UK Research and Innovation

NEC4 Facilities Management Contract for UKRI

UKRI-3313 - STFC Fire Extinguisher, Fire Door and Fire Damper Maintenance for UKRI

via

KCS Framework Y23025 Lot 1 (Fire Safety Products and Associated Services)

UK Research and Innovation

Contents

UK Research and Innovation

STFC Fire Extinguisher, Fire Door and Fire Damper Maintenance for UKRI

UKRI-3313

Contract Data

Contract Data

PART ONE – DATA PROVIDED BY THE *CLIENT*

Completion of the data in full, according to the Options chosen, is essential to create a complete contract.

1 General

The *conditions of contract* are the core clauses and the clauses for the following main Option, the Option for resolving and avoiding disputes and secondary Options of the NEC4 Facilities Management Contract June 2021 (with amendments January 2023)

Main Options: A — Option for resolving and avoiding disputes: W2

Secondary Options: X1, X8, X18, X19, X21, X23, X27, Y(UK)2 and Z clauses

The *service* is: Planned, Preventative Maintenance (PPM), reactive and remedial works pertaining to Fire extinguisher, doors and dampers across the UKRI, STFC sites stated in the Specification.

The *Client* is

Name: UK Research and Innovation

Address for communications: Polaris House, North Star Avenue, Swindon, SN2 1SZ

Address for electronic communications: STFCProcurement@ukri.org

The *Service Manager* is: FOIA Section 40 Personal Information

Name

Address for communications: UKRI, Science and Technology Facilities Council, Rutherford Appleton Laboratory, Harwell Campus, Didcot, OX11 0QX, UK

Address for electronic communications: TBC

The Affected Property is: UKRI, Science and Technology Facilities Council, Rutherford Appleton Laboratory, Harwell Campus, Didcot, OX11 0QX, UK
The Cosener's House, 15 - 16 Abbey Close, Abingdon, Oxfordshire, OX14 3JD, UK

The Scope is in: UKRI-3313 Specification

The *shared services* which may be carried out outside the Service Areas are

The *language of the contract* is English

The *law of the contract* is the law of England and Wales

The *period for reply* is 5 working days except that

- The *period for reply* for _____ is _____
- The *period for reply* for _____ is _____

The following matters will be included in the Early Warning Register

Any resource, capacity or supply issue that may delay or prevent the Service from being completed successfully.

Early warning meetings are to be held at intervals no longer than 12 weeks

2 The *Service Provider's* main responsibilities

If Option C or E is used

The *Service Provider* prepares forecasts of the total Defined Cost for the whole of the *service* at intervals no longer than

3 Time

The *starting date* is 02 April 2024

The *service period* is Up to 4 years (2+1+1)

The *Service Provider* submits revised plans at intervals no longer than

If no plan is identified in part two of the Contract Data

The period after the Contract Date within which the *Service Provider* is to submit a first plan for acceptance is

If a mobilisation plan is required, and no mobilisation plan is identified in part two of the Contract Data

The period after the Contract Date within which the *Service Provider* is to submit a mobilisation plan for acceptance is 1 week

The period after the Contract Date within which the *Service Provider* is to submit a first demobilisation plan for acceptance is

60 days

4 Quality management

The period after the Contract Date within which the *Service Provider* is to submit a quality policy statement and quality plan is

5 Payment

The *currency of the contract* is the GBP Sterling

The *assessment interval* is Monthly

The *interest rate* is _____ % per annum (not less than 2) above the _____ rate of the _____ bank

If the period in which payments are made is not three weeks and Y(UK)2 is not used

The period within which is payments are made is _____

The *performance table* is in _____

If the period for certifying a final assessment is not thirteen weeks

The period for certifying a final assessment is _____

If Option C is used

The *Service Provider's share percentages* and the *share ranges* are

share range				*Service Provider's share percentage*
less than			%	%
from	%	to	%	%
from	%	to	%	%
greater than			%	%

The *Service Provider's* share is assessed on (dates)

If Option C or E is used

The *exchange rates* are those published in _____

on _____ (date)

6 Compensation events

If Option A is used

The *efficiency percentage* is 50%, unless another percentage is stated here, in which case it is [ ] %

If there are additional compensation events

These are additional compensation events

[ ]

8 Liabilities and insurance

If there are additional *Client's* liabilities

These are additional *Client's* liabilities

(1) [ ]

(2) [ ]

(3) [ ]

The minimum amount of cover for insurance against loss of or damage to property (except Plant and Materials, Equipment and equipment provided by the *Client* to the *Service Provider*) and liability for bodily injury to or death of a person (not an employee of the *Service Provider*) arising from or in connection with the *Service Provider* Providing the Service for any one event is [ ]

The minimum amount of cover for insurance against death of or bodily injury to employees of the *Service Provider* arising out of and in the course of their employment in connection with the contract for any one event is [ ]

If the *Client* is to provide Plant and Materials

The insurance against loss of or damage to Plant and Materials, Equipment and the *Client's* equipment is to include cover for Plant and Materials provided by the *Client* for an amount of [ ]

If the *Client* is to provide equipment

The insurance against loss of or damage to Plant and Materials, Equipment and the *Client's* equipment is to include cover for equipment provided by the *Client* for an amount of [ ]

If the *Service Provider* is liable for loss of or damage to any property owned or occupied by the *Client,* other than the Affected Property

The *Service Provider* is liable for loss of or damage to any property owned or occupied by the *Client,* other than the Affected Property, arising from or in connection with the *Service Provider* Providing the Service. The minimum amount of cover for insurance for any one event is [£10M]

If the *Service Provider* is liable for loss of or damage to the Affected Property

The *Service Provider* is liable for loss of or damage to the Affected Property arising from or in connection with the *Service Provider* Providing the Service. The minimum amount of cover for insurance for any one event is [£10M]

If the *Client* is to provide any of the insurances stated in the Insurance Table

The *Client* provides these insurances from the Insurance Table

(1) Insurance against [ ]

Minimum amount of cover is [ ]

The deductibles are [ ]

(2) Insurance against

Minimum amount of cover is

The deductibles are

(3) Insurance against

Minimum amount of cover is

The deductibles are

If additional insurances are to be provided

The *Client* provides these additional insurances

(1) Insurance against

Minimum amount of cover is

The deductibles are

(2) Insurance against

Minimum amount of cover is

The deductibles are

(3) Insurance against

Minimum amount of cover is

The deductibles are

The *Service Provider* provides these additional insurances

(1) Insurance against

Minimum amount of cover is

The deductibles are

(2) Insurance against

Minimum amount of cover is

The deductibles are

(3) Insurance against

Minimum amount of cover is

The deductibles are

Resolving and avoiding disputes

The *tribunal* is: The Courts of England and Wales

If the *tribunal* is arbitration

The *arbitration procedure* is

The place where arbitration is to be held is

The person or organisation who will choose an arbitrator if the Parties cannot agree a choice or if the *arbitration procedure* does not state who selects an arbitrator is

The *Senior Representatives* of the *Client* a

Name (1) [redacted]

Address for communications: UKRI Procurement, Rutherford Appleton Laboratory, Harwell, Oxford, OX11 0QX

Address for electronic communications: STFCProcurement@ukri.org

Name (2)

Address for communications: UKRI Commercial, North Star Avenue, Swindon, SN2 1EU

Address for electronic communications: Commercial@ukri.org

The *Adjudicator* is

Name

Address for communications

Address for electronic communications

The *Adjudicator nominating body* is: The Royal Institution of Chartered Surveyors

X1: Price adjustment for inflation (used only with Options A and C)

If Option X1 is used

The proportions used to calculate the Price Adjustment Factor are

0.		linked to the index for	
0.			
0.			
0.			
0.			
0.			
0.		non-adjustable	
1.00			

The *base date* for indices is: The Start Date

The *inflation adjustment dates* are

These indices are: Consumer Price Index (CPI)

X3: Multiple currencies (used only with Option A)

If Option X3 is used

The *Client* will pay for the items or activities listed below in the currencies stated

items and activities	other currency	total maximum payment in the currency

The *exchange rates* are those published in

on (date)

X4: Performance guarantee

If Option X4 is used

The *Service Provider* **provides an ultimate holding company guarantee/provides a performance bond** (Delete as applicable)

If a performance bond is provided

The amount of the performance bond is

X8: Undertakings to the *Client* or Others

If Option X8 is used

The *undertakings to Others* are

provided to

The authority or agency named in each Task Order

The *Subcontractor undertaking to Others* are

works	provided to

The *Subcontractor undertaking to the Client* are

works

X10: Information modelling

If Option X10 is used

If no *information execution plan* is identified in part two of the Contract Data

The period after the Contract Date within which the *Service Provider* is to submit a first Information Execution Plan for acceptance is

The minimum amount of insurance cover for claims made against the *Service Provider* arising out of its failure to use the skill and care normally used by professionals providing information similar to the Project Information is, in respect of each claim

The period following the end of the Service Period or earlier termination for which the *Service Provider* maintains insurance for claims made against it arising out of its failure to use the skill and care is

X12: Multiparty collaboration

If Option X12 is used

The *Promoter is*

The Schedule of Partners is in

The *Promoter's objective* is

The Partnering Information is in

X15: The *Service Provider's* design

If Option X15 is used

The *period for retention* following the end of the Service Period or earlier termination is

The minimum amount of insurance cover for claims made against the *Service Provider* arising out of its failure to use the skill and care normally used by professionals designing service similar to the *service* is, in respect of each claim

The period following the end of the Service Period or earlier termination for which the *Service Provider* maintains insurance for claims made against it arising out of its failure to use the skill and care is

X18: Limitation of liability

If Option X18 is used

The *Service Provider's* liability to the *Client* for indirect or consequential loss is limited to £10M

If the *Service Provider* is liable for loss of or damage to any property owned or occupied by the *Client*, other than the Affected Property, the *Service Provider's* liability to the *Client* for loss of or damage to any property owned or occupied by the *Client*, other than the Affected Property, for any one event is limited to £10M

If the *Service Provider* is liable for loss of or damage to the Affected Property, the *Service Provider's* liability to the *Client* for loss of or damage to the Affected Property for any one event is limited to £10M

If Option X15 applies, the *Service Provider's* liability for Service Failures due to its design is limited to

The *Service Provider's* total liability to the *Client* for all matters arising under or in connection with the contract, other than excluded matters, is limited to £10M

The *end of liability date* is 6 years after the end of the Service Period

X19: Termination by either Party (not used with Option X11)

If Option X19 is used

The *minimum period of service* is 2 years after the *starting date*

The *notice period* is 3 months

X23: Extending the Service Period

If Option X23 is used

The *maximum service period* is 4 years after the *starting date*

The *periods for extension* are

Order	*period for extension* (months)	*notice date*
First	12	3 months
Second	12	3 months

Third		
Fourth		

If there are *criteria for extension*

The *criteria for extension* are

(1)

(2)

(3)

X24: The *accounting periods*

Option X24 is used and Option C is not used

The *accounting periods* are

If Option X24 is used with Option C

The *accounting periods* are the dates stated in the Contract Data of assessment of the *Service Provider's* share

X27: Project Orders

If Option X27 is used

The period within which the *Service Provider* is to submit a Project Order programme for acceptance is 7 days

X28: Change of Control

If Option X28 is used

The required financial position of the controller of the *Service Provider* is in

The *ethical principles of the Client* are in

X29: Climate change

If Option X29 is used

If no *climate change plan* is identified in part two of the Contract Data

The period after the Contract Date within which the *Service Provider* is to submit a first climate change plan for acceptance is

Y(UK)1: Project Bank Account

If Option Y(UK)1 is used

The *Service Provider* **is/is not** to pay any charges made and to be paid any interest paid by the *project bank* (Delete as applicable)

The *account holder* is the ***Service Provider*/the Parties** (Delete as applicable)

Y(UK)2: The Housing Grants, Construction and Regeneration Act 1996

If Y(UK)2 is used and the date on which the final payment becomes due is not fifteen weeks after the end of the Service Period

The period is [ ] weeks

If Y(UK)2 is used and the final date for payment is not seven days after the date on which payment becomes due

The period for payment is [ ] days after the date on which payment becomes due

Y(UK)3: The Contracts (Rights of Third Parties) Act 1999

If Option Y(UK)3 is used

term	*beneficiary*

If Y(UK)3 is used with Y(UK)1 the following entry is added to the table for Y(UK)3

term	*beneficiary*
The provisions of Options Y(UK)1	Named Suppliers

Z: *Additional conditions of contract*

If Option Z is used

The *additional conditions of contract* are

As per the Z clauses listed at the foot of this contract.

PART TWO – DATA PROVIDED BY THE *SERVICE PROVIDER*

Completion of the data in full, according to the Options chosen, is essential to create a complete contract.

1 General

The *Service Provider* is

Name: Stand-By Fire Protection

Address for communications: Kestrel House, Garth Road, Morden, SM4 4LP

Address for electronic communication: FOIA Section 40 Personal Information

The *fee percentage* is: %

The *service areas* are:

The *key persons* are

Name (1): FOIA Section 40 Personal Information

Job: Sales

Responsibilities:

Qualifications:

Experience:

Name (2): FOIA Section 40 Personal Information

Job:

Responsibilities:

Qualifications:

Experience:

The following matters will be included in the Early Warning Register

2 The *Service Provider's* main responsibilities

If the *Service Provider* is to provide Scope for its plan	The Scope provided by the *Service Provider* for its plan is in	

3 Time

If a plan is to be identified in the Contract Data	The plan identified in the Contract Data is	
If a mobilisation plan is to be identified in the Contract Data	The mobilisation plan identified in the Contract Data is	

5 Payment

If Option A, C or E is used	The *price list* is	As Per the Price List below
If Option A or C is used	The tendered total of the Prices is	As per the Price List in this Contract The Contract shall not exceed £560,000.00 GBP ex VAT for the full potential duration.

Resolving and avoiding disputes

The *Senior Representatives* of the *Service Provider* are

Name (1)	
Address for communications	
Address for electronic communications	
Name (2)	
Address for communications	
Address for electronic communications	

X10: Information modelling

If Option X10 is used

If an *information execution plan* is to be identified in the Contract Data	The *information execution plan* identified in the Contract Data is	

The rates for Defined Cost of manufacture and fabrication outside the Service Areas by the *Service Provider* are

category of person	rate

The rates for people providing *shared services* outside the Service Areas are

shared service	category of person	rate

Data for the Short Schedule of Cost Components (used only with Option A)

The *people rates* are

category of person	unit	rate

The published list of Equipment is the edition current at the Contract Date of the list published by

The percentage for adjustment for Equipment in the published list is [ ] % (state plus or minus)

The rates for other Equipment are

Equipment	rate

The rates for Defined Cost of manufacture and fabrication outside the Service Areas by the *Service Provider* are

category of person	rate

The rates for people providing *shared services* outside the Service Areas are

shared service	category of person	rate

UK Research and Innovation

STFC Fire Extinguisher, Fire Door and Fire Damper Maintenance for UKRI

UKRI-3313
Schedule of Amendments to NEC Contract

UK Research and Innovation

Option Z2 - Identified and defined terms

Insert new clause 11.3 additional defined terms.

11.3 (1) Client Confidential Information is all Personal Data and any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel, and contractors of the *Client*, including all IPRs, together with all information derived from any of the above, and any other information clearly designated as being confidential (whether or not it is marked "confidential") or which ought reasonably be considered to be confidential.

11.3 (2) Client Data is the 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, and

- which are supplied to the *Contractor* by or on behalf of the *Client*,
- which the *Contractor* is required to generate, process, store or transmit pursuant to this contract or
- which are any Personal Data for which the *Client* is the Data Controller to the extent that such Personal Data is held or processed by the Contractor.

11 (3) Commercially Sensitive Information is the information agreed between the Parties (if any) comprising the information of a commercially sensitive nature relating to the *Contractor*, the charges for the works, its IPR or its business or which the *Contractor* has indicated to the *Client* that, if disclosed by the *Client*, would cause the *Contractor* significant commercial disadvantage or material financial loss.

11.3 (4) Confidential Information is the Client's Confidential Information and/or the Contractor's Confidential Information.

11.3 (5) Contracting Body is any Contracting Body as defined in Regulation 5(2) of the Public Contracts (Services, Service and Supply) (Amendment) Regulations 2000 other than the Client.

11.3 (6) Contractor's Confidential Information is any information, however it is conveyed, that relates to the business, affairs, developments, trade secrets, know-how, personnel and contractors of the *Contractor*, including IPRs, together with all information derived from the above, and any other information clearly designated as being confidential (whether or not it is marked as "confidential") or which ought reasonably to be considered to be confidential, including the Commercially Sensitive Information.

11.3 (7) Crown Body is any department, office or agency of the Crown.

11.3 (8) Data Controller has the meaning given to it in the Data Protection Act 2018.

11.3 (9) DOTAS is the Disclosure of Tax avoidance Schemes rules which require a promoter of tax schemes to tell HM Revenue & Customs of any specified notable arrangements or proposals and to provide prescribed information on those arrangements or proposals within set time limits as contained in Part 7 of the Finance Act 2004 and in secondary legislation made under vires contained in Part 7 of the Finance Act 2004 and as extended to National Insurance Contributions by the National Insurance Contributions (Application of Part 7 of the Finance Act 2004) Regulations 2012, SI 2012/1868 made under s.132A Social Security Administration Act 1992.

11.3 (10) Environmental Information Regulations is the Environmental Information Regulations 2004, or if applicable, the Environmental Information Regulations (Scotland) (2004), and any guidance and/or codes of practice issued by the Information Commissioner in relation to such regulations.

11.3(11) FOIA is the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner in relation to such legislation.

11.3 (12) General Anti-Abuse Rule is

- the legislation in Part 5 of the Finance Act 2013 and
- any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements and to avoid national insurance contributions.

11.3 (13) Halifax Abuse Principle is the principle explained in the CJEU Case C-255/02 Halifax and others.

11.3 (14) Intellectual Property Rights or "IPRs" is

- copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information,
- applications for registration, and the right to apply for registration, for any of the rights listed in the first bullet point that are capable of being registered in any country or jurisdiction,
- all other rights having equivalent or similar effect in any country or jurisdiction and
- all or any goodwill relating or attached thereto.

11.3 (15) Law is any law, statute, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of section 2 of the European Communities Act 1972 and section 4 of the European Union (Withdrawal Act 2018), regulation, order, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the *Contractor* is bound to comply under the *law of*

the contract.

11.3(16) An Occasion of Tax Non-Compliance is

- where any tax return of the *Contractor* submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of
- a Relevant Tax Authority successfully challenging the *Contractor* under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle or
- the failure of an avoidance scheme which the *Contractor* was involved in, and which was, or should have been, notified to a Relevant Tax Authority under DOTAS or any equivalent or similar regime and

where any tax return of the *Contractor* submitted to a Relevant Tax Authority on or after 1 October 2012 gives rise, on or after 1 April 2013, to a criminal conviction in any jurisdiction for tax related offences which is not spent at the Contract Date or to a civil penalty for fraud or evasion.

11.3(17) Personal Data has the meaning given to it in the Data Protection Act 2018.

11.3 (18) Prohibited Act is

- to directly or indirectly offer, promise or give any person working for or engaged by the *Client* or other Contracting Body or any other public body a financial or other advantage to
  - induce that person to perform improperly a relevant function or activity or
  - reward that person for improper performance of a relevant function or activity,
- to directly or indirectly request, agree to receive or accept any financial or other advantage as an inducement or a reward for improper performance of a relevant function or activity in connection with this contract,
- committing any offence
  - under the Bribery Act 2010 (or any legislation repealed or revoked by such Act),
  - under legislation or common law concerning fraudulent acts or
  - defrauding, attempting to defraud or conspiring to defraud the *Client* or
- any activity, practice or conduct which would constitute one of the offences listed above if such activity, practice or conduct had been carried out in the UK.

11.3 (19) Request for Information is a request for information or an apparent request under the Code of Practice on Access to government Information, FOIA or the Environmental Information Regulations.

11.3 (20) Relevant Requirements are all applicable Laws relating to bribery, corruption and fraud, including the Bribery Act 2010 and any guidance issued by the Secretary of State for Justice pursuant to section 9 of the Bribery Act 2010.

11.3 (21) Relevant Tax Authority is HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the *Contractor* is established.

11.3 (22) Security Policy means the *Client*'s security policy attached as Appendix 1 to Contract Schedule A (Security Provisions) as may be updated from time to time.

Option Z 4 - Admittance to *site*

Insert new clause 19A:

19A.1 The *Contractor* submits to the *Service Manager* details of people who are to be employed by it and its Subcontractors in Providing the Services. The details include a list of names and addresses, the capabilities in which they are employed, and other information required by the *Service Manager*.

19A.2 The *Service Manager* may instruct the *Contractor* to take measures to prevent unauthorised persons being admitted to the Affected Property.

19A.3 Employees of the *Contractor* and its Subcontractors are to carry a *Client's* pass and comply with all conduct requirements from the *Client* whilst they are on the parts of the Affected Property identified in the Scope.

19A.4 The *Contractor* submits to the *Service Manager* for acceptance a list of the names of the people for whom passes are required. On acceptance, the *Service Manager* issues the passes to the *Contractor*. Each pass is returned to the *Service Manager* when the person no longer requires access to that part of the Affected Property or after the *Service Manager* has given notice that the person is not to be admitted to the Affected Property.

19A.5 The *Contractor* does not take photographs of the Affected Property or of work carried out in connection with the *works* unless it has obtained the acceptance of the *Service Manager*.

19A.6 The *Contractor* takes the measures needed to prevent its and its Subcontractors' people taking, publishing or otherwise circulating such photographs.

Option Z5 - Prevention of fraud and bribery

Insert new clauses:

18.4.1 The *Contractor* represents and warrants that neither it, nor to the best of its knowledge any of its people, have at any time prior to the Contract Date

- committed a Prohibited Act or been formally notified that it is subject to an investigation or prosecution which relates to an alleged Prohibited Act or

- been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act.

18.4.2 During the carrying out of the *works* the *Contractor* does not

- commit a Prohibited Act and
- do or suffer anything to be done which would cause the *Client* or any of the *Client's*

employees, consultants, contractors, sub-contractors or agents to contravene any of the Relevant Requirements or otherwise incur any liability in relation to the Relevant Requirements.

18.4.3 In Providing the Services the *Contractor*

- establishes, maintains and enforces, and requires that its Subcontractors establish, maintain and enforce, policies and procedures which are adequate to ensure compliance with the Relevant Requirements and prevent the occurrence of a Prohibited Act,

- keeps appropriate records of its compliance with this contract and make such records available to the *Client* on request and

- provides and maintains and where appropriate enforces an anti-bribery policy (which shall be disclosed to the *Client* on request) to prevent it and any *Contractor's* people or any person acting on the *Contractor's* behalf from committing a Prohibited Act.

18.4.4 The *Contractor* immediately notifies the *Client* in writing if it becomes aware of any breach of clause 18.4.1, or has reason to believe that it has or any of its people or Subcontractors have

- been subject to an investigation or prosecution which relates to an alleged Prohibited Act,

- been listed by any government department or agency as being debarred, suspended, proposed for suspension or debarment, or otherwise ineligible for participation in government procurement programmes or contracts on the grounds of a Prohibited Act or

- received a request or demand for any undue financial or other advantage of any kind in connection with the performance of this contract or otherwise suspects that any person or party directly or indirectly connected with this contract has committed or attempted to commit a Prohibited Act.

18.4.5 If the *Contractor* makes a notification to the *Client* pursuant to clause 18.4.4, the *Contractor* responds promptly to the *Client's* enquiries, co-operates with any investigation, and allows the *Client* to audit any books, records and/or any other relevant documentation in accordance with this contract.

18.4.6 If the *Contractor* breaches Clause 18.4.3, the *Client* may by notice require the *Contractor* to remove from carrying out the *works* any person whose acts or omissions have caused the *Contractor*'s breach.

Option Z7 - Legislation and Official secrets

Insert new clauses:

20.5 The *Contractor* complies with Law in the carrying out of the *works.*

UK Research and Innovation

Option Z10 - Freedom of information

Insert new clauses:

29.3 The *Contractor* acknowledges that unless the *Service Manager* has notified the *Contractor* that the *Client* is exempt from the provisions of the FOIA, the *Client* is subject to the requirements of the Code of Practice on Government Information, the FOIA and the Environmental Information Regulations. The *Contractor* cooperates with and assists the *Client* so as to enable the *Client* to comply with its information disclosure obligations.

29.4 The *Contractor*

- transfers to the *Service Manager* all Requests for Information that it receives as soon as practicable and in any event within two working days of receiving a Request for Information,
- provides the *Service Manager* with a copy of all information in its possession, or power in the form that the *Service Manager* requires within five working days (or such other period as the *Service Manager* may specify) of the *Service Manager's* request,
- provides all necessary assistance as reasonably requested by the *Service Manager*to enable the *Client* to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations and
- procures that its Subcontractors do likewise.

29.5 The *Client* is responsible for determining in its absolute discretion whether any information is exempt from disclosure in accordance with the provisions of the Code of Practice on Government Information, FOIA or the Environmental Information Regulations.

29.6 The *Contractor* does not respond directly to a Request for Information unless authorised to do so by the *Service Manager*.

29.7 The *Contractor* acknowledges that the *Client* may, acting in accordance with the Department of Constitutional Affairs' Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of information Act 2000, be obliged to disclose information without consulting or obtaining consent from the *Contractor* or despite the *Contractor* having expressed negative views when consulted.

29.8 The *Contractor* ensures that all information is retained for disclosure throughout the *period for retention* and permits the *Service Manager* to inspect such records as and when reasonably requested from time to time.

Option Z13 - Confidentiality and Information Sharing

UK Research and Innovation

Insert a new clause

29.9 Except to the extent set out in this clause or where disclosure is expressly permitted elsewhere in this contract, each Party shall

- treat the other Party's Confidential Information as confidential and safeguard it accordingly,
- not disclose the other Party's Confidential Information to any other person without prior written consent,
- immediately notify the other Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information and
- notify the Serious Fraud Office where the Party has reasonable grounds to believe that the other Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

29.10 The clause above shall not apply to the extent that

- such disclosure is a requirement of the Law placed upon the party making the disclosure, including any requirements for disclosure under the FOIA or the Environmental Information Regulations pursuant to clause Z10 (Freedom of Information),
- such information was in the possession of the party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner,
- such information was obtained from a third party without obligation of confidentiality,
- such information was already in the public domain at the time of disclosure otherwise than by a breach of this contract or
- it is independently developed without access to the other party's Confidential Information.

29.11 The *Contractor* may only disclose the *Client's* Confidential Information to the people who are directly involved in Providing the Services and who need to know the information, and shall ensure that such people are aware of and shall comply with these obligations as to confidentiality.

The *Contractor* shall not, and shall procure that the *Contractor's* people do not, use any of the Client Confidential Information received otherwise than for the purposes of this contract.

29.12 The *Contractor* may only disclose the Client Confidential Information to *Contractor's* people who need to know the information, and shall ensure that such people are aware of, acknowledge the importance of, and comply with these obligations as to confidentiality. In the event that any default, act or omission of any *Contractor's* people causes or contributes (or could cause or contribute) to the *Contractor* breaching its obligations as to confidentiality under or in connection with this contract, the *Contractor* shall take such action as may be appropriate in the circumstances, including the use of disciplinary procedures in serious cases. To the fullest extent permitted by its own obligations of confidentiality to any *Contractor's* people , the *Contractor* shall provide such evidence to the *Client* as the *Client* may reasonably require (though not so as to risk compromising or prejudicing the case) to demonstrate that the *Contractor* is taking appropriate steps to comply with this clause, including copies of any written communications to and/or from *Contractor's* people, and any minutes of meetings and any other records which provide an audit trail of any discussions or exchanges with *Contractor's* people in connection with obligations as to confidentiality.

29.13 At the written request of the *Client*, the *Contractor* shall procure that those members of the *Contractor's* people identified in the *Client*'s request signs a confidentiality undertaking prior to commencing any work in accordance with this contract.

29.14 Nothing in this contract shall prevent the *Client* from disclosing the *Contractor*'s Confidential Information

- to any Crown Body or any other Contracting Bodies. All Crown Bodies or Contracting Bodies receiving such Confidential Information shall be entitled to further disclose the Confidential Information to other Crown Bodies or other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown Body or any Contracting Body,

- to a professional adviser, contractor, consultant, supplier or other person engaged by the *Client* or any Crown Body (including any benchmarking organisation) for any purpose connected with this contract, or any person conducting an Office of Government Commerce Gateway Review,

- for the purpose of the examination and certification of the *Client*'s accounts,

- for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the *Client* has used its resources,

- for the purpose of the exercise of its rights under this contract or

- to a proposed successor body of the *Client* in connection with any assignment, novation or disposal of any of its rights, obligations or liabilities under this contract,

and for the purposes of the foregoing, disclosure of the Contractor's Confidential Information shall

be on a confidential basis and subject to a confidentiality agreement or arrangement containing terms no less stringent than those placed on the *Client* under this clause 29.14.

29.15 The *Client* shall use all reasonable endeavours to ensure that any government department, Contracting Body, people, third party or subcontractor to whom the *Contractor*'s Confidential Information is disclosed pursuant to the above clause is made aware of the *Client*'s obligations of confidentiality.

29.16 Nothing in this clause shall prevent either party from using any techniques, ideas or know-how gained during the performance of the contract in the course of its normal business to the extent that this use does not result in a disclosure of the other party's Confidential Information or an infringement of IPR.

29.17 The *Client* may disclose the Confidential Information of the *Contractor*

- to Parliament and Parliamentary Committees or if required by any Parliamentary reporting requirement,
- to the extent that the *Client* (acting reasonably) deems disclosure necessary or appropriate in the course of carrying out its public functions,

Option Z14 - Security Requirements

The *Contractor* complies, and procures the compliance of the *Contractor's* people, with any Security Policy and arrangements made known by the Contracting Authority, and the Security Management Plan produced by the *Contractor* and the *Contractor* shall ensure that the Security Management Plan fully complies with the Security Policy and Contract Schedule A.

Option Z15 – Key Performance Indicators

Delete clause X20.4 and insert:

X20.4 The reference to incentive schedule and Key Performance Schedule are for the purposes of interpretation in the documents forming part of this contract the same.

X20.4(a). The Contractor is paid the price for services provided to date less the sum calculated for deduction by the KPI schedule in the Scope. The sum for deduction is assessed at the next assessment date following the Contractors reporting of the performance criteria. A sum deducted in error is included in the amount due at the next assessment date after it is agreed that the deduction was in error.

X20.4(b) If the Contractor fails to provide the key performance data required for the Service Managers assessment, the Service Manager assesses a deduction from the amount due for that assessment as the greater of:

- The deduction from the last assessment, or

- The Service Managers assessment of the deduction for the period, as notified to the Contractor with supporting calculations.

Option Z16 - Tax Compliance

Insert new clauses:

29.18 The *Contractor* represents and warrants that at the Contract Date, it has notified the *Client* in writing of any Occasions of Tax Non-Compliance or any litigation that it is involved in that is in connection with any Occasions of Tax Non-Compliance.

29.19 If, at any point prior to the *defects date*, an Occasion of Tax Non-Compliance occurs, the *Contractor* shall

- notify the *Client* in writing of such fact within 5 days of its occurrence and
- promptly provide to the *Client*
    - details of the steps which the *Contractor* is taking to address the Occasions of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant and
    - such other information in relation to the Occasion of Tax Non-Compliance as the *Client* may reasonably require.

29.20 The relationship between Client and the Contractor shall be that of "independent contractor" which means that the Contractor is not a Client employee, worker, agent or partner, and the Contractor shall not give the impression that they are. As this is not an employment Contract, the Contractor shall be fully responsible for all their own tax, including any national insurance contributions arising from carrying out the Services.

Option Z22 - Fair payment

Insert a new clause:

57.1 The *Contractor* assesses the amount due to a Subcontractor without taking into account the amount certified by the *Service Manager*.

57.2 The *Contractor* includes in the contract with each Subcontractor

- a period for payment of the amount due to the Subcontractor not greater than 5 days after the final date for payment in this contract. The amount due includes, but is not limited to, payment for work which the Subcontractor has completed from the previous assessment date up to the current assessment date in this contract,
- a provision requiring the Subcontractor to include in each subsubcontract the same requirement (including this requirement to flow down, except that the period for payment is to be not greater than 9 days after the final date for payment in this contract and

- a provision requiring the Subcontractor to assess the amount due to a subsubcontractor without taking into account the amount paid by the *Contractor.*

Option Z42 - The Housing Grants, Construction and Regeneration Act 1996

Add an additional clause Y2.6

Y2.6

If Option Y(UK)2 is said to apply then notwithstanding that this contract relates to the carrying out of construction operations other than in England or Wales or Scotland, the Act is deemed to apply to this contract.

Option Z44 - Intellectual Property Rights

Delete clause 22 and insert the following clause

In this clause 22 only:

"Document" means all designs, drawings, specifications, software, electronic data, photographs, plans, surveys, reports, and all other documents and/or information prepared by or on behalf of the *Contractor* in relation to this contract.

22.1 The Intellectual Property Rights in all Documents prepared by or on behalf of the *Contractor* in relation to this contract and the work executed from them remains the property of the *Contractor*. The *Contractor* hereby grants to the *Client* an irrevocable, royalty free, non-exclusive licence to use and reproduce the Documents for any and all purposes connected with the construction, use, alterations or demolition of the *works*. Such licence entitles the *Client* to grant sub-licences to third parties in the same terms as this licence provided always that the *Contractor* shall not be liable to any licencee for any use of the Documents or the Intellectual Property Rights in the Documents for purposes other than those for which the same were originally prepared by or on behalf of the *Contractor*.

22.2 The *Client* may assign novate or otherwise transfer its rights and obligations under the licence granted pursuant to 22.1 to a Crown Body or to anybody (including any private sector body) which performs or carries on any functions and/or activities that previously had been performed and/or carried on by the *Client*.

22.3 In the event that the *Contractor* does not own the copyright or any Intellectual Property Rights in any Document the *Contractor* uses all reasonable endeavours to procure the right to grant such rights to the *Client* to use any such copyright or Intellectual Property Rights from any third party owner of the copyright or Intellectual Property Rights. In the event that the *Contractor* is unable to procure the right to grant to the *Client* in accordance with the foregoing the *Contractor*

procures that the third party grants a direct licence to the *Client* on industry acceptable terms.

22.4 The *Contractor* waives any moral right to be identified as author of the Documents in accordance with section 77, Copyright Designs and Patents Acts 1988 and any right not to have the Documents subjected to derogatory treatment in accordance with section 8 of that Act as against the *Client* or any licensee or assignee of the *Client*.

22.5 In the event that any act unauthorised by the *Client* infringes a moral right of the *Contractor* in relation to the Documents the *Contractor* undertakes, if the *Client* so requests and at the *Client*'s expense, to institute proceedings for infringement of the moral rights.

22.6 The *Contractor* warrants to the *Client* that it has not granted and shall not (unless authorised by the *Client*) grant any rights to any third party to use or otherwise exploit the Documents.

22.7 The *Contractor* supplies copies of the Documents to the *Service Manager* and to the *Client*'s other contractors and consultants for no additional fee to the extent necessary to enable them to discharge their respective functions in relation to this contract or related works.

22.8 After the termination or conclusion of the *Contractor*'s employment hereunder, the *Contractor* supplies the *Service Manager* with copies and/or computer discs of such of the Documents as the *Service Manager* may from time to time request and the *Client* pays the *Contractor*'s reasonable costs for producing such copies or discs.

22.9 In carrying out the *works* the *Contractor* does not infringe any Intellectual Property Rights of any third party. The *Contractor* indemnifies the *Client* against claims, proceedings,

compensation and costs arising from an infringement or alleged infringement of the Intellectual Property Rights of any third party.

Option Z47 - Small and Medium Sized Enterprises (SMEs)

Insert new clause:

26.5

The *Contractor* is required to take all reasonable steps to engage SMEs as Subcontractors and to seek to ensure that no less than the SME percentage of Subcontractors stated in the Contract Data are SMEs or that a similar proportion of the Defined Cost is undertaken by SMEs.

The *Contractor* is required to report to the *Client* in its regular contract management monthly reporting cycle the numbers of SMEs engaged as Subcontractors and the value of the Defined Cost that has been undertaken by SMEs.

Where available, the *Contractor* is required to tender its Subcontracts using the same online electronic portal as was provided by the *Client* for the purposes of tendering this contract.

The *Contractor* is to ensure that the terms and conditions used to engage Subcontractors are no less favourable than those of this contract. A reason for the *Service Manager* not accepting subcontract documents proposed by the *Contractor* is that they are unduly disadvantageous to the Subcontractor.

Option Z48 - Apprenticeships

Insert new clause:

26.6

The *Contractor* takes all reasonable steps to employ apprentices, and reports to the *Client* the numbers of apprentices employed and the wider skills training provided, during the delivery of the *service*.

The *Contractor* takes all reasonable steps to ensure that no less than a percentage of its people (agreed between the Parties) are on formal apprenticeship programmes or that a similar proportion of hours worked in Providing the Services, (which may include support staff and Subcontractors) are provided by people on formal apprenticeship programmes.

The *Contractor* makes available to its people and Subcontractors working on the contract, information about the Government's Apprenticeship programme and wider skills opportunities.

The *Contractor* provides any further skills training opportunities that are appropriate for its people engaged in Providing the Services.

The *Contractor* provides a report detailing the following measures in its regular contract management monthly reporting cycle and is prepared to discuss apprenticeships at its regular meetings with the *Service Manager*

- the number of people during the reporting period employed on the contract, including support staff and Subcontractors,
- the number of apprentices and number of new starts on apprenticeships directly initiated through this contract,
- the percentage of all people taking part in an apprenticeship programme,
- if applicable, an explanation from the *Contractor* as to why it is not managing to meet the specified percentage target,
- actions being taken to improve the take up of apprenticeships and
- other training/skills development being undertaken by people in relation to this contract, including:

  (a) work experience placements for 14 to 16 year olds,

  (b) work experience /work trial placements for other ages,

  (c) student sandwich/gap year placements,

  (d) graduate placements,

  (e) vocational training,

  (f) basic skills training and

  (g) on site training provision/ facilities.

UK Research and Innovation

SCHEDULE A

1. CONTRACT SCHEDULE J - SECURITY PROVISIONS

1.1 Definitions

For the purposes of this schedule the following terms shall have the meanings given below:

"Affiliates"	in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time;
"Breach of Security"	in accordance with the Security Requirements and the Security Policy, the occurrence of: (a) any unauthorised access to or use of the works the Client Premises, the Affected Properties, the Contractor System and/or any ICT, information or data (including the Confidential Information and the Client Data) used by the *Client* and/or the *Contractor* in connection with this contract; and/or (b) the loss and/or unauthorised disclosure of any information or data (including the Confidential Information and the Client Data), including any copies of such information or data, used by the *Client* and/or the *Contractor* in connection with this contract.
"Clearance"	means national security clearance and employment checks undertaken by and/or obtained from the Defence Vetting Agency;
"Contractor Equipment"	the hardware, computer and telecoms devices and equipment supplied by the *Contractor* or its Subcontractors (but not hired, leased or loaned from the *Client*) for the carrying out of the *works*;
"Contractor Software"	software which is proprietary to the *Contractor*, including software which is or will be used by the *Contractor* for the purposes of carrying out of the *works*;
"Contractor System"	the information and communications technology system used by the *Contractor* in carrying out of the *works* including the Software, the *Contractor* Equipment and related cabling (but excluding the Client System);
"Control"	means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management

	and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and "Controls" and "Controlled" shall be interpreted accordingly;
"Default"	any breach of the obligations of the relevant party (including but not limited to fundamental breach or breach of a fundamental term) or any other default, act, omission, negligence or statement of the relevant party, its employees, servants, agents or Sub contractors in connection with or in relation to the subject-matter of this contract and in respect of which such party is liable to the other;
"Dispute Resolution Procedure"	the dispute resolution procedure set out in this contract (if any) or as agreed between the parties;
"Client Premises"	means premises owned, controlled or occupied by the *Client* or its Affiliates which are made available for use by the *Contractor* or its Subcontractors for carrying out of the *works* (or any of them) on the terms set out in this contract or any separate agreement or licence;
"Client System"	the *Client*'s computing environment (consisting of hardware, software and/or telecommunications networks or equipment) used by the *Client* or the *Contractor* in connection with this contract which is owned by or licensed to the *Client* by a third party and which interfaces with the *Contractor* System or which is necessary for the *Client* to receive the *works*;
"Environmental Information Regulations"	the Environmental Information Regulations 2004 together with any guidance and/or codes of practice issues by the Information Commissioner or relevant Government Department in relation to such regulations;
"FOIA"	the Freedom of Information Act 2000 and any subordinate legislation made under this Act from time to time together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government Department in relation to such legislation;
"Good Industry Practice"	the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector;
"ICT"	information and communications technology;
"ICT Environment"	the Client System and the *Contractor* System;
"Impact Assessment"	an assessment of a Compensation Event;

"Information"	has the meaning given under section 84 of the Freedom of Information Act 2000;
"Information Assets Register"	the register of information assets to be created and maintained by the *Contractor* throughout the carrying out of the *works* as described in the contract (if any) or as otherwise agreed between the parties;
"ISMS"	the Information Security Management System as defined by ISO/IEC 27001. The scope of the ISMS will be as agreed by the parties and will directly reflect the scope of the *works*;
"Know-How"	all ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know how relating to the *works* but excluding know how already in the *Contractor*'s or the *Client*'s possession before this contract;
"List x"	means, in relation to a Subcontractor, one who has been placed on List x in accordance with Ministry of Defence guidelines and procedures, due to that Sub contractor undertaking work on its premises marked as CONFIDENTIAL or above;
"Malicious Software"	any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence;
"Process"	has the meaning given to it under the Data Protection Legislation but, for the purposes of this contract, it shall include both manual and automatic processing;
"Protectively Marked"	shall have the meaning as set out in the Security Policy Framework.
"Regulatory Bodies"	those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this contract or any other affairs of the *Client* and "Regulatory Body" shall be construed accordingly;
"Request for Information"	a request for information or an apparent request under the Code of Practice on Access to Government Information, FOIA or the Environmental Information Regulations;

"Security Management Plan"	the *Contractor*'s security plan prepared pursuant to paragraph 1.5.3 of schedule J (Security Management Plan) an outline of which is set out in Appendix 1 of schedule J (Security Management Plan);
"Security Policy Framework"	means the Cabinet Office Security Policy Framework (available from the Cabinet Office Security Policy Division);
"Security Requirements"	means the requirements in the contract relating to security of the carrying out of the *works* (if any) or such other requirements as the *Client* may notify to the *Contractor* from time to time
"Security Tests"	shall have the meaning set out in Appendix 2 (Security Management Plan) [Guidance: define "Security Tests" in Security Management Plan]
"Software"	Specially Written Software, *Contractor* Software and Third Party Software;
"Specially Written Software"	any software created by the *Contractor* (or by a third party on behalf of the *Contractor*) specifically for the purposes of this contract;
"Staff Vetting Procedures"	the *Client*'s procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989;
"Statement of Applicability"	shall have the meaning set out in ISO/IEC 27001 and as agreed by the parties during the procurement phase;
"Standards"	the British or international standards, *Client*'s internal policies and procedures, Government codes of practice and guidance together with any other specified policies or procedures referred to in this contract (if any) or as otherwise agreed by the parties;
"Third Party Software"	software which is proprietary to any third party other than an Affiliate of the *Contractor* which is or will be used by the *Contractor* for the purposes of carrying out of the *works*; and

1.2 Introduction

1.2.1 This schedule covers:

1.2.1.1 principles of protective security to be applied in carrying out of the *works*;

1.2.1.2 wider aspects of security relating to carrying out of the *works*;

1.2.1.3 the development, implementation, operation, maintenance and continual improvement of an ISMS;

1.2.1.4 the creation and maintenance of the Security Management Plan;

1.2.1.5 audit and testing of ISMS compliance with the Security Requirements;

1.2.1.6 conformance to ISO/IEC 27001 (Information Security Requirements Specification) and ISO/IEC27002 (Information Security Code of Practice) and;

1.2.1.7 obligations in the event of actual, potential or attempted breaches of security.

1.3 Principles of Security

1.3.1 The *Contractor* acknowledges that the *Client* places great emphasis on the confidentiality, integrity and availability of information and consequently on the security provided by the ISMS.

1.3.2 The *Contractor* shall be responsible for the effective performance of the ISMS and shall at all times provide a level of security which:

1.3.2.1 is in accordance with Good Industry Practice, the *law of the contract* and this contract;

1.3.2.2 complies with the Security Policy;

1.3.2.3 complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) available from the Cabinet Office Security Policy Division (COSPD);

1.3.2.4 meets any specific security threats to the ISMS; and

1.3.2.5 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with paragraph 1.3.2 of this schedule;

1.3.2.6 complies with the Security Requirements; and

1.3.2.7 complies with the *Client*'s ICT standards.

1.3.3 The references to standards, guidance and policies set out in paragraph 1.3.2.2 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.

1.3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the *Contractor* gives an early warning to the *Service Manager* of such inconsistency immediately upon becoming aware of the same, and the *Service Manager* shall, as soon as practicable, advise the *Contractor* which provision the *Contractor* shall be required to comply with.

1.4 ISMS and Security Management Plan

1.4.1 Introduction:

(i) The *Contractor* shall develop, implement, operate, maintain and continuously improve and maintain an ISMS which will, without prejudice to paragraph 1.3.2, be accepted, by the *Service Manager*, tested in accordance with the provisions relating to testing as set out in the contract (if any) or as otherwise agreed between the Parties, periodically updated and audited in accordance with ISO/IEC 27001.

1.4.1.1 The *Contractor* shall develop and maintain a Security Management Plan in accordance with this Schedule to apply during the carrying out of the *works*.

1.4.1.2 The *Contractor* shall comply with its obligations set out in the Security Management Plan.

1.4.1.3 Both the ISMS and the Security Management Plan shall, unless otherwise specified by the *Client*, aim to protect all aspects of the *works* and all processes associated with carrying out of the *works*, including the construction, use, alterations or demolition of the *works*, the *Contractor* System and any ICT, information and data (including the Client Confidential Information and the Client Data) to the extent used by the *Client* or the *Contractor* in connection with this contract.

1.4.2 Development of the Security Management Plan:

1.4.2.1 Within 20 Working Days after the Contract Date and in accordance with paragraph 1.4.4 (Amendment and Revision), the *Contractor* will prepare and deliver to the *Service Manager* for acceptance a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan set out in Appendix 2 of this Part 2 of this Contract Schedule J.

1.4.2.2 If the Security Management Plan, or any subsequent revision to it in accordance with paragraph 1.4.4 (Amendment and Revision), is accepted by the *Service Manager* it will be adopted immediately and will replace the previous version of the Security Management Plan at Appendix 2 of this Part 2 of this Contract Schedule J. If the Security Management Plan is not accepted by the *Service Manager* the *Contractor* shall amend it within 10 Working Days or such other period as the parties may agree in writing of a notice of non-acceptance from the *Service Manager* and re-submit to the *Service Manager* for accepted. The parties will use all reasonable endeavours to ensure that the acceptance process takes as little time as possible and in any event no longer than 15 Working Days (or such other period as the parties may agree in writing) from the date of its first submission to the *Service Manager*. If the *Service Manager* does not accept the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure. No acceptance to be given by the *Service Manager* pursuant to this paragraph 1.4.2.2 of this schedule may be unreasonably withheld or delayed. However any failure to accept the Security Management Plan on the grounds that it does not comply with the requirements set outin paragraph 1.4.3.4 shall be deemed to be reasonable.

1.4.3 Content of the Security Management Plan:

1.4.3.1 The Security Management Plan will set out the security measures to be implemented and maintained by the *Contractor* in relation to all aspects of the *works* and all processes associated with carrying out of the *works* and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the *works* comply with the provisions of this schedule (including the principles set out in paragraph 1.3);

1.4.3.2 The Security Management Plan (including the draft version) should also set out the plans for transiting all security arrangements and responsibilities from those in place at the Contract Date to those incorporated in the *Contractor*'s ISMS at the date notified by the *Service Manager* to the *Contractor* for the *Contractor* to meet the full obligations of the Security Requirements.

1.4.3.3 The Security Management Plan will be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other schedules of this contract which cover specific areas included within that standard.

1.4.3.4 The Security Management Plan shall be written in plain English in language which is readily comprehensible to the staff of the *Contractor* and the *Client* engaged in the *works* and shall only

reference documents which are in the possession of the *Client* or whose location is otherwise specified in this schedule.

1.4.4 Amendment and Revision of the ISMS and Security Management Plan:

1.4.4.1 The ISMS and Security Management Plan will be fully reviewed and updated by the *Contractor* annually or from time to time to reflect:

(a) emerging changes in Good Industry Practice;

(b) any change or proposed change to the Contractor System, the *works* and/or associated processes;

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

(d) any reasonable request by the *Service Manager*.

1.4.4.2 The *Contractor* will provide the *Service Manager* with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the *Client*. The results of the review should include, without limitation:

(a) suggested improvements to the effectiveness of the ISMS;

(b) updates to the risk assessments;

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

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

1.4.4.3 On receipt of the results of such reviews, the *Service Manager* will accept any amendments or revisions to the ISMS or Security Management Plan in accordance with the process set out at paragraph 1.4.2.2.

1.4.4.4 Any change or amendment which the *Contractor* proposes to make to the ISMS or Security Management Plan (as a result of a *Service Manager's* request or change to the *works* or otherwise) shall be subject to the early warning procedure and shall not be implemented until accepted in writing by the *Service Manager*.

1.4.5 Testing

1.4.5.1 The *Contractor* shall conduct Security Tests of the ISMS 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 *Service Manager.*

1.4.5.2 The *Service Manager* shall be entitled to witness the conduct of the Security Tests. The *Contractor* shall provide the *Service Manager* with the results of such tests (in a form accepted by the *Client* in advance) as soon as practicable after completion of each Security Test.

1.4.5.3 Without prejudice to any other right of audit or access granted to the *Client* pursuant to this contract, the *Service Manager* and/or its authorised representatives shall be entitled, at any time and without giving notice to the *Contractor*, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the *Contractor*'s compliance with the ISMS and the Security Management Plan. The *Service Manager* may notify the *Contractor* of the results of such tests after completion of each such test. Security Tests shall be designed and implemented so as to minimise the impact on the carrying out of the *works*. If such tests adversely affect the *Contractor*'s ability to carry out the *works* in accordance with the Scope, the *Contractor* shall be granted relief against any resultant under-performance for the period of the tests.

1.4.5.4 Where any Security Test carried out pursuant to paragraphs 1.4.5.2 or 1.4.5.3 above reveals any actual or potential Breach of Security, the *Contractor* shall promptly notify the *Service Manager* of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the *Contractor* proposes to make in order to correct such failure or weakness. Subject to the *Service Manager*'s acceptance in accordance with paragraph (i), the *Contractor* shall implement such changes to the ISMS and the Security Management Plan in accordance with the timetable agreed with the *Service Manager* or, otherwise, as soon as reasonably possible. Where the change to the ISMS or Security Management Plan is made to address a non-compliance with the Security Policy or Security Requirements, the change to the ISMS or Security Management Plan is Disallowed Cost.

1.5 Compliance with ISO/IEC 27001

1.5.1 Unless otherwise agreed by the parties, the *Contractor* shall obtain independent certification of the ISMS to ISO/IEC 27001 within 12 months of the Contract Date and shall maintain such certification until the Defects Certificate or a termination certificate has been issued.

1.5.2 In the event that paragraph 1.5.1 above applies, if certain parts of the ISMS do not conform to Good Industry Practice, or controls as described in

ISO/IEC 27002 are not consistent with the Security Policy, and, as a result, the *Contractor* reasonably believes that it is not compliant with ISO/IEC 27001, the *Contractor* shall promptly notifythe *Service Manager* of this and the *Client* in its absolute discretion may waive the requirement for certification in respect of the relevant parts.

1.5.3 The *Service Manager* shall be entitled to carry out such regular security audits as may be required and in accordance with Good Industry Practice, in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001.

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

1.5.5 If, as a result of any such independent audit as described in paragraph 1.5.4 the *Contractor* is found to be non-compliant with the principles and practices of ISO/IEC 27001 then the *Contractor* 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 *Client* in obtaining such audit.

1.6 Breach of Security

1.6.1 Either party shall give an early warning to the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

1.6.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in paragraph 1.6.1, the *Contractor* shall:

1.6.2.1 immediately take all reasonable steps necessary to:

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

(b) prevent an equivalent breach in the future.

such steps shall include any action or changes reasonably required by the *Service Manager*; and

1.6.2.2 as soon as reasonably practicable provide to the *Service Manager* full details (using such reporting mechanism as defined by the ISMS) of the Breach of Security or the potential or attempted Breach of Security.

Appendix 1 – Contractor's Security Management Plan

In the absence of ISO 27001 and ISO 27002 the Contractor shall maintain compliance with the principles and practices of ISO 27001 and ISO 27002, as per their own plan shown overleaf.

Security Management Plan

Introduction

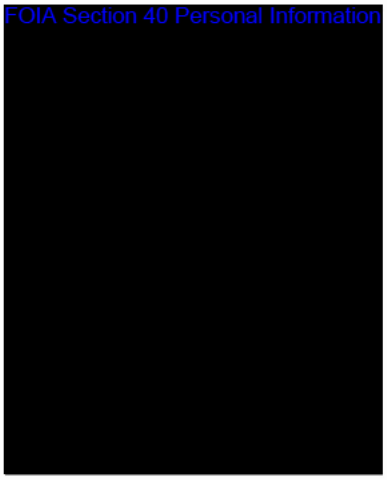
We're committed to maintaining the security and wellbeing of our staff, service users, partners and the surrounding community. Our Security Management Plan is but one aspect of our overall workplace safety efforts. Together, these efforts span personnel, information and asset security and include training and education activities to help ensure our programs' success.

Responsibility for this program has been vested in by Stand-By Fire Protection management. Your cooperation with these efforts will help us all maintain a program that accomplishes all of its goals.

We take specific actions toward identifying security-related threats from cyber crime to workplace violence. You (employees) can expand these efforts by reporting concerns and any security breaches immediately.

Your ongoing knowledge and cooperation as well as participation with the Security Management Plans' efforts will be appreciated, and again, help ensure its success.

FOIA Section 40 Personal Information



YOUR FIRST LINE IN FIRE
Kestrel House, Garth Road, Morden, Surrey, SM4 4LP
Call for fire protection on 020 8335 9800 **Fax** 020 8335 9801
Email sales@standbyfire.co.uk **Visit** www.standbyfire.co.uk

Compliance with Applicable Laws, Regulations, and Standards

There are various laws, regulations, and standards that apply to our organisation. We are committed to comply with these.

Details can be found in the following documents Privacy Policy and Confidentiality Policy

Information Security Policy

Our organisation has an Information Security Policy that is:

- supported by management
- reinforced by basic information security principles regarding:
  - confidentiality
  - integrity
  - availability
  - regulatory obligations

Details can be found in the following documents: Privacy Policy and Confidentiality Policy

Management Commitment and Responsibilities

Management commitment and responsibilities include:

- Program management
- Program review and updates
- Development of a review team if hazards are identified, or for deployment after an event to assist in its review
- Assisting with training
- Enforcing disciplinary actions as needed
- Interaction and assistance with regulatory agencies

Details can be found in the following document: Information Security Policy

Risk Assessment and Analysis

We will perform:

- Frequent Risk and/or Vulnerability Assessments
- Business impact analyses
- Both Personal and Physical Risk Assessments

Security risk assessments will be conducted as we become aware of new or potential threats.

Also see Information Security Policy

Asset Management and Recording

We have a current list of information security assets (i.e., an Asset Register) including details of who is responsible for them.
Details can be found in our Equipment Asset Register.
Also see Information Security Policy

Communications

We ensure secure communications by using ESET Endpoint Security. This uses the following features

Endpoint Protection

Antivirus and Antispyware	Eliminates all types of threats, including viruses, rootkits, worms and spyware **Optional cloud-powered scanning:** Whitelisting of safe files based on file reputation database in the cloud for better detection and faster scanning. Only information about executable and archive files is sent to the cloud – such data are not personally attributable.
Virtualization Support	ESET Shared Local Cache stores metadata about already scanned files within the virtual environment so identical files are not scanned again, resulting in boosted scan speed. ESET module updates and virus signatures database are stored outside of the default location, so these don't have to be downloaded every time a virtual machine is reverted to default snapshot.
Host-Based Intrusion Prevention System (HIPS)	Enables you to define rules for system registry, processes, applications and files. Provides anti-tamper protection and detects threats based on system behavior.
Exploit Blocker	Strengthens security of applications such as web browsers, PDF readers, email clients or MS office components, which are commonly exploited. Monitors process behaviors and looks for suspicious activities typical of exploits. Strengthens protection against targeted attacks and previously unknown exploits, i.e. zero-day attacks that could be used by crypto-ransomware to enter the targeted system.
Advanced Memory Scanner	Monitors the behavior of malicious processes and scans them once they decloak in the memory. This allows for effective infection prevention, even from heavily obfuscated malware, often detecting crypto-ransomware prior to it encrypting valuable files.
Client Antispam	Effectively filters out spam and scans all incoming emails for malware. Native support for Microsoft Outlook (POP3, IMAP, MAPI).
Cross-Platform Protection	ESET security solutions for Windows are capable of detecting Mac OS threats and vice-versa, delivering better protection in multi-platform environments.

Information Systems Protection

We have taken steps to protect data in whatever form it may take including being bound to the GDPR and Data Protection guiding principles.

Details can also be found in the following documents: Data Protection Policy

Preparedness & Recovery

We have Procedures in place to ensure the continuation of services after a critical incident (e.g., including everything from evacuation plans to backing up servers).
Details can be found in the following document Business Continuity Policy
Also see Information Security Policy

Data Classification

We classify data based on the data's sensitivity (i.e., Data Labels, Data Handling, Data Access levels).
Details can be found in the following document: Information Security Policy

Incident Response

During an incident we work through and manage an up-to-date contacts list and also a checklist of responsibilities until the incident is over.
We have a post incident requirement to review any 'lessons learnt' that may help to reduce the possibility of such an incident happening again.
Details can be found in the following documents: Personal Data Breach Policy
Also see Information Security Policy

Human Resources Security Processes

We have HR processes that cover;

- pre-employment checks
- employee screening
- termination of employment

Details can be found in the following documents: Recruitment and Selection Policy

Training & Awareness

We have a training program that ensured all staff are aware, understand and comply with the policies and procedures covered by this Security Management Plan.

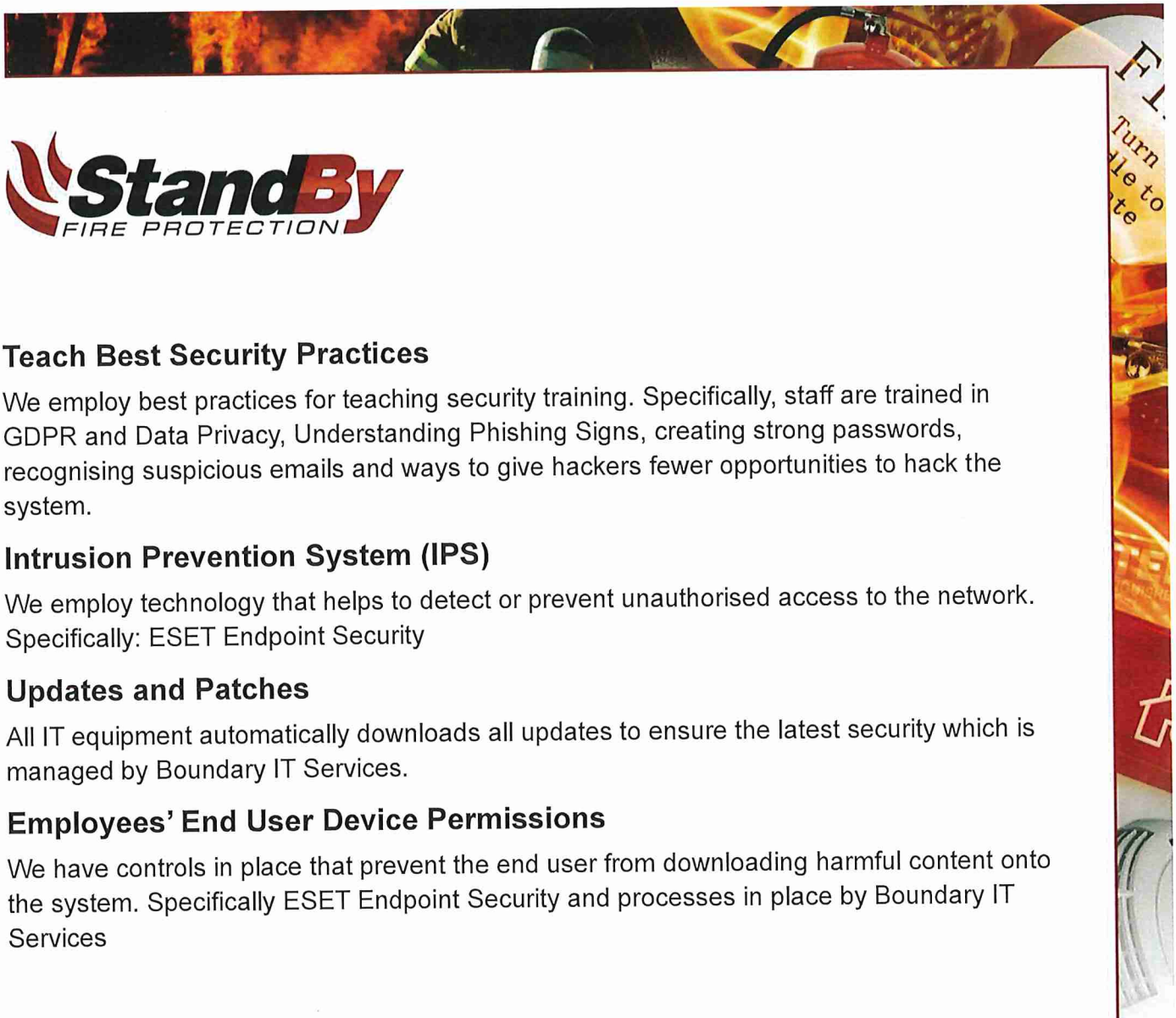
We employ best practices for teaching security training (e.g., create strong passwords, don't open suspicious emails, give hackers fewer opportunities to hack a system).

Details can be found in the following documents: Data Protection Policy, Training Register

Supplementary Information

Proactive Measures in Security Management

We are proactive in preventing security incidents by using ESET Endpoint Security



StandBy FIRE PROTECTION

Teach Best Security Practices

We employ best practices for teaching security training. Specifically, staff are trained in GDPR and Data Privacy, Understanding Phishing Signs, creating strong passwords, recognising suspicious emails and ways to give hackers fewer opportunities to hack the system.

Intrusion Prevention System (IPS)

We employ technology that helps to detect or prevent unauthorised access to the network. Specifically: ESET Endpoint Security

Updates and Patches

All IT equipment automatically downloads all updates to ensure the latest security which is managed by Boundary IT Services.

Employees' End User Device Permissions

We have controls in place that prevent the end user from downloading harmful content onto the system. Specifically ESET Endpoint Security and processes in place by Boundary IT Services

Review of this policy: this will be reviewed annually by the Director.

Next review date: February 2025


UK Research
and Innovation
STFC Fire Extinguisher, Fire Door and Fire Damper Maintenance for UKRI
UKRI-3313
Pricing Documents

UKRI Fire Extinguisher and Fire Door Pricing

Fire Extinguishers

FOIA Section 43 Commercial

[redacted]

Size	Type
2023 Remainder Extinguisher PPM	
2023 Remedial Replacements	
6 Litre	Water Extinguisher
6 Litre	AFFF Foam Extinguisher
2Kg	CO2 Extinguisher
6Kg	Dry Powder Extinguisher
9Kg	L2 Dry Powder Extinguisher
1.2x1.2	Fire Blanket
2024 Extinguisher PPM	
2024 Remedial Replacements	
6 Litre	Water
6 Litre	Foam
2Kg	CO2
6Kg	Powder
9Kg	L2 Powder
9 Litre	Non Mag Water
1.2x1.2	Fire Blanket
2025 Extinguisher PPM	
Replacements required = 321:	
6 Litre	Water
6 Litre	Foam
2Kg	CO2
6Kg	Powder
9Kg	L2 Powder
9 Litre	Non Mag Water
1.2x1.2	Fire Blanket

Fire Doors

FOIA Section 43 Commercial

2024 Fire Doors

Option 1 – Includes Full 44 point Fire Door Insp
Door Leaf is included.
1st 6 Monthly PPM
2nd 6 Monthly PPM

Option 2 - Includes Full 44 point Fire Door Inspe
Door Leaf. Replacement to Missing/Damaged
Closure Adjustment & Replacement Screws/Fix
1st 6 Monthly PPM
2nd 6 Monthly PPM

2025 Fire Doors

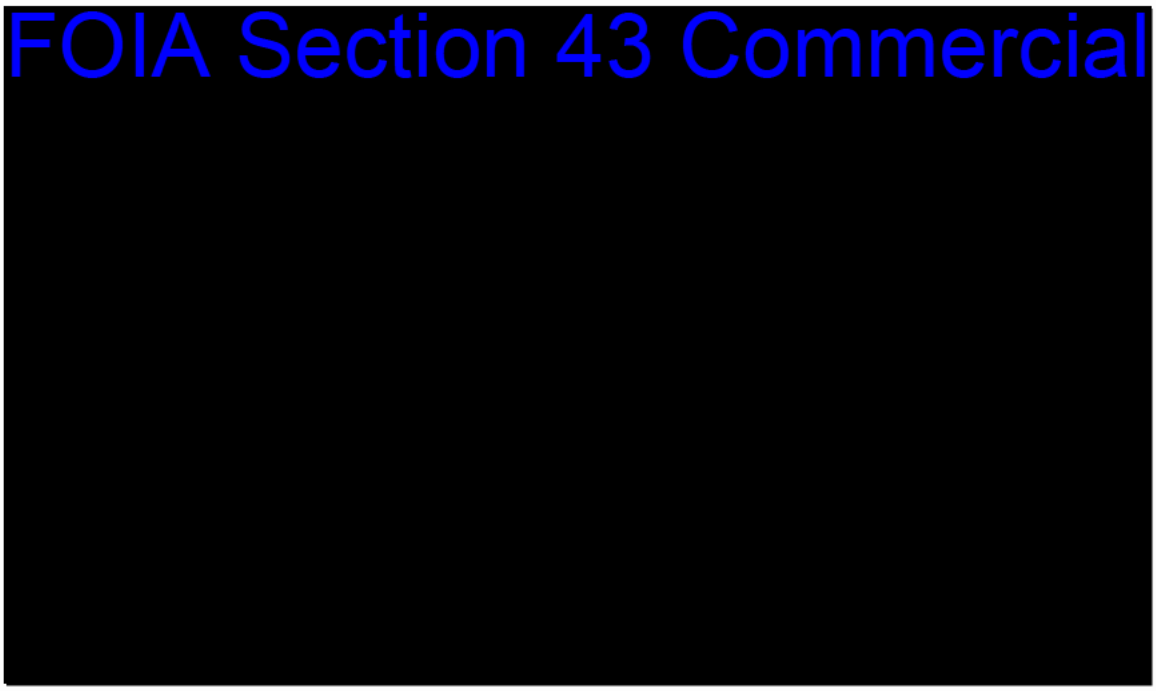
Option 1 – Includes Full 44 point Fire Door Insp
Door Leaf is included.
1st 6 Monthly PPM
2nd 6 Monthly PPM

Option 2 - Includes Full 44 point Fire Door Insp
Door Leaf. Replacement to Missing/Damaged
Closure Adjustment & Replacement Screws/Fix
1st 6 Monthly PPM
2nd 6 Monthly PPM

Fire Damper Locate and Test

Initial Survey to allow for up to 20 Days onsite to Locate and Test Fire Dampers which will then be hand marked onto your building plans for your CAD Team to update. A full documented report and initial asset register will then be produced by our compliance team and sent through as per the attached sample report. Should we need further time to complete the testing schedule we will send through an additional quotation once the initial 20 Days on site have been completed. Our price is based on full unhindered access during normal working hours.

FOIA Section 43 Commercial


FOIA Section 43 Commercial

UK Research and Innovation

STFC Fire Extinguisher, Fire Door and Fire Damper Maintenance for UKRI

UKRI-3313
Form of Agreement

UK Research and Innovation

CONTRACT UKRI-3313

This agreement is made on [.....27 March 2024.....] between:

(1) **United Kingdom Research and Innovation**, a statutory corporation whose registered office is at Polaris House, North Star Avenue, Swindon, England, SN2 1FL ("**the Client**"); and

(2) **Stand-By Fire Protection**, a partnership under the laws of England whose address is Kestrel House, Garth Road, Morden, SM4 4LP, with VAT Number 674 0307 47 (the "**Contractor**").

For the provision of the following service: UKRI-3313 STFC Fire Extinguisher, Fire Door and Fire Damper Maintenance

1. The *Contractor* will Provide the Service in accordance with the *conditions of contract* identified in the Contract Data.
2. The *Client* will pay the *Contractor* the amount due and carry out its duties in accordance with the *conditions of contract* identified in the Contract Data.
3. The documents forming this agreement are:
   - Contract Data part one
   - Contract Data part two and
   - The documents identified in Contract Data.

FOIA Section 40 Personal Information

[redacted]