Framework Schedule 6 (Order Form Template and Call-Off Schedules)

Order Form

CALL-OFF REFERENCE:	**GCFMMSCR1123**
THE BUYER:	Cabinet Office
BUYER ADDRESS	70 Whitehall, London SW1A 2AS
THE SUPPLIER:	Nurole Ltd
SUPPLIER ADDRESS:	Metro Building, 1 Butterwick, London W6 8DL
REGISTRATION NUMBER:	08917794
DUNS NUMBER:	219929991
SID4GOV ID:	

APPLICABLE FRAMEWORK CONTRACT

This Order Form is for the provision of the Call-Off Deliverables and dated 15/11/2023. It's issued under the Framework Contract with the reference number **RM6290** for the provision of Non-Executive Recruitment Services for Crown Representatives.

CALL-OFF LOT(S):
Lot 3: Non-Executive and Public Appointments
CALL-OFF INCORPORATED TERMS

The following documents are incorporated into this Call-Off Contract. Where numbers are missing we are not using those schedules. If the documents conflict, the following order of precedence applies:

1. This Order Form including the Call-Off Special Terms and Call-Off Special Schedules.
2. Joint Schedule 1(Definitions and Interpretation)
3. **RM6290** Framework Special Terms
4. The following Schedules in equal order of precedence:

    - Joint Schedules for **RM6290** ○ Joint Schedule 1Definitions ○ Joint Schedule 2 (Variation Form) ○ Joint Schedule 3 (Insurance Requirements) ○ Joint Schedule 4 (Commercially Sensitive Information) ○ Joint Schedule 5

(Corporate Social Responsibility) ○ Joint Schedule 10 (Rectification Plan)
- ○ Joint Schedule 11 (Processing Data)
- ○ Joint Schedule 12 (Supply Chain Visibility)

- Call-Off Schedules for **RM6290** ○ Call-Off Schedule 1 (Transparency Reports) ○ Call-Off Schedule 2 (Staff Transfer) ○ Call-Off Schedule 3 (Continuous Improvement)
  - ○ Call-Off Schedule 7 (Key Supplier Staff)
  - ○ Call-Off Schedule 8 (Business Continuity and Disaster Recovery)
  - ○ Call-Off Schedule 10 (Exit Management) ○ Call-Off Schedule 13 (Implementation Plan and Testing) ○ Call-Off Schedule 14 (Service Levels) ○ Call-Off Schedule 15 (Call-Off Contract Management)
  - ○ Call-Off Schedule 16 (Benchmarking) ○ Call-Off Schedule 18 (Background Checks)

No other Supplier terms are part of the Call-Off Contract. That includes any terms written on the back of, added to this Order Form, or presented at the time of delivery.

CALL-OFF SPECIAL TERMS

GCFMMSCR1123-Security Management applies as the Security Schedule, appended at Annex 1

CALL-OFF START DATE: **16/11/2023**

CALL-OFF EXPIRY DATE: **30/04/2024**

CALL-OFF INITIAL PERIOD:

5 Months

CALL-OFF DELIVERABLES

Delivery of Non-Executive Recruitment Support services to the Cabinet Office for the role of Crown Representative for three to six candidates, depending on demand, including: (i) creation of role specification and advert materials; (ii) candidate identification and outreach; (iii) support regarding candidate assessment and shortlisting; (iv) support regarding interview scheduling and organisation. This will be delivered within 6-months of the contract start date, at longest.

This will include two core deliverables [related to the payment schedule]:

Deliverable 1 by 16 November 2023: The provision of role specification and advert materials posted live to accept candidate applications.
Deliverable 2 within three months of successfully passing the interview, subject to clearance: the successful appointment of candidates to the Crown Representative role/s.

MAXIMUM LIABILITY
The limitation of liability for this Call-Off Contract is stated in Clause 11.2 of the Core Terms.
The Estimated Year 1 Charges used to calculate liability in the first Contract Year is **a maximum of £42,500.**

CALL-OFF CHARGES

Deliverable 1 [redacted]
REDACTED UNDER FOI ACT SECTION 43, COMMERCIAL INTERESTS

Deliverable 2 [redacted]
REDACTED UNDER FOI ACT SECTION 43, COMMERCIAL INTERESTS

[redacted]

REDACTED UNDER FOI ACT SECTION 43, COMMERCIAL INTERESTS

Where a candidate leaves within the first month of employment and a replacement is sourced from the reserve list, no charge will be made under Deliverable 2 for the replacement candidate.

The maximum total contract value for this requirement will be **£42,500. The final contract value will depend on the number of candidates appointed.**

REIMBURSABLE EXPENSES
None

PAYMENT METHOD
BACS, monthly in arrears

BUYER'S INVOICE ADDRESS:
REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION

BUYER'S AUTHORISED REPRESENTATIVE
REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION

BUYER'S ENVIRONMENTAL POLICY
Available online at: https://www.gov.uk/government/publications/cabinet-officeenvironmental-policy-statement/cabinet-office-environmental-policy-statement#:~:text=reducing%20waste%20and%20increasing%20reuse,including%20in%20our%20supply%20chain

BUYER'S SECURITY POLICY
See GCFMMSCR1123-Security Management, appended at Annex 1

SUPPLIER'S AUTHORISED REPRESENTATIVE
REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION

SUPPLIER'S CONTRACT MANAGER
REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION

PROGRESS REPORT FREQUENCY
Every two weeks by 5pm on the Monday of the week following the report period.

PROGRESS MEETING FREQUENCY
Every two weeks on a day to be determined by the buyer and supplier. This may change to weekly during the recruitment campaign at the request of the buyer or supplier.

KEY STAFF
REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION

KEY SUBCONTRACTOR(S)
REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION

COMMERCIALLY SENSITIVE INFORMATION
Not applicable

SERVICE CREDITS
Not applicable

ADDITIONAL INSURANCES
Not applicable

GUARANTEE
Not applicable

SOCIAL VALUE COMMITMENT
Not applicable

For and on behalf of the Supplier:		**For and on behalf of the Buyer:**	
Signature:	REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION	Signature:	REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION
Name:	REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION	Name:	REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION
Role:	REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION	Role:	REDACTED UNDER FOI ACT SECTION 40, PERSONAL INFORMATION
Date:	16 Nov 2023	Date:	16 Nov 2023

Annex 1 - GCFMMSCR1123-Security Management

1 Buyer Options

Risk assessment

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

Relevant Certifications

	Cyber Essentials	☒

Where the Buyer has assessed this Agreement as a standard consultancy agreement, it requires the Supplier to be certified as compliant with:	Cyber Essentials Plus	☐

2 Supplier obligations

2.1 Where the Buyer has assessed this Agreement as a higher-risk consultancy agreement, the Supplier must comply with all requirements in this Schedule [x] (Security Management).

2.2 Where the Buyer has assessed this Agreement as a standard consultancy agreement, the Supplier must comply with this Schedule [x] (Security Management), other than:

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

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

(c) the requirement to document unencrypted Buyer Data in the Security Management Plan in accordance with paragraph 5.4 of Appendix 1

3 Definitions

In this Schedule [x] (Security Management):

"Anti-virus Software"	means software that: (a) protects the Supplier Information Management System from the possible introduction of Malicious Software; (b) scans for and identifies possible Malicious Software in the Supplier Information Management System;
	(c) if Malicious Software is detected in the Supplier Information Management System, so far as possible: (i) prevents the harmful effects of the Malicious Software; and (ii) removes the Malicious Software from the Supplier Information Management System.

"Breach of Security"	means the occ of: (a) any unauthorised access to or use of the Services, the Buyer Premises, the Sites, the Supplier Information Management System and/or any information or data used by the Buyer, the Supplier 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 Buyer, the Supplier or any Sub-contractor in connection with this Agreement; and/or (c) any part of the Supplier Information Management System ceasing to be compliant with the Certification Requirements.
"Buyer 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 Buyer is a, or the, Data Controller, that is: (i) supplied to the Supplier by or on behalf of the Buyer; or (ii) that the Supplier generates, processes, stores or transmits under this Agreement.
"Buyer Equipment"	means any hardware, computer or telecoms devices, and equipment that forms part of the Buyer System.
"Buyer System"	means the information and communications technology system used by the Buyer to interface with the Supplier Information Management System or through which the Buyer 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 Supplier 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/cloud-security/implementingthe-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-securityguidance.

"Privileged User"	means a user with system administration access to the Supplier 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 Buyer Data prohibited by a Prohibition Notice.
"Prohibition Notice"	means a notice issued under paragraph 1.3 of Appendix 1.
"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 Buyer 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 Supplier manages, organises or otherwise directs the provision or the use of the Services; or (b) where: (i) any part of the Supplier Information Management System is situated; or (ii) any physical interface with the Buyer 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.
"Supplier Information Management System"	means: (a) those parts of the information and communications technology system and the Sites that the Supplier 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.

"Supplier Personnel"	means any individual engaged, directly or indirectly, or employed by the Supplier or any Sub-contractor in the management or performance of the Supplier's obligations under this Agreement.
"UKAS"	means the United Kingdom Accreditation Service.

4 Introduction

4.1 This Schedule [x] (Security Management) sets out:

(a) the arrangements the Supplier must implement before, and comply with when, providing the Services and performing its other obligations under this Agreement to ensure the security of the Buyer Data, the Services and the Supplier Information Management System;

(b) the assessment of this Agreement as either a:

(i) standard consultancy agreement; or

(ii) higher-risk consultancy agreement, in paragraph 1;

(c) the Buyer's access to the Supplier Personnel and Supplier Information Management System, in paragraph 6;

(d) the Certification Requirements, in paragraph 7;

(e) the requirements for a Security Management Plan in the case of higher-risk consultancy agreements, in paragraph 8; and

(f) the security requirements with which the Supplier and Sub-contractors must comply in Appendix 1.

5 Principles of security

5.1 The Supplier acknowledges that the Buyer places great emphasis on the confidentiality, integrity and availability of the Buyer Data and, consequently on the security of:

(a) the Sites;

(b) the Services; and

(c) the Supplier's Information Management System.

5.2 The Supplier is responsible for:

(a) the security, confidentiality, integrity and availability of the Buyer Data when that Buyer Data is under the control of the Supplier or any of its Subcontractors; and

(b) the security of the Supplier Information Management System.

5.3 The Supplier:

(a) comply with the security requirements in Appendix 1; and

(b) ensure that each Sub-contractor that Processes Buyer Data complies with the security requirements in Appendix 1.

5.4 Where the Supplier, a Sub-contractor or any of the Supplier Personnel is granted access to the Buyer System or to the Buyer Equipment, it must comply with and ensure that all such Sub-contractors and Supplier Personnel comply with, all rules, policies and guidance provided to it and as updated from time to time concerning the Buyer System or the Buyer Equipment.

6 Access to Supplier Personnel and Supplier Information Management System

6.1 The Buyer may require, and the Supplier must provide the Buyer and its authorised representatives with:

(a) access to the Supplier Personnel;

(b) access to the Supplier Information Management System to audit the Supplier and its Sub-contractors' compliance with this Agreement; and

(c) such other information and/or documentation that the Buyer or its authorised representatives may reasonably require,

to assist the Buyer to establish whether the arrangements which the Supplier and its Sub-contractors have implemented in order to ensure the security of the Buyer Data and the Supplier Information Management System are consistent with the representations in the Security Management Plan.

6.2 The Supplier must provide the access required by the Buyer in accordance with paragraph 6.1 within ten Working Days of receipt of such request, except in the case of a Breach of Security in which case the Supplier shall provide the Buyer with the access that it requires within 24 hours of receipt of such request.

7 Certification Requirements

7.1 The Supplier shall ensure that, unless otherwise agreed by the Buyer, it is certified as compliant with:

(a) in the case of a standard consultancy agreement the option chosen by the Buyer in Paragraph 1; or

(b) in the case of a higher-risk consultancy agreement:

(i) Cyber Essentials Plus ("**Relevant Certifications**").

7.2 Unless otherwise agreed by the Buyer, the Supplier must provide the Buyer with a copy of the Relevant Certifications before it begins to provide the Services.

7.3 The Supplier must ensure that at the time it begins to provide the Services, the Relevant Certifications are:

(a) currently in effect;

(b) relate to the full scope of the Supplier Information System; and

(c) are not subject to any condition that may impact the provision of the Services.

7.4 The Supplier must notify the Buyer promptly, any in any event within three Working Days of becoming aware that:

(a) a Relevant Certification has been revoked or cancelled by the body that awarded it;

(b) a Relevant Certification expired and has not been renewed by the Supplier;

(c) a Relevant Certification no longer applies to the full scope of the Supplier Information Management System or

(d) the body that awarded a Relevant Certification has made it subject to conditions, the compliance with which may impact the provision of the Services (each a **"Certification Default").**

7.5 Where the Supplier has notified the Buyer of a Certification Default under paragraph 7.4:

(a) the Supplier must, within ten working Days of the date in which the Supplier provided notice under paragraph 7.4 (or such other period as the Parties may agree) provide a draft plan (a "Certification Rectification Plan") to the Supplier setting out:

(i) full details of the Certification Default, including a root cause analysis;

(ii) the actual and anticipated effects of the Certification Default;

(iii) the steps the Supplier will take to remedy the Certification Default;

(b) the Buyer must notify the Supplier as soon as reasonably practicable whether it accepts or rejects the Certification Rectification Plan;

(c) if the Buyer rejects the Certification Rectification Plan, the Buyer must within five Working Days of the date of the rejection submit a revised Certification Rectification Plan and paragraph 7.5(b) will apply to the re-submitted plan;

(d) the rejection by the Buyer of a revised Certification Rectification Plan is a material Default of this Agreement;

(e) if the Buyer accepts the Certification Rectification Plan, the Supplier must start work immediately on the plan.

8 Security Management Plan

8.1 This paragraph 8 applies only where the Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

Preparation of Security Management Plan

8.2 The Supplier shall document in the Security Management Plan how the Supplier and its Sub-contractors shall comply with the requirements set out in this Schedule [x] (Security Management) and the Agreement in order to ensure the security of the Buyer Data and the Supplier Information Management System.

8.3 The Supplier shall prepare and submit to the Buyer within 20 Working Days of the date of this Call-Off Contract, the Security Management Plan, which must include:

(a) an assessment of the Supplier Information Management System against the requirements of this Schedule [x] (Security Management), including Appendix 1

(b) the process the Supplier will implement immediately after it becomes aware of a Breach of Security to restore normal operations as quickly as possible, minimising any adverse impact on the Buyer Data, the Buyer, the Services and/or users of the Services; and

(c) the following information in respect of each Sub-contractor:

(i) the Sub-contractor's:

(A) legal name;

(B) trading name (if any);

(C) registration details (where the Sub-contractor is not an individual);

(ii) the Sites used by the Sub-contractor;

(iii) the Buyer Data Processed by the Sub-contractor;

(iv) the Processing that the Sub-contractor will undertake in respect of the Buyer Data;

(v) the measures the Sub-contractor has in place to comply with the requirements of this Schedule [x] (Security Management).

8.4 The Buyer shall review the Supplier's proposed Security Management Plan as soon as possible and must issue the Supplier with either:

(a) an information security approval statement, which shall confirm that the Supplier may use the Supplier Information Management System to Process Buyer Data; or

(b) a rejection notice, which shall set out the Buyer's reasons for rejecting the Security Management Plan.

8.5 If the Buyer rejects the Supplier's proposed Security Management Plan, the Supplier must prepare a revised Security Management Plan taking the Buyer's reasons into account, which the Supplier must submit to the Buyer for review within ten Working Days of the date of the rejection, or such other period agreed with the Buyer.

Updating Security Management Plan

8.6 The Supplier shall regularly review and update the Security Management Plan, and provide such to the Buyer, at least once each year and as required by this paragraph.

Monitoring

8.7 The Supplier shall notify the Buyer within two Working Days after becoming aware of:

(a) a significant change to the components or architecture of the Supplier Information Management System;

(b) a new risk to the components or architecture of the Supplier Information Management System;

(c) a vulnerability to the components or architecture of the Supplier Information Management System using an industry standard vulnerability scoring mechanism;

(a) a change in the threat profile;

(d) a significant change to any risk component;

(e) a significant change in the quantity of Personal Data held within the Service;

(f) a proposal to change any of the Sites from which any part of the Services are provided; and/or

8.8 Within ten Working Days of such notifying the Buyer or such other timescale as may be agreed with the Buyer, the Supplier shall make the necessary changes to the Security Management Plan and submit the updated Security Management Plan to the Buyer for review and approval.

Appendix 1: Security requirements

1 Location

1.1 Unless otherwise agreed with the Buyer, the Supplier must, and must ensure that its Sub-contractors must, at all times, store, access or process Buyer 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 Supplier or Sub-contractor (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 [x] (Security Management);

(ii) the Supplier 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 Supplier or Sub-contractor has in place appropriate technical and organisational measures to ensure that the Sub-contractor will store, access, manage and/or Process the Government Data as required by this Schedule [◆] (*Security Management*); and

(iii) the Supplier has provided the Buyer with such information as the Buyer requires concerning:

(A) the entity;

(B) the arrangements with the entity; and

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

(iv) the Buyer has not given the Supplier a Prohibition Notice under paragraph 1.3.

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

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

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

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

1.3 The Buyer may by notice in writing at any time give notice to the Supplier that it and its Sub-contractors must not undertake or permit to be undertaken, the storage, access or Processing Buyer 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 Supplier, a Sub-contractor or a third-party entity (a "**Prohibition Notice**").

1.4 Where the Supplier or Sub-contractor, on the date of the Prohibition Notice undertakes any Relevant Activities affected by the notice, the Supplier must, and must procure that Sub-contractors, 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 Supplier must not engage Supplier Personnel, and must ensure that Subcontractors 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 Buyer 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 Buyer for such individuals or such roles as the Buyer may specify; or

(c) such other checks for the Supplier Personnel of Sub-contractors as the Buyer may specify.

Annual training

2.3 The Supplier must ensure, and ensure that Sub-contractors ensure, that all Supplier 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 Supplier must ensure, and ensure that Sub-contractors ensure, that individual Supplier Personnel can access only the Buyer Data necessary to allow individuals to perform their role and fulfil their responsibilities in the provision of the Services.

2.5 The Supplier must ensure, and ensure that Sub-contractors ensure, that where individual Supplier Personnel no longer require access to the Buyer Data or any part of the Buyer Data, their access to the Buyer Data or that part of the Buyer Data is revoked immediately when their requirement to access Buyer Data ceases.

2.6 Where requested by the Buyer, the Supplier must remove, and must ensure that Sub-contractors remove, an individual Supplier Personnel's access to the Buyer Data or part of that Buyer Data specified by the Buyer as soon as practicable and in any event within 24 hours of the request.

Exception for certain Sub-contractors

2.7 Where the Supplier 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 Buyer;

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

(c) comply, at the Supplier's cost, with all directions the Buyer 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 Buyer has assessed that this Agreement is a higher-risk consultancy agreement.

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

3.2 The Supplier must, at the Buyer's option, before providing the Services and when reasonably requested by the Buyer, either:

(a) conduct security testing of the Supplier 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 Supplier Information Management System and the delivery of the Services; and

(iii) providing the Buyer 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 Supplier; or

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

(i) the parts of the Supplier Information Management System tested;

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

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

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

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

(a) before Processing Buyer data where the vulnerability is discovered before the Supplier begins to process Authority Data;

(b) where the vulnerability is discovered when the Supplier has begun to Process Buyer Data:

(i) by the date agreed with the Buyer; 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 Supplier must manage, and must ensure that all Sub-contractors manage, all End-user Devices on which Buyer Data is stored or processed in accordance the following requirements:

(a) the operating system and any applications that store, process or have access to Buyer 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 Buyer Data must be encrypted using a encryption tool agreed to by the Buyer;

(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 Buyer Data;

(f) the Suppler or Sub-contractor, as applicable, can, without physical access to the End-user Device, remove or make inaccessible all Buyer 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 Supplier

4.2 The Supplier 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 [x] (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 Supplier must ensure, and must ensure that all Sub-contractors ensure, that Buyer 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 Supplier, or a Sub-contractor, cannot encrypt Buyer Data as required by paragraph 5.1, the Supplier must:

(a) immediately inform the Buyer of the subset or subsets of Buyer 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 Supplier or Sub-contractor (as applicable) proposes to take to provide equivalent protection to the Buyer as encryption;

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

5.3 The Buyer, the Supplier and, where the Buyer requires, any relevant Sub-contractor shall meet to agree appropriate protective measures for the unencrypted Buyer Data.

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

Where the Buyer and Supplier reach agreement, the Supplier must update the Security Management Plan to include:

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

(b) the protective measure that the Supplier and/or Sub-contractor will put in please in respect of the unencrypted Buyer Data.

5.5 Where the Buyer and Supplier do not reach agreement within 40 Working Days of the date on which the Supplier first notified the Buyer that it could not encrypt certain Buyer 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 Supplier must, and must ensure that all Sub-contractors:

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

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

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

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

6.2 The Supplier must ensure, and must ensure that all Sub-contractors ensure, that the user accounts for Privileged Users of the Supplier 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 Supplier Information Management System after a period of time that is proportionate to the risk environment during which the account is inactive.

6.3 The Supplier 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 Supplier Information Management System.

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

(a) configure any hardware that forms part of the Supplier 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 Supplier shall install and maintain Anti-virus Software or procure that Anti-virus Software is installed and maintained on the Supplier Information Management System.

7.2 The Supplier shall ensure that such Anti-virus Software:

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

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

(c) where Malicious Software has been introduced into the Supplier 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 Buyer 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 Supplier where the Malicious Software originates from the Supplier Software, any third-party software licenced by the Supplier or the Buyer Data (whilst the Buyer Data was under the control of the Supplier) unless the Supplier can demonstrate that such Malicious Software was present and not quarantined or otherwise identified by the Buyer when provided to the Supplier; and

(b) by the Buyer, 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 Supplier 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 Buyer, following the Breach of Security or attempted Breach of Security, provide to the Buyer full details of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

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

9 Sub-contractors

The Supplier 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 Buyer at the Buyer's request.

10 Third-party Software

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

11 Deletion of Buyer Data

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