2.7 Approval by the Customer of the ISMS pursuant to paragraph 2.6 or of any change or amendment to the ISMS shall not relieve the Supplier of its obligations under this Schedule.

3. SECURITY MANAGEMENT PLAN

3.1 Within 20 Working Days after the Call Off Commencement Date, the Supplier shall prepare and submit to the Customer for Approval in accordance with paragraph 3.3 a fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of paragraph 3.2.

3.2 The Security Management Plan shall:

3.1.1 be based on the initial Security Management Plan set out in Annex 2 (Security Management Plan);

3.1.2 comply with the Security Policy;

3.1.3 unless otherwise specified by the Customer in writing, be developed to protect all aspects of the Goods and all processes associated with the delivery of the Goods and/or Services, including the Customer Premises, the Sites, and any ICT, information and data (including the Customer's Confidential Information and the Customer Data) to the extent used by the Customer or the Supplier in connection with this Call Off Contract;

3.1.4 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Goods and all processes associated with the delivery of the Goods and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Goods comply with the provisions of this Call Off Schedule 8 (including the requirements set out in paragraph 2.3);

3.1.5 set out the plans for transiting all security arrangements and responsibilities from those in place at the Call Off Commencement Date to those incorporated in the Supplier's ISMS at the date set out in the Implementation Plan for the Supplier to meet the full obligations of the security requirements set out in Schedule Annex 1 (Security) to this Schedule 8.

3.1.6 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules which cover specific areas included within those standards; and

3.1.7 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Customer engaged in the Goods and shall reference only documents which are in the possession of the Customer or whose location is otherwise specified in this Call Off Schedule 8.

3.3 If the Security Management Plan submitted to the Customer pursuant to paragraph 3.1 is Approved by the Customer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Call Off Schedule 8. If the Security Management Plan is not approved by the Customer, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Customer and re-submit it to the Customer for Approval. The Parties shall use all

reasonable endeavours to ensure that the Approval process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the Parties may agree in writing) from the date of the first submission to the Customer of the Security Management Plan. If the Customer does not Approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No Approval to be given by the Customer pursuant to this Paragraph 3.3 may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 3.2 shall be deemed to be reasonable.

3.4 Approval by the Customer of the Security Management Plan pursuant to paragraph 3.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Call Off Schedule 8.

4. AMENDMENT AND REVISION OF THE ISMS AND SECURITY MANAGEMENT PLAN

4.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier from time to time and at least annually to reflect:

4.1.1 emerging changes in Good Industry Practice;

4.1.2 any change or proposed change to the Supplier System, the Goods and/or associated processes;

4.1.3 any new perceived or changed security threats; and

4.1.4 any reasonable request by the Customer.

4.2 The Supplier shall provide the Customer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Customer. The results of the review shall include, without limitation:

4.2.1 suggested improvements to the effectiveness of the ISMS;

4.2.2 updates to the risk assessments;

4.2.3 proposed modifications to the procedures and controls that effect information security to respond to events that may impact on the ISMS; and

4.2.4 suggested improvements in measuring the effectiveness of controls.

4.3 Subject to paragraph 4.4, any change or amendment which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to paragraph 4.1, a Customer request, change to Annex 1 (Security) or otherwise) shall be subject to the Variation Procedure and shall not be implemented until Approved in writing by the Customer.

4.4 The Customer may, where it is reasonable to do so, Approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Variation Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Variation Procedure for the

purposes of formalising and documenting the relevant change or amendment for the purposes of this Call Off Contract.

5. TESTING OF THE ISMS

5.1 The Supplier shall conduct tests of the ISMS ("Security Tests") from time to time and at least annually and additionally after any change or amendment to the ISMS or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Goods and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Customer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Goods so as to meet the Service Level Performance Measures, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

5.2 The Customer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Customer with the results of such Security Tests (in a form approved by the Customer in advance) as soon as practicable after completion of each Security Test.

5.3 Without prejudice to any other right of audit or access granted to the Customer pursuant to this Call Off Contract, the Customer and/or its authorised representatives shall be entitled, at any time by giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Customer may notify the Supplier of the results of such tests after completion of each such test.

5.4 Where any Security Test carried out pursuant to paragraphs 5.2 or 5.3 reveals any actual or potential breach of security, the Supplier shall promptly notify the Customer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Customer's prior written Approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Customer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or security requirements (as set out in Annex 1 (Security) to this Call Off Schedule 8) or the requirements of this Schedule 8, the change to the ISMS or Security Management Plan shall be at no cost to the Customer.

5.5 If any repeat Security Test carried out pursuant to paragraph 5.4 reveals an actual or potential breach of security exploiting the same root cause failure, such circumstance shall constitute a material Default of the Call Off contract.

6. COMPLIANCE OF THE ISMS WITH ISO/IEC 27001

6.1 The Customer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001.

6.2 If, on the basis of evidence provided by such security audits, it is the Customer's reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Supplier, then the Customer shall notify the Supplier of the same and give the Supplier a reasonable time (having regard to the extent and criticality of any non-compliance and any other relevant circumstances) to become compliant with the principles and practices of ISO/IEC 27001. If the Supplier does not become compliant within the required time then the Customer shall have the right to obtain an independent audit against these standards in whole or in part.

6.3 If, as a result of any such independent audit as described in paragraph 6.2 the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Customer in obtaining such audit.

7. BREACH OF SECURITY

7.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted breach of security.

7.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 7.1, the Supplier shall:

7.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Customer) necessary to:

a) remedy such breach of security or any potential or attempted breach of security or protect the integrity of the ISMS against any such breach of security or any potential or attempted breach of security; and

b) prevent a further breach of security or any potential or attempted breach of security in the future exploiting the same root cause failure; and

7.2.2 as soon as reasonably practicable provide to the Customer full details (using such reporting mechanism as defined by the ISMS) of the breach of security or the potential or attempted breach of security, including a root cause analysis where required by the Customer.

7.3 In the event that such action is taken in response to a breach of security or potential or attempted breach of security that demonstrates non-compliance of the ISMS with the Security Policy or security requirements (as set out in Annex 1 (Security) to this Call Off Schedule 8) or the requirements of this Call Off Schedule 8, then any required change to the ISMS shall be at no cost to the Customer.

11. Information Security Plan

DISCLAIMER

This document is confidential and exempt from disclosure under the Freedom of Information Act, unless the document is formally de-classified and / or redacted by the Equality Human Rights Commission.

INTRODUCTION

This Information Handling Agreement ("IHA") describes the minimum security controls necessary to ensure that both the EHRC (the "Commission") and PHOENIX SOFTWARE LTD (the "Supplier") complies with relevant operational, contractual and legal obligations for the protection and security of Commission assets, including information held on behalf of the Commission by the Supplier.

The Supplier acknowledges that the Commission is ultimately responsible for the protection and security of all information which the Supplier processes on its behalf.

ASSOCIATED READING

The following documents should be read in-conjunction with this Agreement.

- The Schedule 4 to the RM1054 Framework entitled Technology Product Order Form and Technology Product Call Off Terms ("Call Off Terms"),
- The Commission's requirements specification,
- Any additional information provided by the Supplier, describing the solution, its technical design, functionality and security arrangements.

SECURITY CONTROLS

The following security controls must be met by the Supplier to ensure the provision of service meets EHRC requirements.

1. **Definitions**

For the purposes of this IHA:

1.1 The term "Confidential Information" shall have the same meaning as defined at Schedule 1 to the Call Off Terms and this definition shall apply to all forms of information, including Personal Data and Sensitive Personal Data, processed by the Supplier or any sub-Supplier(s) appointed by the Supplier.

1.2 The terms "Personal Data" and "Sensitive Personal Data" shall have the same meaning as defined by the Data Protection Act 1998. For the purposes of this IHA, the Commission shall act in the capacity of the Data Controller and the Supplier, and any approved sub-Supplier(s), shall act in the capacity of a Data Processor.

2. **Governance and Incident Management**

The Supplier shall:

2.1 Appoint a named individual with responsibility for all aspects of information security in connection with this contract of work.

2.2 Retain a central log of all security related incidents concerning systems processing Confidential Information and be prepared to share statistical information with the Commission upon request.

2.3 Notify the Commission's primary contact within a reasonable time frame, of not longer than 1 working day, of any actual or suspected breach of security to the Confidential Information processed on behalf of the Commission.

2.4 Adopt commercial best practice IT tools and utilities in order to maintain accurate logs of all system operations and administrator access to any IT equipment used to process Confidential Information in relation to this contract.

2.5 Upon request, take reasonable measures to provide auditable information to the Commission within 5 working days from receipt of a written request.

3. **Personnel Vetting**

The Supplier shall:

3.1 The Supplier shall ensure all employees and individuals with access to Confidential Information have been appropriately vetted in-line with the HMG Baseline Personnel Security Standard, or equivalent measures, including checks for unspent criminal convictions. The Commission reserves the right to ask for evidence of such checks or undertake additional checks if it deems necessary to do so.

3.2 In the course of providing the Contracted Services the Supplier is not expected to undertake any activities requirement direct access to children or vulnerable adults. Where any such activity is deemed to be necessary the Supplier and the Commission will jointly agree the level of additional personnel vetting required before any such activity may commence.

4. **Confidential Information and Personal Data**

4.1 The Supplier and the Commission acknowledge that the scope of Personal Data processing in connection with this Contract shall not include the processing of Sensitive Personal Data as defined by the DPA.

4.2 The Supplier acknowledges that the Commission's Classification Scheme shall be used to assess the relative confidentiality of information assets. This scheme is based upon HMG's Classification Scheme ("GCS") as published by the Cabinet Office.

4.3 For the purpose of this IHA, the underpinning principles of the GCS shall prevail meaning that both parties shall apply to all information the protective controls commensurate with the OFFICIAL classification.

4.4 Should both Parties agree to Sensitive Personal Data processing then the Supplier shall apply the OFFICIAL-SENSITIVE marking to all information assets unless alternative measures are agreed in writing between the Commission and the Supplier.

4.5 Save for the processing of Sensitive Personal Data, neither party shall be required to include the classification marking on each page of information, but documents containing Confidential Information shall including appropriate wording to alert the reader to the fact they are handling confidential matter.

4.6 The Supplier confirms that all Confidential Information held in digital or hardcopy format, shall be processed using facilities and storage services located within the EU only. For the avoidance of doubt the Supplier shall not process Confidential Information outside the EU nor shall the Supplier use using public and \ or consumer-grade internet-based storage facilities.

5. **Data processing and systems security**

The Supplier shall:

5.1 Control access by its staff to Confidential Information on a strict "need to know" basis and extend this arrangement to any sub-contracted third parties.

5.2 Ensure that all processing of Confidential Information, whether in paper or electronic format, is suitably protected at all times using industry standard controls and procedures, including, but not limited to:

a. The provision at cost to the Supplier of proportionate physical security and IT security controls to reduce to acceptable levels any risks concerning unauthorised access, compromise, theft or loss of Confidential Information. The Commission reserves the right to ask for evidence of the security controls implemented by the Supplier and, as necessary, to undertake to audit the controls for adherence to this IHA and the Contract in general.

b. Suitable logon names and complex passwords for IT systems,

c. Public access computers or computers shared with family members shall not be used for the direct processing Confidential Information. For the avoidance of doubt, this clause does not apply where the host computer is configured as remote access terminal.

d. Data processed on laptops or portable equipment (e.g. tablets) shall be encrypted using Commercial Best Practice products and services. Wherever practicable the Commission prefers the Supplier to use services and products certified by CESG.

e. The application of security updates on at least a quarterly basis to all IT systems processing Confidential Information, or where such systems provide public-facing services.

f. Paper records and physical assets shall be locked away out of sight when not in use.

5.3 Refrain from transferring any Confidential Information to removable media (including CD\DVD, USB memory sticks) without prior written agreement from the Commission.

5.4 Be responsible for the procurement and implementation of any data backup and continuity facilities the Supplier deems necessary to maintain the operational integrity and availability of the information created during the course of the Contract.

5.5 Not transfer any OFFICAL-SENSITIVE information to the Commission or any sub-Supplier, individual or entity unless both the Supplier and the Commission agree in writing a) that such transfers are necessary; and b) the methods for the secure transfer of the data in question.

5.6 Transfer all Confidential Information rated at the OFFICAL classification in digital format using the following authorised methods only:

a. Email correspondence shall be to recognised business addresses of the Parties. Emails to EHRC must use the "@equalityhumanrights.com" domain.

b. Online storage facilities (e.g. cloud services and web portals) shall use strong encryption mechanisms (e.g. HTTPS or SFTP) to protect data in transit and whilst at rest. Security certificates used to encrypt and \ or authenticate access must be linked to a trusted External Certificate Authority. The Supplier shall provide the Commission with technical details describing the security controls for such services if requested by the Commission.

5.7 Ensure that any Confidential Information rated at the OFFICAL level transferred between the Supplier and the Commission in connection with the delivery of this contract and in hardcopy uses the methods detailed below:

a. Royal Mail First Class (or equivalent) shall be used for all general correspondence.

b. The envelope or outer wrapping shall be labelled "FOR ADDRESSEE ONLY" with the Supplier's return address visible on the reverse.

c. Courier packages shall be double-wrapped with the full name and address of the EHRC addressee clearly visible on both wrappings.

d. The Supplier shall be responsible for ensuring all packages are received by the EHRC addressee.

6. Retention

6.1 The Supplier shall retain all data for as long as is reasonably necessary up to a maximum period of 3 years commencing on completion of contractual activities, unless a different retention period is agreed in writing by both Parties. Upon reaching the retention period the Supplier shall apply the Disposal and Sanitisation controls described below.

7. Disposal and Sanitisation

The Supplier shall:

7.1 Be responsible for the secure disposal and sanitisation of all Confidential Information in their possession. It shall be the responsibility of the Supplier to conduct disposal and sanitisation activities when the Retention period has lapsed unless otherwise instructed by the Commission.

7.2 Identify and procure at cost to themselves the necessary products, tools and technologies to meet the disposal and sanitisation requirements. For the purposes of this Contract, the Commission agrees to the use of Commercial Best Practice tools and services for all data rated at the OFFICIAL level. For data rated at OFFICIAL-SENSITIVE the Supplier shall deploy appropriate disposal methods designed to significantly hinder any successful opportunistic reconstruction of the data.

7.3 Provide written confirmation of sanitisation to the EHRC upon request.

8. Additional requirements

8.1 The Supplier shall reciprocate the controls documented herein with any sub-Supplier it engages with the prior written approval of the EHRC in connection with the delivery of services to the EHRC.

COMPLIANCE STATEMENT

By signing the Call Off Terms the Supplier's signatory confirms that:

8.2 The controls described in this IHA have been implemented, and that their importance has been drawn to the attention of those involved in the delivery of services to the EHRC.

8.3 Compliance shall be maintained until the Confidential Information has been disposed.

8.4 If there are requirements that cannot be complied with, then the Supplier will highlight the matter to the EHRC as soon as is practically possible.

CALL OFF SCHEDULE 9: THIRD PARTY SOFTWARE

1. THIRD PARTY SOFTWARE

NOT APPLICABLE

[CALL OFF SCHEDULE 10: BUSINESS CONTINUITY AND DISASTER RECOVERY] – NOT APPLICABLE

[OPTION 1]

CUSTOMER BCDR REQUIREMENTS

[ ]

SUPPLIER BCDR PLAN

[ ]

]OPTION 2]

1. Definitions

1.1 In this Call Off Schedule 10, the following definitions shall apply:

"Business Continuity Plan"	has the meaning given in paragraph 2.2.1.1 of Call Off Schedule 10 (Business Continuity and Disaster Recovery);
"Business Continuity Services"	has the meaning given in paragraph 4.2.2
"Disaster Recovery Plan"	has the meaning 2.2.1.3 of Schedule 10 (Business Continuity and Disaster Recovery);
"Disaster Recovery Services"	the services embodied in the processes and procedures for restoring the Services following the occurrence of a disaster;
"Disaster Recovery System"	the system embodied in the processes and procedures for restoring the provision of Goods following the occurrence of a disaster s;
Review Report	has the meaning as set out in Paragraph 6.2;
Supplier's Proposals	has the meaning as set out in Paragraph 6.2.3;

2. BCDR PLAN

2.1 Within [30] Working Days from the Call Off Commencement Date the Supplier shall prepare and deliver to the Customer for the Customer's written approval a plan, which shall detail the processes and arrangements that the Supplier shall follow to:

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

2.1.2 the recovery of the Services in the event of a Disaster.

2.2 The BCDR Plan shall:

2.2.1 be divided into three parts:

a) Part A which shall set out general principles applicable to the BCDR Plan;

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

c) Part C which shall relate to disaster recovery (the "Disaster Recovery Plan"); and

2.2.2 unless otherwise required by the Customer in writing, be based upon and be consistent with the provisions of Paragraphs 3, 4 and 5.

2.3 Following receipt of the draft BCDR Plan from the Supplier, the Customer shall:

2.3.1 review and comment on the draft BCDR Plan as soon as reasonably practicable; and

2.3.2 notify the Supplier in writing that it approves or rejects the draft BCDR Plan no later than 20 Working Days after the date on which the draft BCDR Plan is first delivered to the Customer.

2.4 If the Customer rejects the draft BCDR Plan:

2.4.1 the Customer shall inform the Supplier in writing of its reasons for its rejection; and

2.4.2 the Supplier shall then revise the draft BCDR Plan (taking reasonable account of the Customer's comments) and shall re-submit a revised draft BCDR Plan to the Customer for the Customer's approval within 20 Working Days of the date of the Customer's notice of rejection. The provisions of paragraph 2.3 and this paragraph 2.4 shall apply again to any resubmitted draft BCDR Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

3. PART A OF THE BCDR PLAN AND GENERAL PRINCIPLES AND REQUIREMENTS

3.1 Part A of the BCDR Plan shall:

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

3.1.2 provide details of how the invocation of any element of the BCDR Plan may impact upon the operation of the Services and any services provided to the Customer by a Related Supplier;

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

3.1.4 detail how the BCDR Plan links and interoperates with any overarching and/or connected disaster recovery or business continuity plan of the Customer and any of its other Related

Supplier in each case as notified to the Supplier by the Customer from time to time;

3.1.5 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 Customer;

3.1.6 contain a risk analysis, including:

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

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

c) identification of risks arising from the interaction of the Services with the services provided by a Related Supplier; and

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

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

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

3.1.9 identify the procedures for reverting to "normal service";

3.1.10 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;

3.1.11 identify the responsibilities (if any) that the Customer has agreed it will assume in the event of the invocation of the BCDR Plan; and

3.1.12 provide for the provision of technical advice and assistance to key contacts at the Customer as notified by the Customer from time to time to inform decisions in support of the Customer's business continuity plans.

3.2 The BCDR Plan shall be designed so as to ensure that:

3.2.1 the Services are provided in accordance with this Call Off Contract at all times during and after the invocation of the BCDR Plan;

3.2.2 the adverse impact of any Disaster, service failure, or disruption on the operations of the Customer is minimal as far as reasonably possible;

3.2.3 it complies with the relevant provisions of [ISO/IEC 27002] and all other industry standards from time to time in force; and

3.2.4 there is a process for the management of disaster recovery testing detailed in the BCDR Plan.

3.3 The BCDR Plan 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 Service Levels 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 Call Off Contract.

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 Customer expressly states otherwise in writing:

4.1.1 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

4.1.2 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:

4.2.1 address the various possible levels of failures of or disruptions to the Services;

4.2.2 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");

4.2.3 specify any applicable Service Levels with respect to the provision of the Business Continuity Services and details of any agreed relaxation to the Service Levels in respect of other Services during any period of invocation of the Business Continuity Plan; and

4.2.4 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 Customer 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:

5.3.1 the technical design and build specification of the Disaster Recovery System;

5.3.2 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:

a) (data centre and disaster recovery site audits;

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

c) identification of all potential disaster scenarios;

d) risk analysis;

e) documentation of processes and procedures;

f) hardware configuration details;

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

h) invocation rules;

i) Service recovery procedures; and

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

5.3.3 any applicable Service Levels with respect to the provision of the Disaster Recovery Services and details of any agreed relaxation to the Service Levels in respect of other Services during any period of invocation of the Disaster Recovery Plan;

5.3.4 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;

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

5.3.6 testing and management arrangements.

6. REVIEW AND AMENDMENT OF THE BCDR PLAN

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

6.1.1 on a regular basis and as a minimum once every 6 months;

6.1.2 within three (3) calendar months of the BCDR Plan (or any part) having been invoked pursuant to Paragraph 7; and

6.1.3 where the Customer requests any additional reviews (over and above those provided for in Paragraphs 6.1.1 and 6.1.2) by notifying the Supplier to such effect in writing, whereupon the Supplier shall conduct such reviews in accordance with the Customer's written requirements. Prior to starting its review, the Supplier shall provide an accurate written estimate of the total costs payable by the Customer for the Customer's approval. The costs of both Parties of any such additional reviews shall be met

by the Customer except that the Supplier shall not be entitled to charge the Customer for any costs that it may incur above any estimate without the Customer's prior written approval.

6.2 Each review of the BCDR Plan pursuant to Paragraph 6.1 shall be a review of the procedures and methodologies set out in the BCDR Plan 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 BCDR Plan or the last review of the BCDR 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 BCDR Plan. The review shall be completed by the Supplier within the period required by the BCDR Plan or, if no such period is required, within such period as the Customer shall reasonably require. The Supplier shall, within 20 Working Days of the conclusion of each such review of the BCDR Plan, provide to the Customer a report (a "Review Report") setting out:

6.2.1 the findings of the review;

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

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

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

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

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

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

6.4.1 the Customer shall inform the Supplier in writing of its reasons for its rejection; and

6.4.2 the Supplier shall then revise the Review Report and/or the Supplier's Proposals as the case may be (taking reasonable account of the Customer'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 Customer for the Customer's approval within 20 Working Days of the date of the Customer'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 Customer'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 BCDR PLAN

7.1 The Supplier shall test the BCDR Plan on a regular basis (and in any event not less than once in every Contract Year). Subject to Paragraph 7.2, the Customer may require the Supplier to conduct additional tests of some or all aspects of the BCDR Plan at any time where the Customer 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 BCDR Plan.

7.2 If the Customer requires an additional test of the BCDR Plan, it shall give the Supplier written notice and the Supplier shall conduct the test in accordance with the Customer's requirements and the relevant provisions of the BCDR Plan. The Supplier's costs of the additional test shall be borne by the Customer unless the BCDR Plan 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 BCDR Plan in full consultation with the Customer and shall liaise with the Customer in respect of the planning, performance, and review, of each test, and shall comply with the reasonable requirements of the Customer in this regard. Each test shall be carried out under the supervision of the Customer 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 Customer. Copies of live test data used in any such testing shall be (if so required by the Customer) destroyed or returned to the Customer on completion of the test.

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

7.5.1 the outcome of the test;

7.5.2 any failures in the BCDR Plan (including the BCDR Plan's procedures) revealed by the test; and

7.5.3 the Supplier's proposals for remedying any such failures.

7.6 Following each test, the Supplier shall take all measures requested by the Customer, (including requests for the re-testing of the BCDR Plan) to remedy any failures in the BCDR Plan and such remedial activity and re-testing shall be completed by the Supplier, at no additional cost to the Customer, by the date reasonably required by the Customer and set out in such notice.

7.7 For the avoidance of doubt, the carrying out of a test of the BCDR Plan (including a test of the BCDR Plan's procedures) shall not relieve the Supplier of any of its obligations under this Call Off Contract.

7.8 The Supplier shall also perform a test of the BCDR Plan in the event of any major reconfiguration of the Services or as otherwise reasonably requested by the Customer.

8. INVOCATION OF THE BCDR PLAN

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

CALL OFF SCHEDULE 11: EXIT MANAGEMENT – NOT APPLICABLE

1. DEFINITIONS

1.1 In this Call Off Schedule, the following definitions shall apply:

"Exclusive Assets"	those Supplier Assets used by the Supplier or a Key Sub-Contractor which are used exclusively in the provision of the Services;
"Exit Information"	has the meaning given to it in paragraph 1;
"Exit Manager"	the person appointed by each Party pursuant to paragraph 3.3 for managing the Parties' respective obligations under this Call Off Schedule;
"Net Book Value"	the net book value of the relevant Supplier Asset(s) calculated in accordance with the depreciation policy of the Supplier set out in the letter in the agreed form from the Supplier to the Costumer of even date with this Call Off Contract;
"Non-Exclusive Assets"	those Supplier Assets (if any) which are used by the Supplier or a Key Sub-Contractor in connection with the Services but which are also used by the Supplier or Key Sub-Contractor for other purposes;
"Registers"	the register and configuration database referred to in paragraphs 3.1.1 and 3.1.2;
"Termination Assistance"	the activities to be performed by the Supplier pursuant to the Exit Plan, and any other assistance required by the Customer pursuant to the Termination Assistance Notice;
"Termination Assistance Notice"	has the meaning given in paragraph 1;
"Termination Assistance Notice Period"	in relation to a Termination Assistance Notice, the period specified in the Termination Assistance Notice for which the Supplier is required to provide the Termination Assistance as such period may be extended pursuant to paragraph 6.2;
"Transferable Assets"	those of the Exclusive Assets which are capable of legal transfer to the Customer;
"Transferable Contracts"	the Sub-contracts, licences for Supplier's Software, licences for Third Party Software or other agreements which are

	necessary to enable the Customer or any Replacement Supplier to perform the Services or the Replacement Services, including in relation to licences all relevant Documentation;
"Transferring Assets"	has the meaning given to it in paragraph 9.2.1;
"Transferring Contracts"	has the meaning given to it in paragraph 9.2.3.

2. INTRODUCTION

2.1 This Call Off Schedule describes provisions that should be included in the Exit Plan, the duties and responsibilities of the Supplier to the Customer leading up to and covering the Call Off Expiry Date and the transfer of service provision to the Customer and/or a Replacement Supplier.

2.2 The objectives of the exit planning and service transfer arrangements are to ensure a smooth transition of the availability of the Services from the Supplier to the Customer and/or a Replacement Supplier at the Call Off Expiry Date.

3. OBLIGATIONS DURING THE CALL OFF CONTRACT PERIOD TO FACILITATE EXIT

3.1 During the Call Off Contract Period, the Supplier shall:

3.1.1 create and maintain a Register of all:

a) Supplier Assets, detailing their:

i. make, model and asset number;

ii. ownership and status as either Exclusive Assets or Non-Exclusive Assets;

iii. Net Book Value;

iv. condition and physical location; and

v. use (including technical specifications); and

b) Sub-Contracts and other relevant agreements (including relevant software licences, maintenance and support agreements and equipment rental and lease agreements) required for the performance of the Services;

3.1.2 create and maintain a configuration database detailing the technical infrastructure and operating procedures through which the Supplier provides the Services, which shall contain sufficient detail to permit the Customer and/or Replacement Supplier to understand how the Supplier provides the Services and to enable the smooth transition of the Services with the minimum of disruption;

3.1.3 agree the format of the Registers with the Customer as part of the process of agreeing the Exit Plan; and

3.1.4 at all times keep the Registers up to date, in particular in the event that Assets, Sub-Contracts or other relevant agreements are added to or removed from the Services.

3.2 The Supplier shall:

3.2.1 procure that all Exclusive Assets listed in the Registers are clearly marked to identify that they are exclusively used for the provision of the Services under this Call Off Contract.

3.3 Each Party shall appoint a person for the purposes of managing the Parties' respective obligations under this Call Off Schedule and provide written notification of such appointment to the other Party within three (3) months of the Call Off Commencement Date. The Supplier's Exit Manager shall be responsible for ensuring that the Supplier and its employees, agents and Sub-Contractors comply with this Call Off Schedule. The Supplier shall ensure that its Exit Manager has the requisite Customer to arrange and procure any resources of the Supplier as are reasonably necessary to enable the Supplier to comply with the requirements set out in this Call Off Schedule. The Parties' Exit Managers will liaise with one another in relation to all issues relevant to the termination of this Call Off Contract and all matters connected with this Call Off Schedule and each Party's compliance with it.

4. OBLIGATIONS TO ASSIST ON RE-TENDERING OF SERVICES

4.1 On reasonable notice at any point during the Call Off Contract Period, the Supplier shall provide to the Customer and/or its potential Replacement Suppliers (subject to the potential Replacement Suppliers entering into reasonable written confidentiality undertakings), the following material and information in order to facilitate the preparation by the Customer of any invitation to tender and/or to facilitate any potential Replacement Suppliers undertaking due diligence:

4.1.1 details of the Service(s);

4.1.2 a copy of the Registers, updated by the Supplier up to the date of delivery of such Registers;

4.1.3 an inventory of Customer Data in the Supplier's possession or control;

4.1.4 details of any key terms of any third party contracts and licences, particularly as regards charges, termination, assignment and novation;

4.1.5 a list of on-going and/or threatened disputes in relation to the provision of the Services;

4.1.6 all information relating to Transferring Supplier Employees required to be provided by the Supplier under this Call Off Contract; and

4.1.7 such other material and information as the Customer shall reasonably require,

(together, the "Exit Information").

4.2 The Supplier acknowledges that the Customer may disclose the Supplier's Confidential Information to an actual or prospective Replacement Supplier or any third party whom the Customer is

considering engaging to the extent that such disclosure is necessary in connection with such engagement (except that the Customer may not under this paragraph 4.2 disclose any Supplier's Confidential Information which is information relating to the Supplier's or its Sub-contractors' prices or costs).

4.3 The Supplier shall:

4.3.1 notify the Customer within five (5) Working Days of any material change to the Exit Information which may adversely impact upon the provision of any Services and shall consult with the Customer regarding such proposed material changes; and

4.3.2 provide complete updates of the Exit Information on an as-requested basis as soon as reasonably practicable and in any event within ten (10) Working Days of a request in writing from the Customer.

4.4 The Supplier may charge the Customer for its reasonable additional costs to the extent the Customer requests more than four (4) updates in any six (6) month period.

4.5 The Exit Information shall be accurate and complete in all material respects and the level of detail to be provided by the Supplier shall be such as would be reasonably necessary to enable a third party to:

4.5.1 prepare an informed offer for those Services; and

4.5.2 not be disadvantaged in any subsequent procurement process compared to the Supplier (if the Supplier is invited to participate).

5. EXIT PLAN

5.1 The Supplier shall, within three (3) months after the Call Off Commencement Date, deliver to the Customer an Exit Plan which:

5.1.1 sets out the Supplier's proposed methodology for achieving an orderly transition of the Services from the Supplier to the Customer and/or its Replacement Supplier on the expiry or termination of this Call Off Contract;

5.1.2 complies with the requirements set out in paragraph 5.3;

5.1.3 is otherwise reasonably satisfactory to the Customer.

5.2 The Parties shall use reasonable endeavours to agree the contents of the Exit Plan. If the Parties are unable to agree the contents of the Exit Plan within twenty (20) Working Days of its submission, then such Dispute shall be resolved in accordance with the Dispute Resolution Procedure.

5.3 Unless otherwise specified by the Customer or Approved, the Exit Plan shall set out, as a minimum:

5.3.1 how the Exit Information is obtained;

5.3.2 the management structure to be employed during both transfer and cessation of the Services;

5.3.3 the management structure to be employed during the Termination Assistance Period;

5.3.4 a detailed description of both the transfer and cessation processes, including a timetable;

5.3.5 how the Services will transfer to the Replacement Supplier and/or the Customer, including details of the processes, documentation, data transfer, systems migration, security and the segregation of the Customer's technology components from any technology components operated by the Supplier or its Sub-Contractors (where applicable);

5.3.6 details of contracts (if any) which will be available for transfer to the Customer and/or the Replacement Supplier upon the Call Off Expiry Date together with any reasonable costs required to effect such transfer (and the Supplier agrees that all Transferable Assets and Transferable Contracts used by the Supplier in connection with the provision of the Goods and/or Services will be available for such transfer);

5.3.7 proposals for the training of key members of the Replacement Supplier's personnel in connection with the continuation of the provision of the Services following the Call Off Expiry Date charged at rates agreed between the Parties at that time;

5.3.8 proposals for providing the Customer or a Replacement Supplier copies of all documentation:

a) used in the provision of the Services and necessarily required for the continued use thereof, in which the Intellectual Property Rights are owned by the Supplier; and

b) relating to the use and operation of the Services;

5.3.9 proposals for the assignment or novation of the provision of all services, leases, maintenance agreements and support agreements utilised by the Supplier in connection with the performance of the supply of the Services;

5.3.10 proposals for the identification and return of all Customer Property in the possession of and/or control of the Supplier or any third party (including any Sub-Contractor);

5.3.11 proposals for the disposal of any redundant Services and materials;

5.3.12 procedures to deal with requests made by the Customer and/or a Replacement Supplier for Staffing Information pursuant to Call Off Schedule 12 (Staff Transfer);

5.3.13 how each of the issues set out in this Call Off Schedule will be addressed to facilitate the transition of the Services from the Supplier to the Replacement Supplier and/or the Customer with the aim of ensuring that there is no disruption to or degradation of the Services during the Termination Assistance Period; and

5.3.14 proposals for the supply of any other information or assistance reasonably required by the Customer or a Replacement Supplier in order to effect an orderly handover of the provision of the Services.

6. TERMINATION ASSISTANCE

6.1 The Customer shall be entitled to require the provision of Termination Assistance at any time during the Call Off Contract Period by giving written notice to the Supplier (a **"Termination Assistance Notice"**) at