by and the business operations supported by the Services.

3.4 The Supplier shall not be entitled to any relief from its obligations under the Performance Indicators or to any increase in the Charges to the extent that a Disaster occurs as a consequence of any breach by the Supplier of this Agreement.

4 BUSINESS CONTINUITY PLAN - PRINCIPLES AND CONTENTS

4.1 The Business Continuity Plan shall set out the arrangements that are to be invoked to ensure that the business processes and operations facilitated by the Services remain supported and to ensure continuity of the business operations supported by the Services including, unless the Authority expressly states otherwise in writing:

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

(b) 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.

4.2 The Business Continuity Plan shall:

(a) set out the purpose and scope of the plan;

(b) set out the strategic aims and objectives;

(c) define the roles and responsibilities of the Supplier Personnel;

(d) set out the recovery periods;

(e) clearly set out the communication arrangements including communications to Claimants, to the Authority and to any other relevant third parties;

(f) include a contact list and details of how the BCDRP will be flowed down and distributed to contacts;

(g) address the various possible levels of failures of or disruptions to the Services and the possible threats and contingency plans;

(h) clearly set out the plans for continuity and recovery in relation to the loss, failure or unavailability of services including:

(i) technology, personnel, telecommunications, Supplier equipment, Sites and Premises, Sub-Contractors, partners, other relevant third party suppliers, data and failure of the overall Services;

(i) provide details of how the security assets will be maintained;

(j) provide details of the clerical contingency arrangements that will be put in place for ensuring the continuity of all elements of the assessment Services (including Management Information) in the event of IT failure or unavailability;

(k) set out the services to be provided and the steps to be taken to remedy the different levels of failures of and disruption to the Services (such services and steps, the "**Business Continuity Services**");

(l) set out the processes in place to ensure minimum disruption to the Authority's required standard of Services in the event of a major system failure or building evacuation;

(m) specify any applicable Performance Indicators with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Business Continuity Plan; and

(n) clearly set out the conditions and/or circumstances under which the Business Continuity Plan is invoked.

5 DISASTER RECOVERY PLAN - PRINCIPLES AND CONTENTS

5.1 The Disaster Recovery Plan shall be designed so as to ensure that upon the occurrence of a Disaster the Supplier ensures continuity of the business operations of the Authority supported by the Services following any Disaster or during any period of service failure or disruption with, as far as reasonably possible, minimal adverse impact.

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

5.3 The Disaster Recovery Plan shall include the following:

(a) the technical design and build specification of the Disaster Recovery System;

(b) details of the procedures and processes to be put in place by the Supplier 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:

(i) data centre and disaster recovery site audits;

(ii) backup methodology and details of the Supplier's approach to data back-up and data verification;

(iii) identification of all potential disaster scenarios;

(iv) risk analysis;

(v) documentation of processes and procedures;

(vi) hardware configuration details;

(vii) network planning including details of all relevant data networks and communication links;

(viii) invocation rules;

(ix) Service recovery procedures; and

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

(c) any applicable Performance Indicators with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the Performance Indicators in respect of other Services during any period of invocation of the Disaster Recovery Plan;

(d) 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;

(e) access controls to any disaster recovery sites used by the Supplier in relation to its obligations pursuant to this Schedule; and

(f) testing and management arrangements.

6 REVIEW AND AMENDMENT OF THE BCDRP

6.1 The Supplier shall review the BCDRP (and the risk analysis on which it is based):

(a) on a regular basis and as a minimum once every six (6) Months;

(b) within three calendar months of the BCDRP (or any part) having been invoked pursuant to Paragraph 8; and

(c) where the Authority requests any additional reviews (over and above those provided for in Paragraphs 6.1(a) and 6.1(b)) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Authority's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Authority for the Authority's approval. The costs of both Parties of any such additional reviews shall be met by the Authority except that the Supplier shall not be entitled to charge the Authority for any costs that it may incur above any estimate without the Authority's prior written approval.

6.2 Each review of the BCDRP pursuant to Paragraph 6.1 shall be a review of the procedures and methodologies set out in the BCDRP, and shall assess their suitability having regard to any change to the Services or any underlying business processes and operations facilitated by or supported by the Services which have taken place since the later of the original approval of the BCDRP or the last review of the BCDRP 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 BCDRP. The review shall be completed by the Supplier within the period required by the BCDRP or, if no such period is required, within such period as the Authority shall reasonably require. The Supplier shall, within twenty (20) Working Days of the conclusion of each such review of the BCDRP, provide to the Authority a report (a **"Review Report"**) setting out:

(a) the findings of the review;

(b) any changes in the risk profile associated with the Services; and

(c) the Supplier's proposals (the **"Supplier's Proposals"**) for addressing any changes in the risk profile and its proposals for amendments to the BCDRP 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 a third party.

6.3 Following receipt of the Review Report and the Supplier's Proposals, the Authority shall:

(a) review and comment on the Review Report and the Supplier's Proposals as soon as reasonably practicable; and

(b) notify the Supplier in writing that it approves or rejects the Review Report and the Supplier's Proposals no later than twenty (20) Working Days after the date on which they are first delivered to the Authority.

6.4 If the Authority rejects the Review Report and/or the Supplier's Proposals:

(a) the Authority shall inform the Supplier in writing of its reasons for its rejection; and

(b) the Supplier shall then revise the Review Report and/or the Supplier's Proposals as the case may be (taking reasonable account of the Authority's comments and carrying out any necessary actions in connection with the revision) and shall re-submit a revised Review Report and/or revised Supplier's Proposals to the Authority for the Authority's approval within twenty (20) Working Days of the date of the Authority's notice of rejection. The provisions of Paragraph 6.3 and this Paragraph 6.4 shall apply again to any resubmitted Review Report and Supplier's Proposals, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

6.5 The Supplier shall as soon as is 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.

7 TESTING OF THE BCDRP

7.1 The Supplier shall test the BCDRP 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 BCDRP at any time where the Authority considers it necessary, including where there has been any change to the Services or any underlying business processes, or on the occurrence of any event which may increase the likelihood of the need to implement the BCDRP.

7.2 If the Authority requires an additional test of the BCDRP, 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 BCDRP. The Supplier's costs of the additional test shall be borne by the Authority unless the BCDRP fails the additional test in which case the Supplier's costs of that failed test shall be borne by the Supplier.

7.3 The Supplier shall undertake and manage testing of the BCDRP 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.

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

7.5 The Supplier shall, within twenty (20) Working Days of the conclusion of each test and each invocation of the BCDRP, provide to the Authority a report setting out:

(a) the outcome of the test;

(b) any failures in the BCDRP (including the BCDRP's procedures) revealed by the test;

(c) the Supplier's proposals for remedying any such failures; and

(d) a full report of the lessons learned and plans for improvement of the BCM Policy and BCDRP.

7.6 Following each test, the Supplier shall take all measures requested by the Authority (including requests for the re-testing of the BCDRP), and the Supplier shall set out its plan of action to remedy any failures in the BCDRP 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 notice.

7.7 The plans prepared by the Supplier pursuant to Paragraph 7.6 above shall include clearly assigned roles and responsibilities for action points, clear timescales and deadlines for completion and regular progress checks and updates.

7.8 For the avoidance of doubt, the carrying out of a test of the BCDRP (including a test of the BCDRP's procedures) shall not relieve the Supplier of any of its obligations under this Agreement.

7.9 The Supplier shall also perform a test of the BCDRP in the event of any major reconfiguration of the Services or as otherwise reasonably requested by the Authority.

8 INVOCATION OF THE BCDRP

In the event of a complete loss of service or in the event of a Disaster, the Supplier shall immediately invoke the BCDRP (and shall inform the Authority promptly of such invocation). In all other instances the Supplier shall invoke or test the BCDRP only with the prior consent of the Authority.

9 ASIS SERVICES

The Supplier shall, in addition to any other obligation in this Schedule, ensure that it has in place at all times contingency plans to enable Services to be provided (to the extent reasonably practicable) in the event of a failure of any relevant IT system, including a failure of the ASIS IT System.