Work Order

This document is a Work Order according to the definitions contained within the provisions of the Services Delivery Agreement (SDA) dated **3RD DECEMBER 2024**, between **BLOOM PROCUREMENT SERVICES LTD** and **FACTOR FINANCIAL PLANNING LTD**.

Except where stated herein, all the clauses and conditions specified in the said supplier terms are included herein by reference and form part of this Work Order.

For the avoidance of doubt, the Bloom Standard Terms & Conditions (only where applicable), the SDA and this Work Order constitute the contract between Bloom and the SPS Provider and are hereinafter referred to collectively as the Supplier Terms.

We are delighted to advise that **BLOOM PROCUREMENT SERVICES LTD** have been authorised to obtain the following services on behalf of the Authority.

Project Number:	Project_6806 Contract_15804
Project Name:	NEPRO3 - Infected Blood Compensation Authority: Provision of Financial Advice to Compensation Recipients
SPS Provider:	Factor Financial Planning Ltd
For the Attention of:	REDACTED TEXT under FOIA Section 40, Personal Information
E-mail:	REDACTED TEXT under FOIA Section 40, Personal Information
Telephone Number:	REDACTED TEXT under FOIA Section 40, Personal Information
Address:	REDACTED TEXT under FOIA Section 40, Personal Information

Description of Specialist Professional Services / deliverables required:

Factor Financial Planning Ltd have been appointed by Bloom Procurement Services Ltd on behalf of the Cabinet Office on behalf of Infected Blood Compensation Authority ('IBCA') to provide the first group of persons claiming (being a group of up to 50) with advice on the safe management of their money through a tailored introductory session with Factor Financial Planning Ltd's independent financial advisor.

Scope of the Work Order

References in this specification to the Cabinet Office and IBCA shall be deemed to be references to the Relevant Authority. The Cabinet Office intends, at a later date, to novate its contractual arrangements to IBCA, which may include the Collateral Warranty and Data Sharing Agreement.

Through the very nature of the scheme, compensation recipients are vulnerable people with complex medical and other needs. Factor Financial Planning Ltd must be able to provide a service and advice sensitive to those needs and compliant with the vulnerable customer policy held by Factor Financial Planning Ltd.

Cabinet Office have interpreted advice for the 'safe management of money' to mean the provision to the person claiming of independent financial advice in the tailored introductory session on:

- The safe and practical management of their funds (e.g. using an appropriate and secure account).
- The choice of lump-sum or periodic payments.
- Safeguarding against fraud.
- The importance of a will and other relevant topics.

And accordingly, the requirement is for Factor Financial Planning Ltd to deliver this scope of advice to each person claiming in that session.

The person claiming may also have other specific questions and requests that Factor Financial Planning Ltd's financial advisor may also address so long as they fall within the scope of advice under this Work Order. To help a person claiming make the choice between lump-sum or regular compensation payments it may be necessary to discuss money management, including investment. This advice should be illustrative and whilst it may include recommendations on investments in certain asset classes, it should not include recommendations for specific products (including specific stock and shares, trusts, funds, ISAs, or similar accounts or products) or financial products owned or managed by Factor Financial Planning Ltd or any employee, officer or associate of Factor Financial Planning Ltd which shall include any affiliated person and any firm for whom Factor Financial Planning Ltd is an appointed representative (or a person which they have any financial or commercial interest in).

Any further paid-for financial advice from Factor Financial Planning Ltd's financial advisor should be only pursued on request of the person in receipt of compensation and should not be provided within the scope of the session paid for by IBCA and must be carried out as a separate engagement with the person claiming. If the person claiming asks for information on further financial advice services and products during the introductory session this must include a full and accurate description of the services that may be offered, and the relevant fees for which the person claiming would be liable - making clear that this would not be paid for by the Delivery Partner or IBCA.

Detailed Requirements Provision of Advice

- Factor Financial Planning Ltd's financial advisor will provide a tailored introductory session of a minimum of one hour to people in receipt of compensation covering the scope of advice identified in Section Three.
- Factor Financial Planning Ltd's financial advisor will gather relevant information about the financial situation of the person in receipt of compensation ahead of the meeting, to identify in advance their specific needs for the session (and the format of this request for information is to be shared with

IBCA in advance of Factor Financial Planning Ltd's financial advisor issuing the request to the first claimant which they will deal with).

- Once the person claiming has accepted their compensation offer IBCA will provide the person claiming with a comparison between the two options for receiving compensation i.e. lump sum or monthly payments; Factor Financial Planning Ltd's financial advisor should provide the person claiming during the introductory session with information and advice to help them make this decision, if requested by the person claiming.

- Following the introductory session, Factor Financial Planning Ltd's financial advisor will produce for the person claiming a summary of their discussion, including - but not limited to - actionable recommendations derived from the discussion which the person claiming may choose to take forward. It should also contain a written statement on the choice between lump-sum or regular compensation of payments. This written summary shall be written in plain, jargon-free English

insofar as possible, and must not solely consist of a recommendation for additional paid-for financial advice.

- Liability for the provision of advice to the person claiming (including where such advice is negligent) rests with Factor Financial Planning Ltd. Factor Financial Planning Ltd's financial advisors are obligated to act in the best interests of their clients and to provide accurate and suitable advice based on the client's individual circumstances. If they fail to meet these obligations, they shall be accountable for any resulting financial losses. Factor Financial Planning Ltd's obligations to take out and maintain for the duration specified in this Work Order professional indemnity insurance are set out in the Work Order. Clients who believe they have received poor advice have the right to seek redress through appropriate channels, such as the Financial Ombudsman Service or the Financial Services Compensation Scheme, if applicable.
- For the purposes of clause 12.2 of the Service Delivery Agreement, no subcontracting by Factor Financial Planning Ltd shall be permitted unless both the Relevant Authority and the Delivery Partner have given their prior written approval.

Sensitivity to Individual Circumstances

- Factor Financial Planning Ltd must ensure that financial advisors consider the specific circumstances of the Infected Blood Compensation Scheme and are sensitive to the history of the contaminated blood scandal so that they can approach discussions with people in receipt of compensation in an informed and sensitive way.

- We consider all compensation recipients will be classed as vulnerable customers under the FCA rules. Factor Financial Planning Ltd must have appropriate procedures in place to support vulnerable customers and follow that procedure when dealing with compensation recipients. Factor Financial Planning Ltd should also demonstrate they have processes in place to apply Consumer Duty (which requires firms to seek good outcomes for consumers).

- Factor Financial Planning Ltd should be willing to work alongside any trusted third party or recognised intermediaries, (solicitors, those with power of attorney, existing IFA etc) in the provision of the service.

- Factor Financial Planning Ltd should be aware of, and accommodating to, those with accessibility needs.

Service Monitoring

- Factor Financial Planning Ltd must submit to IBCA details of the amount of time spent on each session, separated into time spent with each person claiming (i.e. the length of each claimant's session, which must be at minimum one hour) and preparatory time spent thereon, and the provision of the summary and statement required above. This reporting should be sent to IBCA monthly in a format agreed between the parties.

- Factor Financial Planning Ltd must submit service delivery KPIs as described below on a monthly basis.

Mandatory Requirements

Factor Financial Planning Ltd must ensure that all financial advisors advising and/or meeting persons claiming hold Competent Advisor Status and hold at minimum the qualifications set out by the regulating authority which should include but are not limited to an in-date Level 4 financial advisor qualification e.g. the Diploma for Financial Advisors. Where available, financial advisors holding an indate Level 6 financial advisor qualification (e.g. the Advanced Diploma in Financial Planning) is most desirable.

For so long as (and to the extent that) Factor Financial Planning Ltd's ability to comply with and perform the obligations under this Work Order are dependent upon any third party (such as the holding of appointed representative status for a third party independent financial advisor), such circumstances

shall be subject to the prior written approval of the Delivery Partner and of IBCA and, once so approved, shall be maintained for the duration of the delivery of services under this Work Order. Any changes to

this must be communicated in writing to the Relevant Authority and the Delivery Partner within 24 hours.

The financial advisor will gather relevant information about the financial situation of the person in receipt of compensation ahead of the meeting, to identify in advance their specific needs for the session.

Factor Financial Planning Ltd must ensure that financial advisors consider the specific circumstances of the Infected Blood Compensation Scheme, the statutory framework and are sensitive to the history of contaminated blood in the United Kingdom so that they can approach discussions with people in receipt of compensation in an informed and sensitive way.

Factor Financial Planning Ltd must hold and maintain Cyber Essentials certification. Cyber Essentials certification must be renewed annually by Factor Financial Planning Ltd for the duration of the Work Order. To the extent that Factor Financial Planning Ltd does not hold Cyber Essentials certification at the date on which this Work Order commences, it warrants that it will operate at all times in accordance with such certification in providing services under this Work Order and, in any event, will procure that such certification is obtained no later than 14 days from the date of this Work Order.

Factor Financial Planning Ltd shall remain ISO27001 certified during the period of the Work Order.

Factor Financial Planning Ltd shall adhere to the Information Security Schedule set out in Annex 3 during the period of the Work Order.

Safeguarding

The parties acknowledge that Factor Financial Planning Ltd is responsible for the management and control of the activity provided under this Work Order and for the purposes of the Safeguarding Vulnerable Groups Act 2006. Factor Financial Planning Ltd shall act in accordance with any relevant statutory framework, legislation, policy and guidance.

Factor Financial Planning Ltd shall comply with the Relevant Authority's safeguarding policies as amended from time to time.

Factor Financial Planning Ltd shall comply with all statutory obligations including but not limited to safeguarding and any relevant statutory obligations relating to the delivery of the Specialist Professional Services.

Factor Financial Planning Ltd shall indemnify the Delivery Partner and the Relevant Authority against all actions, claims, demands, losses, charges, costs, penalties, and expenses which the Delivery Partner and/or Relevant Authority may suffer or incur as a result of or in connection with any breach or alleged breach of its safeguarding obligations referenced immediately above.

Factor Financial Planning Ltd shall on or before the date on which this Work Order is signed by both parties, promptly and without undue delay supply a fully executed Collateral Warranty and Data Sharing Agreement in favour of the Relevant Authority substantially in the form attached to this Specification at Annex 4. To the extent that this is not done within 24 hours of the signature of this Work Order, this Work Order shall be deemed to be cancelled and shall have no effect. In such circumstances, no compensation or other payment of any kind shall be due to Factor Financial Planning Ltd from the Delivery Partner or Relevant Authority.

Factor Financial Planning Ltd and the Relevant Authority acknowledge and agree that the circumstances and sensitivities of the Infected Blood Compensation Scheme require a strong commitment to data protection standards. The precise requirements stemming from this are set out in the Services Delivery Agreement (for data protection provisions relating to the Delivery Partner and Factor Financial Planning Ltd and are set out in the Collateral Warranty and Data Sharing Agreement (for data protection provisions relating to the Relevant Authority and Factor Financial Planning Ltd).

Milestones

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Service Levels and Key Performance Indicators (KPIs)
REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Termination
REDACTED TEXT under FOIA Section 43 (2), Commercial Information
Contract Management (Measuring Success and Review)
REDACTED TEXT under FOIA Section 43 (2), Commercial Information

REDACTED TEXT under FOIA Section 43 (2), Commercial Information	
REDACTED TEXT under FOIA Section 43 (2), Commercial Information	
REDACTED TEXT under FOIA Section 43 (2), Commercial Information	
Commencement Date	09/12/2024
Completion Date	31/03/2025
REDACTED TEXT under FOIA Section 43 (2), Commercial Information	
REDACTED TEXT under FOIA Section 43 (2), Commercial Information	
REDACTED TEXT under FOIA Section 43 (2), Commercial Information	

Invoicing procedure

The SPS Provider shall complete and submit a Payment Request/Highlight Report via the Technology Platform. This will initiate the Self-Billing Process once approved by the Authority or requirement owner.

Milestone reporting and Payment (Subject to agreed Payment Request/Highlight Report)
Payment Schedule

Description		Deliverables	Invoice Frequency	Total Price
	REDACTED TEXT under FOIA Section 43 (2), Commercial Information			
Total:				**£103,947.50**

Total Price	Commencement Date	Currency
£103,947.50	09/12/2024	Pounds Sterling

Acknowledgment re supervision and control of SPS Provider personnel

By signing this Work Order and agreeing to the Supplier Terms, the SPS Provider confirms for the duration of the Services provided (subject to the contractual terms governing the Services to be provided):

1. The SPS Provider shall procure that its personnel do not act or operate in a manner which could be perceived in such a way as to infer that the SPS Provider's personnel are employees of the Authority;
2. The SPS Provider shall always ensure that the Authority shall not supervise or control the work being carried out by the SPS Provider's personnel;
3. The SPS Provider is free to determine the personnel it uses to provide the services provided that all personnel meet the standards specified by the Authority (including security clearances where applicable);
4. The SPS Provider shall not assume any line management responsibility for any of the Authority's employees;
5. The SPS Provider shall use their own equipment to deliver the Services, except where the provision of equipment by the Authority is necessary for security purposes;

6. The SPS Provider shall determine their own place and hours of work, except where the nature of the project naturally enforces restriction e.g. attending project meetings at client site during business hours;

If at any time, the SPS Provider fails to comply with the above terms, this shall amount to a material breach of the Work Order which is not capable of remedy for the purposes of the termination clause of the SDA and this Work Order will be terminated with immediate effect. If the SPS Provider breaches these provisions it may be liable for the payment of income tax or national insurance contributions.

ANNEX 1 – to record permitted project specific processing of personal data.

1. The Contractor shall comply with any further written instructions with respect to processing by the Data Controller.

2. Any such further instructions shall be incorporated into this Schedule and this Schedule may be amended at any time during the Term by agreement in writing between the Data Controller and the Contractor to ensure that the description and detail set out in this Schedule with regard to the processing of personal data reflects the arrangements between the Parties, is accurate and is compliant against the Data Protection Legislation.

No	Description	Details
1	Subject Matter of the Processing	The SPS Provider will process the Delivery Partner and/or the Relevant Authority businessto-business personal data to enable effective communication between the parties in relation to the provision of services under the Work Order.
2	Duration of the Processing	The processing will continue for the duration of the Work Order and until the completion/expiry/termination of the Work Order.
3	Nature and Purposes of the Processing	The nature of the processing includes the collection, recording, organisation storage, retrieval, use, disclosure by transmission, dissemination or otherwise making available, erasure or destruction of data (whether by automated means). The purpose of the processing is the fulfilment of the SPS Providers obligations arising under the Work Order for the provision of specialist professional services and to ensure effective communication between the SPS Provider, the Delivery Partner and the Relevant Authority.
4	Type of Personal Data	For the purposes of the contract, the Delivery Partner will disclose the following information directly to the SPS Provider: Contact details for individuals concerned with the management of the Work Order. Contact details for individuals concerned with specific projects under the Work Order. (Name, business email address, business telephone number).
5	Categories of Data Subject	Employees or representatives of the Delivery Partner or the Relevant Authority concerned with Work Order.

6	Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The SPS Provider agrees that all personal data supplied will be retained no longer that is necessary after the expiry or termination of the Work Order and shall be destroyed as soon as practicable.

ANNEX 2

1. This Annex lists the sub-processors that the Data Controller has authorised the Contractor to use in accordance with the Supplier Terms.

2. The Data Controller may, at any time and upon such notice as is reasonable in the circumstances, withdraw its approval in relation to any or all sub-processors listed within this Annex and upon such withdrawal the Contractor must immediately cease using that sub-processor.

3. If the Contractor wishes to propose a new sub-processor for approval, it must provide written notice to the Data Controller detailing the identity of the proposed sub-processor, the nature of the sub-processing and confirmation that a written contract in relation to the sub-processing is in place between the Contractor and the sub-processor. The Data Controller must not unreasonably refuse or delay approval.

4. The Data Controller may at any time and upon reasonable notice request copies of the contracts between the Contractor and its approved sub –processors in relation to the sub-processing.

Sub-contractor details: (name, address and company registration number)	**Nature of sub-processing:**	**Commencement date and term of contract between Contractor and Subprocessor:**
N/A	N/A	N/A

Signature Area

Signature: REDACTED TEXT under FOIA Section 40, Personal Information Name: REDACTED TEXT under FOIA Section 40, Personal Information Title: REDACTED TEXT under FOIA Section 40, Personal Information	Signature: REDACTED TEXT under FOIA Section 40, Personal Information Name: REDACTED TEXT under FOIA Section 40, Personal Information Title: REDACTED TEXT under FOIA Section 40, Personal Information

ANNEX 3 Cabinet Office Information Security Management Requirements

Information Security Management

Cabinet Office project requirements for Consultancy/Professional Services

1 Cabinet Office Options

Risk assessment

The Cabinet Office has assessed this Agreement as	a standard consultancy agreement	☒
	a higher-risk consultancy agreement	☐

Relevant Certifications

Where the Cabinet Office has assessed this Agreement as a standard consultancy agreement, it requires the SPS Provider to be certified as compliant with:	Cyber Essentials	☒
	Cyber Essentials Plus	☐

2 SPS Provider obligations

2.1 Where the Cabinet Office has assessed this Agreement as a higher-risk consultancy agreement, the SPS Provider must comply with all requirements in this Schedule Annex 3 (Security Management).

2.2 Where the Cabinet Office has assessed this Agreement as a standard consultancy agreement, the SPS Provider must comply with this Schedule Annex 3 (Security Management), other than:

(a) the requirement to be certified as compliant with ISO/IEC 27001:2013 under Paragraph 7.1(b);

(b) the requirement to undertake security testing of the SPS Provider Information Management System in accordance with paragraph 3 of Appendix 1;

(c) the requirement to produce a Security Management Plan in accordance with Paragraph 8.

(d) the requirement to document unencrypted Cabinet Office Data in the Security Management Plan in accordance with paragraph 5.4 of Appendix 1.

3 Definitions

In this Schedule Annex 3 (Security Management):

"Anti-virus Software"	means software that: (a) protects the SPS Provider Information Management System from the possible introduction of Malicious Software; (b) scans for and identifies possible Malicious Software in the SPS Provider Information Management System; (c) if Malicious Software is detected in the SPS Provider Information Management System, so far as possible: (i) prevents the harmful effects of the Malicious Software; and
	(ii) removes the Malicious Software from the SPS Provider Information Management System.
"Breach of Security"	means the occu of: (a) any unauthorised access to or use of the Services, the Cabinet Office Premises, the Sites, the SPS Provider Information Management System and/or any information or data used by the Cabinet Office, the SPS Provider or any Sub-contractor in connection with this Agreement; (b) the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Cabinet Office, the SPS Provider or any Subcontractor in connection with this Agreement; and/or (c) any part of the SPS Provider Information Management System ceasing to be compliant with the Certification Requirements.
"Cabinet Office Data"	means any: (a) data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; or (b) Personal Data for which the Cabinet Office is a, or the, Data Controller, that is: (i) supplied to the SPS Provider by or on behalf of the Cabinet Office; or (ii) that the SPS Provider generates, processes, stores or transmits under this Agreement.
"Cabinet Office Equipment"	means any hardware, computer or telecoms devices, and equipment that forms part of the Cabinet Office System.

"Cabinet Office System"	means the information and communications technology system used by the Cabinet Office to interface with the SPS Provider Information Management System or through which the Cabinet Office receives the Services.
"Certification Default"	means the occurrence of one or more of the circumstances listed in paragraph 7.4.
"Certification Rectification Plan"	means the plan referred to in paragraph 7.5(a).
"Certification Requirements"	means the information security requirements set out in paragraph 7.
"Cyber Essentials"	means the Cyber Essentials certificate issued under the Cyber Essentials Scheme.
"Cyber Essentials Plus"	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme.

"Cyber Essentials Scheme"	means the Cyber Essentials scheme operated by the National Cyber Security Centre.
"End-user Device"	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
"HMG Baseline Personnel Security Standard"	means the employment controls applied to any individual member of the SPS Provider Personnel that performs any activity relating to the provision or management of the Services, as set out in "HMG Baseline Personnel Standard", Version 6.0, May 2018 https://assets.publishing.service.gov.uk /government/uploads/system/uploads/attachment_data/file/714002/HMG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time.
"Malicious Software"	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations.
"NCSC Cloud Security Principles"	means the National Cyber Security Centre's document "Implementing the Cloud Security Principles" as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloudsecurity/implementing-the-cloud-security-principles.
"NCSC Device Guidance"	means the National Cyber Security Centre's document "Device Security Guidance", as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance.

"Privileged User"	means a user with system administration access to the SPS Provider Information Management System, or substantially similar access privileges.
"Process"	means any operation performed on data, whether or not by automated means, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of that data.
"Prohibited Activity"	means the storage, access or Processing of Cabinet Office Data prohibited by a Prohibition Notice.
"Prohibition Notice"	means a notice issued under paragraph 1.3 of Appendix **Error! Reference source not found.**.
"Relevant Certifications"	means those certifications specified in paragraph 7.1.
"Relevant Convictions"	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Cabinet Office may specify.
"Security Management Plan"	means the document prepared in accordance with the requirements of paragraph 8.
"Sites"	means any premises: (a) from or at which: (i) the Services are (or are to be) provided; or (ii) the SPS Provider manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the SPS Provider Information Management System is situated; or (ii) any physical interface with the Cabinet Office System takes place.
"Standard Contractual Clauses"	means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area.

"SPS Provider Information Management System"	means: (a) those parts of the information and communications technology system and the Sites that the SPS Provider or its Sub-contractors will use to provide the Services; and (b) the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);
"Sub-contractor Personnel"	means: (a) any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and (b) engaged in or likely to be engaged in: (i) the performance or management of the Services; (ii) or the provision of facilities or services that are necessary for the provision of the Services.
"SPS Provider Personnel"	means any individual engaged, directly or indirectly, or employed by the SPS Provider or any Sub-contractor in the management or performance of the SPS Provider's obligations under this Agreement.
"UKAS"	means the United Kingdom Accreditation Service.

4 Introduction

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

5 Principles of security

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

6 Access to SPS Provider Personnel and SPS Provider Information Management System

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

7 Certification Requirements

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

8 Security Management Plan

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

9 Notices

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Appendix 1 - Security requirements

1 Location

1.1 Unless otherwise agreed with the Cabinet Office, the SPS Provider must, and must ensure that its Sub-contractors must, at all times, store, access or process Cabinet Office Data either:

(a) in the United Kingdom;

(b) the European Economic Area; or

(c) in a facility operated by an entity where:

(i) the entity has entered into a binding agreement with the SPS Provider or Subcontractor (as applicable);

(i) that binding agreement includes obligations on the entity in relation to security management at least an onerous as those relating to Subcontractors in this Schedule Annex 3 (Security Management);

(ii) the SPS Provider or Sub-contractor has taken reasonable steps to assure itself that

(A) the entity complies with the binding agreement;

(B) any system operated by the SPS Provider or Sub-contractor has in place appropriate technical and organisational measures to ensure that the Subcontractor will store, access, manage and/or Process the Government Data as required by this Schedule Annex 3 (*Security Management*); and

(iii) the SPS Provider has provided the Cabinet Office with such information as the Cabinet Office requires concerning:

(A) the entity;

(B) the arrangements with the entity; and

(C) the entity's compliance with the binding agreement; and

(iv) the Cabinet Office has not given the SPS Provider a Prohibition Notice under paragraph 1.3.

1.2 Where the SPS Provider cannot comply with one or more of the requirements of paragraph 1.1:

(a) it must provide the Cabinet Office with such information as the Cabinet Office requests concerning the security controls in places at the relevant location or locations; and

(b) the Cabinet Office may grant approval to use that location or those locations, and that approval may include conditions; and

(c) if the Cabinet Office does not grant permission to use that location or those locations, the SPS Provider must cease to store, access or process Cabinet Office Data at that location or those locations within such period as the Cabinet Office may specify.

1.3 The Cabinet Office may by notice in writing at any time give notice to the SPS Provider that it and its Sub-contractors must not undertake or permit to be undertaken, the storage, access or Processing Cabinet Office Data as specified in the notice (a "**Prohibited Activity**").

(a) in any particular country or group of countries;

(b) in or using facilities operated by any particular entity or group of entities; or

(c) in or using any particular facility or group of facilities, whether operated by the SPS Provider, a Sub-contractor or a third-party entity (a "**Prohibition Notice**").

1.4 Where the SPS Provider or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the SPS Provider must, and must procure that Subcontractors, cease to undertake that Prohibited Activity within 40 Working Days of the date of the Prohibition Notice.

2 Vetting, Training and Staff Access

Vetting before performing or managing Services

2.1 The SPS Provider must not engage SPS Provider Personnel, and must ensure that Sub-contractors do not engage Sub-contractor Personnel, in any activity relating to the performance and management of the Services unless:

(a) That individual has passed the security checks listed in paragraph 2.2; or

(b) The Cabinet Office has given prior written permission for a named individual to perform a specific role.

2.2 For the purposes of paragraph 2.1, the security checks are:

(a) the checks required for the HMG Baseline Personnel Security Standard (BPSS) to verify:

(i) the individual's identity;

(ii) the individual's nationality and immigration status so as to demonstrate that they have a right to work in the United Kingdom;

(iii) the individual's previous employment history; and

(iv) that the individual has no Relevant Convictions;

(b) national security vetting clearance to the level specified by the Cabinet Office for such individuals or such roles as the Cabinet Office may specify; or

(c) such other checks for the SPS Provider Personnel of Sub-contractors as the Cabinet Office may specify.

Annual training

2.3 The SPS Provider must ensure, and ensure that Sub-contractors ensure, that all SPS Provider Personnel, complete and pass security training at least once every calendar year that covers:

(a) general training concerning security and data handling; and

(b) phishing, including the dangers from ransomware and other malware.

Staff access

2.4 The SPS Provider must ensure, and ensure that Sub-contractors ensure, that individual SPS Provider Personnel can access only the Cabinet Office Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

2.5 The SPS Provider must ensure, and ensure that Sub-contractors ensure, that where individual SPS Provider Personnel no longer require access to the Cabinet Office Data or any part of the Cabinet

Office Data, their access to the Cabinet Office Data or that part of the Cabinet Office Data is revoked immediately when their requirement to access Cabinet Office Data ceases.

2.6 Where requested by the Cabinet Office, the SPS Provider must remove, and must ensure that Subcontractors remove, an individual SPS Provider Personnel's access to the Cabinet Office Data or part of that Cabinet Office Data specified by the Cabinet Office as soon as practicable and in any event within 24 hours of the request.

Exception for certain Sub-contractors

2.7 Where the SPS Provider considers it cannot ensure that a Sub-contractors will undertake the relevant security checks on any Sub-contractor Personnel, it must:

(a) as soon as practicable, and in any event within 20 Working Days of becoming aware of the issue, notify the Cabinet Office;

(b) provide such information relating to the Sub-contractor, its vetting processes and the roles the affected SPS Provider Personnel will perform as the Cabinet Office reasonably requires; and

(c) comply, at the SPS Provider's cost, with all directions the Cabinet Office may provide concerning the vetting of the affected Sub-contractor Personnel and the management of the Sub-contractor.

3 Security Testing

3.1 This paragraph applies only where the Cabinet Office has assessed that this Agreement is a higherrisk consultancy agreement.

Note: the definition of SPS Provider Information Management System includes those information and communications technology systems that Sub-contractors will use to assist or contribute to the SPS Provider providing the Services.

3.2 The SPS Provider must, at the Cabinet Office's option, before providing the Services and when reasonably requested by the Cabinet Office, either:

(a) conduct security testing of the SPS Provider Information Management System by:

(i) engaging a CHECK Service Provider or a CREST Service Provider;

(ii) designing and implementing the testing so as to minimise its impact on the SPS Provider Information Management System and the delivery of the Services; and

(iii) providing the Cabinet Office with a full, unedited and unredacted copy of the testing report without delay and in any event within ten Working Days of its receipt by the SPS Provider; or

(b) Provide details of any security testing undertaken by a CHECK Service Provider or a CREST Service Provider in respect of the SPS Provider Information Management System in the calendar year immediately preceding the Cabinet Office's request or the Effective Date (as appropriate), including:

(i) the parts of the SPS Provider Information Management System tested;

(ii) a full, unedited and unredacted copy of the testing report; and

(iii) the remediation plan prepared by the SPS Provider to address any vulnerabilities disclosed by the security testing; and

(iv) the SPS Provider's progress in implementing that remediation plan.

3.3 The SPS Provider must remediate any vulnerabilities classified as "medium" or above in the security testing:

(a) before Processing Cabinet Office data where the vulnerability is discovered before the SPS Provider begins to process Authority Data;

(b) where the vulnerability is discovered when the SPS Provider has begun to Process Cabinet Office Data:

(i) by the date agreed with the Cabinet Office; or

(ii) where no such agreement is reached:

(A) within five Working Days of becoming aware of the vulnerability and its classification where the vulnerability is classified as critical;

(B) within one month of becoming aware of the vulnerability and its classification where the vulnerability is classified as high; and

(C) within three months of becoming aware of the vulnerability and its classification where the vulnerability is classified as medium.

4 End-user Devices

4.1 The SPS Provider must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Cabinet Office Data is stored or processed in accordance the following requirements:

(a) the operating system and any applications that store, process or have access to Cabinet Office Data must be in current support by the vendor, or the relevant community in the case of open source operating systems or applications;

(b) users must authenticate before gaining access;

(c) all Cabinet Office Data must be encrypted using a encryption tool agreed to by the Cabinet Office;

(d) the End-user Device must lock and require any user to re-authenticate after a period of time that is proportionate to the risk environment, during which the End-user Device is inactive;

(e) the End-user Device must be managed in a way that allows for the application of technical policies and controls over applications that have access to Cabinet Office Data;

(f) the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Cabinet Office Data on the device and prevent any user or group of users from accessing the device;

(g) all End-user Devices are within in the scope of any current Cyber Essentials Plus certificate held by the SPS Provider, or any ISO/IEC 27001:2018 certification issued by a UKASapproved certification body, where the scope of that certification includes the Services.

4.2 The SPS Provider must comply, and ensure that all Sub-contractors comply, with the recommendations in NCSC Device Guidance as if those recommendations were incorporated as specific obligations under this Agreement.

4.3 Where there any conflict between the requirements of this Schedule Annex 3 (Security Management) and the requirements of the NCSC Device Guidance, the requirements of this Schedule will take precedence.

5 Encryption

5.1 Unless paragraph 5.2 applies, the SPS Provider must ensure, and must ensure that all Subcontractors ensure, that Cabinet Office Data is encrypted:

(a) when stored at any time when no operation is being performed on it; and

(b) when transmitted.

5.2 Where the SPS Provider, or a Sub-contractor, cannot encrypt Cabinet Office Data as required by paragraph 5.1, the SPS Provider must:

(a) immediately inform the Cabinet Office of the subset or subsets of Cabinet Office Data it cannot encrypt and the circumstances in which and the reasons why it cannot do so;

(b) provide details of the protective measures the SPS Provider or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Cabinet Office as encryption;

(c) provide the Cabinet Office with such information relating to the Cabinet Office Data concerned, the reasons why that Cabinet Office Data cannot be encrypted and the proposed protective measures as the Cabinet Office may require.

5.3 The Cabinet Office, the SPS Provider and, where the Cabinet Office requires, any relevant Subcontractor shall meet to agree appropriate protective measures for the unencrypted Cabinet Office Data.

5.4 This paragraph applies where the Cabinet Office has assessed that this Agreement is a higher-risk consultancy agreement.

Where the Cabinet Office and SPS Provider reach agreement, the SPS Provider must update the Security Management Plan to include:

(a) the subset or subsets of Cabinet Office Data not encrypted and the circumstances in which that will occur;

(b) the protective measure that the SPS Provider and/or Sub-contractor will put in please in respect of the unencrypted Cabinet Office Data.

5.5 Where the Cabinet Office and SPS Provider do not reach agreement within 40 Working Days of the date on which the SPS Provider first notified the Cabinet Office that it could not encrypt certain Cabinet Office Data, either party may refer the matter to [be determined by an expert in accordance with the Dispute Resolution Procedure].

6 Access Control

6.1 The SPS Provider must, and must ensure that all Sub-contractors:

(a) identify and authenticate all persons who access the SPS Provider Information Management System and Sites before they do so;

(b) require multi-factor authentication for all user accounts that have access to Cabinet Office Data or that are Privileged Users;

(c) allow access only to those parts of the SPS Provider Information Management System and Sites that those persons require;

(d) maintain records detailing each person's access to the SPS Provider Information Management System and Sites, and make those records available to the Cabinet Office on request.

6.2 The SPS Provider must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the SPS Provider Information Management System:

(a) are accessible only from dedicated End-user Devices;

(b) are configured so that those accounts can only be used for system administration tasks;

(c) require passwords with high complexity that are changed regularly;

(d) automatically log the user out of the SPS Provider Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.

6.3 The SPS Provider must require, and must ensure that all Sub-contractors require, that Privileged Users use unique and substantially different passwords for their different accounts on the SPS Provider Information Management System.

6.4 The SPS Provider must, and must ensure that all Sub-contractors:

(a) configure any hardware that forms part of the SPS Provider Information Management System that is capable of requiring a password before it is accessed to require a password; and

(b) change the default password of that hardware to a password of high complexity that is substantially different from the password required to access similar hardware.

7 Malicious Software

7.1 The SPS Provider shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the SPS Provider Information Management System.

7.2 The SPS Provider shall ensure that such Anti-virus Software:

(a) is configured to perform automatic software and definition updates;

(b) performs regular scans of the SPS Provider Information Management System to check for and prevent the introduction of Malicious Software; and

(c) where Malicious Software has been introduced into the SPS Provider Information Management System, identifies, contains the spread of, and minimises the impact of Malicious Software.

7.3 If Malicious Software is found, the Parties shall cooperate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or

corruption of Cabinet Office Data, assist each other to mitigate any Losses and to restore the Services to their desired operating efficiency.

7.4 Any cost arising out of the actions of the parties taken in compliance with the provisions of paragraph 7.3 shall be borne by the parties as follows:

(a) by the SPS Provider where the Malicious Software originates from the SPS Provider Software, any third-party software licenced by the SPS Provider or the Cabinet Office Data

(whilst the Cabinet Office Data was under the control of the SPS Provider) unless the SPS Provider can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Cabinet Office when provided to the SPS Provider; and

(b) by the Cabinet Office, in any other circumstance.

8 Breach of Security

8.1 If either party becomes aware of a Breach of Security it shall notify the other as soon as reasonably practicable after becoming aware of the breach, and in any event within 24 hours.

8.2 The SPS Provider must, upon becoming aware of a Breach of Security or attempted Breach of Security immediately take those steps identified in the Security Management Plan (if applicable) and all other reasonably steps necessary to:

(a) minimise the extent of actual or potential harm caused by such Breach of Security;

(b) remedy such Breach of Security to the extent possible;

(c) apply a tested mitigation against any such Breach of Security; and

(d) prevent a further Breach of Security in the future which exploits the same root cause failure.

8.3 As soon as reasonably practicable and, in any event, within five Working Days, or such other period agreed with the Cabinet Office, following the Breach of Security or attempted Breach of Security, provide to the Cabinet Office full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Cabinet Office.

8.4 The SPS Provider must take the steps required by paragraph 8.2 at its own cost and expense.

9 Sub-contractors

The SPS Provider must assess the parts of the information and communications technology system and the Sites that its Sub-contractors will use to provide the Services against the NCSC Cloud Security Principles at their own cost and expense to demonstrate that the people, process, technical and physical controls have been delivered in an effective way. The Sub-contractor must document that assessment and make that documentation available to the Cabinet Office at the Cabinet Office's request.

10 Third-party Software

The SPS Provider must not, and must ensure that Sub-contractors do not, use any software to Process Cabinet Office Data where the licence terms of that software purport to grant the licensor rights to Progress the Cabinet Office Data greater than those rights strictly necessary for the use of the software.

11 Deletion of Cabinet Office Data

The SPS Provider must, and must ensure that all Sub-contractors, securely erase any or all Cabinet Office Data held by the SPS Provider or Sub-contractor when requested to do so by the Cabinet Office using a deletion method that ensures that even a determined expert using specialist techniques can recover only a small fraction of the data deleted.

ANNEX 4 Collateral Warranty and Data Sharing Agreement

REDACTED TEXT under FOIA Section 43 (2), Commercial Information