Crown Hosting Framework Agreement

Schedule 3.6

Security Management

1. Introduction

1.1 This Schedule covers:

(a) principles of protective security to be applied by the Supplier in performing its obligations under this Framework Agreement and any Call-Off Agreement and in delivering any of the Services;

(b) the creation and maintenance of the Security Management Plan; and

(c) obligations in the event of actual, potential or attempted Breaches of Security.

2. Principles of Security

2.1 The Parties shall provide a reasonable level of access to any members of their personnel for the purposes of designing, implementing, operating, managing and continually improving security.

2.2 The Supplier shall use, as a minimum, Good Industry Practice in the day to day provision of the Services and the operation of the Data Centres.

2.3 Subject to Clause 17 (Change in Standards) of the Framework Agreement, the references to standards, guidance and policies set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, from time to time.

2.4 In the event that the Supplier becomes aware of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier shall immediately notify the Framework Authority of such inconsistency immediately upon becoming aware of the same, and the Framework Authority shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with and any Framework Contract Changes and/or changes to the Call-Off Agreements shall be made in accordance with the Change Control Procedure.

2.5 The Supplier shall at all times comply with the Minimum Security Requirements set out in Annex 1 of this Schedule.

3. Security Management Plan

3.1 Within 20 Working Days after the Framework Effective Date, the Supplier shall prepare and submit to the Framework Authority 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:

(a) be based on the initial Security Management Plan set out in Annex 2 of this Schedule;

(b) comply with the Minimum Security Requirements set out in Annex 1 of this Schedule;

(c) identify the necessary delegated organisational roles defined for those responsible for ensuring this Schedule is complied with by the Supplier;

(d) detail the process for managing any security risks from Sub-contractors and third parties authorised by the Framework Authority with access to the Services, processes associated with the delivery of the Services and the Data Centres and any IT, Information and data (including Customer Stored Data, the Framework Authority Confidential Information and the Framework Authority Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

(e) unless otherwise specified by the Framework Authority in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Data Centres, and any IT, Information and data (including Customer Stored Data, the Framework Authority Confidential Information and the Framework Authority Data) to the extent used by the Framework Authority, any Customer or Service Recipient or the Supplier in connection with this Framework Agreement or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services; and

(f) set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Schedule.

3.3 If the Security Management Plan submitted to the Framework Authority pursuant to paragraph 3.1 is approved by the Framework Authority, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Schedule. If the Security Management Plan is not approved by the Framework Authority, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Framework Authority and re-submit it to the Framework Authority 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 its first submission to the Framework Authority. If the Framework Authority 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 Framework Authority 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 Framework Authority 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 Schedule.

4. Amendment and Revision of the Security Management Plan

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

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the IT Environment, the Services and/or associated processes;

(c) any new perceived or changed security threats; and

(d) any reasonable request by the Framework Authority.

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

(a) updates to the risk assessments; and

(b) suggested improvements in measuring the effectiveness of controls.

4.3 Subject to paragraph 4.4, any change which the Supplier proposes to make to the Security Management Plan shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Framework Authority.

4.4 The Framework Authority may, where it is reasonable to do so, approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment for the purposes of this Framework Agreement.

5. **Breach of Security – General Principles**

5.1 Either Party shall notify the other Party and the relevant Customer(s) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security of which it becomes aware.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 5.1, the Supplier shall:

(a) immediately take all reasonable steps necessary to:

(i) remedy such Breach of Security or protect the Services and Data Centre against any such potential or attempted Breach of Security; and

(ii) prevent an equivalent Breach of Security in the future.

Such steps shall include any action or changes reasonably required by the Framework Authority. In the event that such action is taken in response to any actual, potential or attempted Breach of Security that is determined by the Framework Authority, acting reasonably, not to be covered by the obligations of the Supplier under this Framework Agreement or any Call-Off Agreement (as applicable), then the Supplier shall be entitled to refer the matter to the Change Control Procedure or the change control procedure under that Call-Off Agreement; and

(b) as soon as reasonably practicable following the Breach of Security or the potential or attempted Breach of Security, provide to the Framework Authority and the relevant Customer(s) full details of the Breach of Security or the potential or attempted Breach of Security.

Annex 1

REDACTED

Annex 2

Security Management Plan