SCHEDULE 6

SECURITY MANAGEMENT PLAN

# INTRODUCTION

## This Schedule 6 covers:

### principles of protective security to be applied in delivering the Services;

### the creation and maintenance of the Security Management Plan;

### the implementation, operation, testing and audit of Sub-Contractors’ ISMS in respect of the Services, which shall form part of the Security Management Plan;

### obligations in the event of actual, potential or attempted Breaches of Security.

# PRINCIPLES OF SECURITY

## The Supplier acknowledges that the Authority places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the Security Management Plan.

## Notwithstanding any approval provided by the Authority hereunder the Supplier shall be responsible for the effective performance of the Security Management Plan and shall (and shall procure that its Sub-Contractors shall) at all times provide a level of security in respect of the Services and generally in connection with the agreement which:

### is in accordance with Best Industry Practice, all applicable Laws and complies with the security requirements set out in this agreement;

### complies with the minimum set of security measures and standards as determined by the HMG Security Policy Framework (as detailed in schedule 4 (Standards) and/or as published by the Cabinet Office on the [www.gov.uk](http://www.gov.uk) website);

### meets any specific security threats to the provision of the Services and/or any ISMS;

### complies with the Security Requirements and the Specification as it relates to security;

### reflects that the Sub-Contractors responsible for supporting the delivery of the Services comply with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 5 of this schedule; and

## The references to standards, guidance and policies set out in paragraph 2.2 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.

## In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Authority’s Authorised Representative of such inconsistency immediately upon becoming aware of the same, and the Authority’s Authorised Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

# CONTENT AND APPROVAL OF THE ISMS

## **Introduction**

### The Supplier shall:

#### comply with its obligations set out in the Security Management Plan; and

#### include within the Security Management Plan an ISMS provided by the respective Sub-Contractor responsible for supporting the delivery of the Services in accordance with the requirements of this schedule and the Security Management Plan.

### The Security Management Plan (including each respective Sub-Contractor ISMS) shall, unless otherwise specified by the Authority, aim to protect all aspects of the Services and all processes associated with the delivery of the Services, (including the Authority’s Confidential Information and Authority Data) by preventing any Breaches of Security from occurring.

## **Development of the Security Management Plan**

### The Supplier shall maintain a fully complete and up-to-date Security Management Plan in accordance with the requirements of this schedule.

### No later than the date specified in the Implementation Timetable, the Supplier shall prepare and deliver to the Authority for approval in accordance with the Plan Approval Process a detailed Security Management Plan (based on and be consistent with the outline Security Management Plan). For the avoidance of doubt, in no circumstances may the Security Management Plan place upon the Authority any additional responsibilities and/or compel the Authority to accept risks not envisaged and documented in the Agreement as at the Commencement Date. Once agreed the detailed Security Management Plan shall be adopted immediately.

### The Supplier shall prepare and deliver updates to the Security Management Plan to the Authority for approval in accordance with this schedule 6.

### If any revision to the Security Management Plan is approved by the Authority it will be adopted immediately and will replace the previous version of the Security Management Plan.

### If any revision to the Security Management Plan is not approved by the Authority, the Supplier shall amend it within 10 Working Days of a notice of non-approval from the Authority to reflect the Authority’s comments and re-submit it to the Authority for approval.

### The parties will ensure that the approval process in respect of the Security Management Plan takes as little time as possible and no longer than fifteen (15) Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the Authority. If the Authority does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

### The Authority shall not unreasonably withhold or delay any approval required of it pursuant to this paragraph 3.2. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements of this agreement shall be deemed to be reasonable.

## **Content of the Security Management Plan**

### The Security Management Plan shall set out:

#### the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services (including all security measures relevant to specific locations from which the Services are delivered) and all processes associated with the delivery of the Services;

#### a mechanism and schedule for the testing of the Security Management Plan;

#### full details of the ISMS that has been included within the Security Management Plan in respect of those elements of the Services provided by Sub-Contractors; and

#### details of the proposed security and information assurance solution tests that shall be carried out during the implementation of the Services.

### The Security Management Plan shall include the Supplier's approach to:

#### the categorisation of security incidents and/or events;

#### the appropriate logging and audit trails required for Authority Data, the Authority’s Confidential Information and Personal Data;

#### the encryption procedures to apply and the tools to be used in all circumstances in which encryption in required and the related encryption key management;

#### vulnerability and penetration testing;

#### the specification of data types and formats that will require digital signatures; and

#### how Authority Data, the Authority’s Confidential Information and Personal Data will be classified and handled in line with existing classification and handling procedures.

### The Security Management Plan will be structured in accordance with ISO/IEC 27001 and ISO/IEC 27002, cross-referencing if necessary to other schedules of this agreement which cover specific areas included within the applicable standard.

### The Security Management Plan shall be written in plain English in language which is readily comprehensible to the Supplier’s Personnel and the Authority’s staff engaged in the Services, and shall only reference documents which are in the possession of the Authority or whose location is otherwise specified in this schedule.

## **Content and approval of the ISMS**

### The Supplier shall procure that Sub-Contractors responsible for supporting the delivery of the Services provide an ISMS that shall:

#### be subject to approval by the Authority as part of the approval of the Security Management Plan;

#### be tested by the relevant Sub-Contractor pursuant to paragraph 4; and

#### be periodically updated and audited by the relevant Sub-Contractor in accordance with ISO/IEC 27001;

### The Supplier shall procure that each Sub-Contractor’s ISMS shall include:

#### the security controls and mitigating solutions to be implemented and maintained by the Supplier in relation to the security and information assurance of the Services and all processes associated with the delivery of the Services;

#### documentation and evidence setting out the process for the implementation of the control objectives and the implementation of the ISMS;

#### the results of reviews in accordance with the monitoring and reviewing procedures;

#### the results of the first and most recent risk assessment(s);

#### the results of the first and most recent ISMS audit(s);

#### the ISMS documentation mandated by the ISO 27001 Standard; and

#### an agreed reporting route and defined process to follow when a Breach of Security (e.g. data loss or compromise) has occurred.

### The Supplier shall procure that the ISMS shall contain processes and procedures acceptable to the Authority (and shall at the request of the Authority provide to the Authority evidence of the same) that implement the required controls to prevent:

#### loss or corruption of Authority Data and which preserve the integrity of Authority Data;

#### unauthorised access to and unauthorised disclosure and use of Authority Data and the Authority’s Confidential Information; and

#### loss of availability of the Services and the Supplied System.

## **Amendment and Revision of the Security Management Plan**

### The Security Management Plan will be fully reviewed and updated by the Supplier annually, or on such shorter periods as may be required, to reflect:

#### emerging changes in Best Industry Practice;

#### any change or proposed change to the Supplied System, the Services, the premises of the Authority and the Supplier, and/or associated processes;

#### any change or proposed change to the Security Requirements;

#### any new perceived or changed security threats; and

#### any reasonable request by the Authority.

### The Supplier will provide the Authority with the results of the reviews carried out in accordance with paragraph 3.5.1 as soon as reasonably practicable after their completion and amend the Security Management Plan at no additional cost to the Authority. The results of such review shall include, without limitation:

#### suggested improvements to the effectiveness of the Security Management Plan;

#### updates to the risk assessments contained within the Security Management Plan;

#### proposed modifications to the procedures and controls that effect information security in response to any events which may impact the Security Management Plan; and

#### suggested improvements for measuring the effectiveness of controls.

### On receipt of the results of such reviews, the Authority will approve any amendments or revisions to the Security Management Plan in accordance with the process set out in paragraph 3.2.

### Any change or amendment which the Supplier proposes to make to the Security Management Plan other than those required pursuant to paragraph  3.5.1 above (whether as a result of an Authority request, a change to the Specification, or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Authority.

# TESTING AND AUDIT

## The Supplier shall conduct tests in accordance with the Security Management Plan (**"Security Tests"**) on an annual basis or as otherwise agreed by the parties. The date, timing, content and conduct of such Security Tests shall be agreed in advance with the Authority.

## The Security Tests shall include vulnerability and penetration testing, carried out by an appropriately accredited independent external assessor to be agreed with the Authority (such agreement not to be unreasonably withheld or delayed) and the Supplier shall at the request of the Authority provide evidence that the external assessor is accredited and independent.

## The Authority shall be entitled to send a representative to witness the conducting of the Security Tests subject to this being agreed with any external tester where any such Security Tests are conducted other than on the Supplier’s premises. The Supplier shall provide the Authority with the results of such tests (in a form approved by the Authority in advance) as soon as practicable after completion of each Security Test.

## Where any Security Test carried out pursuant to paragraph 4.3 above reveals any actual or potential Breach of Security, the Supplier shall promptly notify the Authority of any changes 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 Authority’s, approval in accordance with paragraph 3.5.4 the Supplier shall implement such changes to the Security Management Plan in accordance with the timetable agreed with the Authority or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the Security Management Plan is to address non-compliance with the Security Requirements or any other requirement of this agreement, such change shall be at no cost to the Authority.

# COMPLIANCE WITH ISO/IEC 27001

## The Supplier shall ensure that each Sub-Contractor, if applicable, obtains independent certification to ISO/IEC 27001 within two months of the ‘go-live’ date and shall maintain such certification for the duration of the agreement. The Supplier shall promptly upon request by the Authority provide to the Authority evidence of such independent certification to the reasonable satisfaction of the Authority.

## If:

### certain parts of a Sub-Contractor’s ISMS (do not conform to Best Industry Practice); or

### controls (as described in ISO/IEC 27002), in relation to services provided by a Sub-Contractor are not consistent with the Security Requirements,

and, as a result, the Supplier reasonably believes that a Sub-Contractor’s ISMS, or sections thereof, is not compliant with ISO/IEC 27001, the Supplier shall promptly notify the Authority of this and the Authority in its absolute discretion may waive the requirement for compliance in respect of the respective Sub-Contractor ISMS or the relevant parts thereof.

## The Authority shall on giving reasonable prior notice, such notice to include statements of audit aims and deliverables, be entitled no more than once in any Contract Year (or more regularly should the Authority reasonably determine that there is a heightened risk of security breach/threat) and during normal office hours, to carry out such security audits as may be required, in accordance with good industry practice, in order to ensure that the ISMS maintains compliance with the principles and practices of ISO/IEC 27001.

## If, on the basis of evidence obtained as a result of the audits carried out pursuant to the provisions of paragraph 5.3, it is the Authority’s reasonable opinion that compliance with the principles and practices of ISO/IEC 27001 is not being achieved by the Supplier, then the Authority 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, as a result of any such independent audit as described in paragraph 5.3, 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 Authority in obtaining such audit.

# BREACH OF SECURITY

## Without prejudice to the provisions of Clause 32 (Data Processing), each party shall notify the other in accordance with the agreed security incident management process set out in the Security Management Plan upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

## Without prejudice to the security incident management process set out in the Security Management Plan and Clause 32 (Data Processing), upon becoming aware of any of the circumstances referred to in paragraph 6.1, the Supplier shall:

### immediately take all reasonable steps necessary to:

#### remedy such Breach of Security or protect the integrity of the ISMS against any such potential or attempted Breach of Security or threat thereof; and

#### prevent an equivalent Breach of Security in the future,

and such steps shall include any action or changes reasonably required by the Authority. If such action is taken in response to a Breach of Security that is determined by the Authority, acting reasonably, not to be covered by the obligations of the Supplier under this agreement, then the Supplier shall be entitled to refer the matter to the Change Control Procedure; and

### as soon as reasonably practicable provide to the Authority full details of the Breach of Security or the potential or attempted Breach of Security and the steps taken or to be taken by the Supplier in accordance with this paragraph 6.2.

### In the event of an incident which in the opinion of the Authority constitutes a serious Breach of Security, the Supplier shall commission an ad hoc security audit at the Supplier’s expense within five days, to be carried out by an appropriate external auditor approved by the Authority.

### The Supplier shall make the results of any security audits available to the Authority within five Working Days after receipt of the audit results, along with a plan to address any shortcomings or failures identified, if appropriate.