Dated: 27th March 2024

CORPORATE OFFICER OF THE HOUSE OF LORDS
and
CORPORATE OFFICER OF THE HOUSE OF COMMONS
acting jointly

and

PHD MODULAR ACCESS SERVICES LIMITED

CONTRACT

in respect of PRINCIPAL CONTRACTOR: EVENTS

CONTRACT REFERENCE: STC1173(A)

Table of Contents

This Agreement is made on 27th March 2024

Between

(1) The Corporate Officer of the House of Lords and the Corporate Officer of the House of Commons, acting jointly of the Palace of Westminster, London, SW1A 0AA (***Client***) which expression shall include its successors in title, transferees and permitted assignees; and

and

(2) PHD Modular Access Services Limited, Company number 02690003 whose registered office is at 54 Oxford Road, Denham, Uxbridge, Middlesex UB9 4DN (***Contractor***)

Whereas

A. The *Contractor* submitted a tendered Price List (Part 1 – business as usual) of £XXXXXXXXX excluding VAT with (Part 2 – which includes estimated Task Orders for possible Rehearsals, though not guaranteed) of £XXXXXXXXX excluding VAT. Total anticipated cost for initial 3 years of £XXXXXXXXXX excluding VAT. The anticipated duration of the Services is from the *starting date* (1st April 2024 as set out in Contract Data Part 1) to the *completion date* (31st March 2027 as set out in Contract Data Part 1) being a period of 3 years with 1 + 1 Option Years (as may be adjusted in accordance with the *conditions of contract*).

B. The *Contractor* was subsequently selected by the *Client* to provide the Services.

C. The *Contractor* has agreed to provide the Services in accordance with this Contract (**"Contract"**).

D. The *Client* appoints the *Contractor* on the terms of this Contract to Provide the Services as more particularly described in the Scope.

1. Definitions and interpretation

1.1. In this Contract:

a) ***conditions of contract*** are as defined in Contract Data Part 1, incorporating the Z clauses;

b) **Contract Data Part 1** means the contract data part 1 in Annex 1;

c) **Contract Data Part 2** means the contract data part 2 in Annex 2;

d) **Scope** means the Scope in Annex 3;

e) **Services** means the *services* as defined in Contract Data Part 1;

f) **Z clauses** means the *Client*'s Z clauses in Annex 4;

g) **Security Aspects Letter** means the contract's Security Aspects Letter with its Schedules and PSMP in Annex 7.

h) **Principal Contractor and Principal Designer Appointment Letter** means the contract's CDM appointment letter.

1.2. Other words and expressions have the same meaning given to them in the *conditions of contract* unless otherwise stated.

2. Contract

2.1. In consideration of the *Client* making payment in accordance with this Contract, the *Contractor* hereby agrees to Provide the Services in accordance with this Contract.

2.2. This Contract is the entire agreement between the Parties in relation to the subject matter herein and supersedes all previous agreements between the Parties regarding the Services.

2.3. Neither party has been given, nor entered into this Contract in reliance on any arrangements, understandings, agreements, statements, representations or warranties other than those expressly set out in this Contract or expressly set out by the *Contractor* as

part of their tender response. Nothing in this clause or clause 2.2 above shall exclude liability in respect of misrepresentations made fraudulently.

2.4. The documents forming this Contract are:

a) This Agreement;

b) The *conditions of contract* (incorporating the Z clauses);

c) Contract Data Part 1;

d) Contract Data Part 2;

e) Scope;

f) Price List in Annex 5;

g) Not used;

h) Security Aspects Letter including Schedules and PSMP and Principal Contractor and Principal Designer Appointment Letter in Annex 7.

and all other documents referred to in them.

ANNEX 1: Contract Data Part 1

Contract Data

The *Client's* Contract Data

The *Client* is

Name	The Corporate Officer of the House of Lords and the Corporate Officer of the House of Commons, acting jointly.
Address for communications	Palace of Westminster, London SW1A 0AA
Address for electronic communications	XXXXXxxxxxxxxx

If the *Client* appoints a *Client's Agent,* the *Client's Agent* is

Name	Not applicable
Address for communications	Not applicable
Address for electronic communications	Not applicable

The authority of the *Client's Agent* is

Not applicable

The *service* is	Principal Contractor: Events (services as detailed in the Scope)	
The *starting date* is	1st April 2024	
The *service period* is	36 (plus Option years of 12 + 12 months)	months
The *period for reply* is	2 (two)	weeks
The *assessment day* is the	23rd	of each month

Are the rates and Prices in the contract adjusted for inflation? **No**

If yes the *index* is _____ provided by _____

The United Kingdom Housing Grants, Construction and Regeneration Act (1996) **does** apply

Contract Data

The *Client's* Contract Data

The *Adjudicator* is

Name	Royal Institute of Chartered Surveyors
Address for communications	
Address for electronic communications	

The interest rate on late payment is [ ] % per complete week of delay.

Insert a rate only if a rate less than 0.5% per week of delay has been agreed.

The *Client* provides this insurance	

Only enter details here if the *Client* is to provide insurance.

The minimum amount of cover for the second insurance stated in the Insurance Table is, for any one event	£10,000,000
The minimum amount of cover for the third insurance stated in the Insurance Table is, for any one event	£10,000,000
For any one event, the liability of the *Contractor* to the *Client* for loss of or damage to the *Client's* property is limited to	£10,000,000
The *Contractor's* total liability to the *Client* which arises under or in connection with the contract is limited to	£10,000,000
The *Adjudicator nominating body* is	Royal Institute of Chartered Surveyors
The *tribunal* is	Arbitration
If the *tribunal* is arbitration, the arbitration procedure is	Royal Institute of Chartered Surveyors

Contract Data

The *Client's* Contract Data

The *conditions of contract* are the NEC4 Term Service Short Contract June 2017 (with amendments January 2023) and the following additional conditions

Only enter details here if additional conditions are required.

See document ref: NEC4 TSSC Additional Conditions (A clauses).docx

ANNEX 2: Contract Data Part 2

Contract Data

The *Contractor's* Contract Data

The *Contractor* is

Name	PHD Modular Access Services Ltd
Address for communications	54 Oxford Road, Denham, Uxbridge UB9 4DN
Address for electronic communications	

The *fee percentage* is XXXX %

The *people rates* are

category of person	unit	rate
People Rates – in the Price List		

The *published list of Equipment* is: As published by CECA current at the date of contract.

The *percentage for adjustment for Equipment* is: XXXX % (state plus or minus)

The *Contractor's* Offer and *Client's* Acceptance

The *Contractor* offers to Provide the Service in accordance with these *conditions of contract* for an amount to be determined in accordance with these *conditions of contract*.

The offered total of the Prices for part of the *service* in Part 1 of the Price List is	£XXXXXXXX excluding VAT – (see Annex 5 of contract for Price List including Pricing Schedule and People Rates).
The offered total of the Prices for part of the *service* in Part 2 of the Price List is	£XXXXXXXX excluding VAT. This figure is subject to the number of Rehearsals and / or Activations that may occur during the lifetime of the contract, so can increase or decrease depending on Task Orders raised. – (see Annex 5 of contract for Price List including Pricing Schedule and People Rates).

Enter the total of the Prices from the Price List.

ANNEX 3: Scope

Scope

The Scope should be a complete and precise statement of the *Client's* requirements. If it is incomplete or imprecise there is a risk that the *Contractor* will interpret it differently from the *Client's* intention. The Scope should state clearly the part of the *service* which is to be carried out by the *Contractor* and which does not require the *Client* to issue a Task Order. This part of the *service* is priced in Part 1 of the Price List. Information provided by the *Contractor* should be listed in the Scope only if the *Client* is satisfied that it is required, is part of a complete statement of the *Client's* requirements and is consistent with the other parts of the Scope.

1 Description of the *service*

Give a detailed description of what the *Contractor* is required to do. This may include drawings.

See the Scope below.

2 Specifications

See the Scope below.

TITLE	DATE OR REVISION	TICK IF PUBLICLY AVAILABLE

Scope

3 Constraints on how the *Contractor* Provides the Service

State any constraints on the sequence and timing of work and on the methods and conduct of work including the requirements for any work by the *Client*.

See the Scope below

4 Requirements for the plan

State whether a plan is required and, if it is, state what form it is to be in, what information is to be shown on it, when it is to be submitted and when it is to be updated.

A plan and programme is required and the initial plan and programme will be the *Contractor's* submitted responses to all of the Invitation to Tender Technical Questions.

Both the programme and plan should be updated by the *Contractor* as required by the *Client*.

Scope

5 Services and other things provided by the *Client*

Describe what the *Client* will provide, such as services (including water and electricity) and ''free issue'' Plant and Materials and equipment.

ITEM	DATE BY WHICH IT WILL BE PROVIDED
See Information in Scope Documents below regarding Client supplied materials, equipment and venue(s).	1st April 2024

Scope

6 Property affected by the service

Give information about any property affected by the *service* and any other information which is likely to affect the *Contractor's* work.

See Scope below.

STC1173 – Scope

Redacted due to Security

ANNEX 4: Z Clauses

NEC4 TSSC ADDITIONAL CONDITIONS

AC1 Amendments and additions to the *conditions of contract*

The following amendments and/or additions are made to the ***conditions of contract***:

Clause heading	**Clause number**	**Amendment / addition**
Actions	10.3	Add new clause: "Within 2 weeks of the Contract Date, the *Client* notifies the *Contractor* of the purchase order number relevant to the contract."
Identified and defined terms	11.2(1A)	Not Used
	11.2(1)	Delete first bullet point and replace with: • "the requesting, offering, promising, giving, agreeing to receive, accepting or soliciting of a financial or other advantage to any person intended to induce that person to perform a function or activity illegally, unethically or improperly, perform an action which is a breach of trust or to reward any person for the illegal, unethical or improper performance of a function or activity or breach of trust, or where it is known that the acceptance of the advantage would itself constitute the illegal, unethical or improper performance of a function or activity or breach of trust"
	11.2(11A)	Add new clause: "A Subcontractor is a person or organisation who has a contract with the *Contractor* to provide a service which is necessary to Provide the Service, except for the • hire of Equipment or • supply of people paid for by the *Contractor* according to the time they work.
	11.2(30)	Add new clause: "The following definitions also apply to this contract: (a) **Authorised Retention and**

Disposal Policy refers to the *Client*'s retention and disposal policy available at:

http://www.parliament.uk/business/publications/parliamentary-archives/who-we-are/information-records-management-service/

b) Beneficiary means:

- any landlord;
- any Public Sector Entity that has an interest of any kind in the *services*;
- any replacement consultant or Subcontractor;
- any facilities maintenance contractor (meaning any contractor that carries out facilities maintenance and repair at the *site* including for any building or equipment on the *site*);
- any Funder (meaning a provider of finance (private or public) to any part of the Project, including having or acquiring a mortgage or charge over the Project or any building on the *site* in which the service is undertaken, whether that person acts on its own account, as agent for a syndicate of other parties or otherwise);
- any first Purchaser of each and every separate saleable part of the Project or the premises;
- any first Tenant of each and every separate lettable part of the Project or premises;
- (for Subcontractor warranties only) the *Client*.

(a) Controller, Processor, Data Subject, Personal Data, Personal Data Breach, Data Protection Officer take the meanings given in the UK GDPR.

(b) Crowned Portcullis means the Royal badge of that description used by the House of Commons and the House of Lords by licence from His Majesty the King.

(c) Data Loss Event means any event that results, or may result, in unauthorised access to Personal Data held by the *Contractor* under or in

		connection with this contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this contract, including any Personal Data Breach. **(d) Data Protection Impact Assessment** means an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data. **(e) Data Protection Legislation** means (i) the UK GDPR and any applicable national implementing laws as amended from time to time; (ii) the Data Protection Act 2018; (iii) any other applicable law about the processing of personal data and privacy. (f) **Data Subject Access Request** means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data. (g) **Dedicated Personnel** means, in relation to the London Living Wage, the *Contractor*'s staff (including all people engaged directly or indirectly by the *Contractor* (or any Subcontractor) who undertake any work in relation to this contract, other than an apprentice or intern) who provides a service to or on behalf of the *Client* involving two or more hours of work in any given day in a week, for eight or more consecutive weeks in a year. (h) **Delivery Authority** means the company limited by guarantee referred to in the Parliamentary Buildings (Restoration and Renewal) Act 2019. In the event of any amendments to that Act which alter the name or legal status of the Delivery Authority, any references in this contract to the Delivery Authority shall be construed as meaning any successor legal entity to the Delivery Authority. (i) **Government Provision** means any statutory provision, warrant, order, scheme, regulations or conditions of service applicable to the *Client*'s employees providing for continuance of pay or the payment of sick pay, or any allowance to or for the benefit of the *Client*'s employees, or their families or dependents, during or in respect of sickness, injury or disablement

		suffered by such employees. (j) **Information** refers to data, documents, records, files, drawings and other recorded information (whether hard copy or electronic) which has been created, derived or obtained in the course of the contract by the *Contractor* or received by the *Contractor* from the *Client* during the course of the contract or prior to the Contract Date. **(k) Information Management Policy** refers to policy available at: http://www.parliament.uk/business/publications/parliamentary-archives/who-we-are/information-records-management-service/ (l) **Intellectual Property Rights** means patents, inventions, trademarks, service marks, logos, design rights (whether registerable or otherwise), applications for any of the foregoing, copyright, database rights, domain names, trade or business names, moral rights and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom) and the right to sue for passing off. This definition includes **Parliamentary Copyright** pursuant to section 165 of the Copyright, Designs and Patents Act 1988, as applicable and unless the contrary intention appears. (m) **Living Wage** means an hourly rate as published from time to time, calculated according to the cost of living in the UK by the Living Wage Foundation, part of Citizens UK. (n) **London Living Wage** means an employer duly accredited by the Living Wage Foundation and paying its Dedicated Personnel at least the London Living Wage. (o) **New Fair Deal** means the New Fair Deal Policy introduced in October 2013 by HM Treasury setting out how pensions issues are to be dealt with when employees are compulsorily transferred from the public sector to independent providers delivering public services.

		(p) **Parliamentary Estate** includes the property affected by the *Contractor*'s work. It means all land and buildings belonging to or occupied or controlled by the Corporate Officer of the House of Lords and the Corporate Officer of the House of Commons, individually or jointly. For the purpose of the delivery of goods, it also includes the Parliamentary Offsite Consolidation Centre. **(q) Parliamentary Offsite Consolidation Centre** means Parliament's offsite facility for the delivery of goods, Plant and Materials, Equipment and other items as detailed in the Scope. (r) **PCR 2015** means the Public Contracts Regulations 2015. **(s) Protective Measures** means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data; ensuring confidentiality, integrity, availability and resilience of systems and services; ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident; and regularly assessing and evaluating the effectiveness of such measures adopted by it. **(t) Public Sector Entity** means any contracting authority as defined in regulation 2(1) of the PCR 2015; any body or holder of office that is a public authority as defined in section 3 of the Freedom of Information Act 2000; or any other public sector entity including, but not limited to, the Delivery Authority set up for the purposes of delivering the Restoration and Renewal programme. **(u) Restoration and Renewal Programme** means the major refurbishment works to the Palace of Westminster. This programme is delivered by a separate legal entity to the *Client* as established under the Parliamentary Buildings (Restoration and Renewal) Act 2019. **(v) Security Aspects Letter** means any security aspects letter ("**SAL**") entered into or to be entered into by the *Contractor* in respect of the contract.

		A SAL requires the *Contractor* to agree to meet the *Client*'s information security requirements for the *Contractor*'s own information systems (and that of its Subcontractors) where such systems hold information from the *Client*. A SAL informs the *Contractor* what types of sensitive information requires protection and includes the right for the *Client* to audit the *Contractor*'s information security management process. **Sub-Processor** means any third party appointed to process Personal Data on behalf of the *Contractor* related to this contract. **TUPE Information** means information regarding: • the activities employees perform • age • start date • place of work • notice period • redundancy payment entitlement • salary, benefits and pension entitlements • employment status • identity of employer • working arrangements • outstanding liabilities • sickness absence • copies of all relevant employment contracts and related documents • all information required under regulation 11 of TUPE or as reasonably requested by the *Client* or the new contractor. (w) **UK GDPR** has the meaning given in section 3(10) of the Data Protection Act 2018."
Interpretation and the law	12.2	Add to the end of the clause: "A reference to any enactment, order, regulation or other similar instrument is construed as a reference to the enactment, order, regulation or instrument as extended, consolidated, re-

		enacted or amended by any subsequent enactment, order, regulation or instrument."
	12.4	Before the full stop, add the following: "in relation to the subject matter herein and supersedes all previous agreements between the Parties regarding the *service"* After the full stop, add the following: "For the avoidance of doubt: (a) the contract includes any obligations, duties, rights and powers the Parties may have under any relevant non-disclosure agreement and/or Security Aspects Letter; and (b) should there be any conflict between any terms associated with a purchase order and this contract, the terms of this contract take priority."
	12.5	Add new clause: "Neither Party has been given, nor entered into this contract in reliance on any arrangements, understandings, agreements, statements, representations or warranties other than those expressly set out in this contract. Nothing in this clause or clause 12.4 shall exclude liability in respect of misrepresentations made fraudulently."
	12.6	Add new clause: "Any reference in this contract to: (a) a European Union ("**EU**") law is to be read as a reference to that EU law as it has effect from time to time in the law of the UK or part of the UK by virtue of the European Union (Withdrawal) Act 2018; and (b) an EU institution or EU authority or other EU body shall be read as a reference to the relevant UK institution, authority or body to which its functions were transferred by virtue of the Act."
	12.7	Add new clause: "The headings of clauses do not affect their interpretation."
	12.8	Add new clause: "Nothing in this contract is construed as creating a partnership, a contract of employment or a relationship of principal and agent between the *Client* and the *Contractor*."

	12.9	Add new clause: "The courts of England and Wales have exclusive jurisdiction in respect of all matters arising under or in connection with this contract, provided that nothing in this clause or clause 93 limits (or is construed so as to limit) the right of the *Client* to commence and pursue proceedings against the *Contractor* in the courts of any country in which the *Contractor* has assets or in any other court of competent jurisdiction nor shall the commencement and pursuit of proceedings in any one or more jurisdictions preclude the commencement and pursuit of proceedings in any other jurisdiction (whether concurrently or not) if and to the extent permitted by applicable law."
	12.10	Add new clause: "The *Contractor* warrants that in the performance of this contract, it will at all times comply with the *law of the contract* (whether or not the same applies to or are binding on the *Client*)."
	12.11	Add new clause: "If any provision of this contract is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision is severed to the extent necessary and the remainder of the provisions continue in full force and effect as if the contract had been executed without the invalid, illegal or unenforceable provision."
The *Client*'s authority, delegation and *Client's Agent*	14.2	At the end of the clause, add the following: "An instruction given by the *Client* to change to the Scope or a Task Order may be an instruction to omit part of the *service* from the Scope or Task Order. The *Client* has the right to appoint any other person to carry out the omitted *service* (or part thereof) at any time."
Prevention	18	Add new clause 18.1: "If an even occurs which • stops the *Contractor* completing the whole of the *service* or • stops the *Contractor* completing the *service* by the end of the *service period* or • stops the *Contractor* completing a Task Order by the

		Task Completion Date and which • neither Party could prevent and • an experienced contractor would have judged at the Contract Date to have such a small change of occurring that it would have been unreasonable to have allowed for it the *Client* gives an instruction to the *Contractor* stating how the event is to be dealt with."
Subcontracting and people	21.3	Add at the end of clause: "The *Contractor* gives **30 days'** notice of a proposed replacement person to the *Client* for acceptance and submits with the notice the name, relevant qualifications and experience of the proposed replacement person. A reason for not accepting the person is that the *Client* (in its absolute discretion) does not consider their relevant qualifications and experience to be as good as those of the person who is to be replaced."
	21.4	Add clause: "The employment, qualifications, competence and security clearance of each person, or replacement person, and all members of the *Contractor*'s or its Subcontractors' staff employed to Provide the Service complies with the requirements set out in the Scope."
Subcontracting	21.5	Add new clause: "The *Contractor* submits the name of each proposed Subcontractor to the *Client* for acceptance. Reasons the *Client* may not accept a proposed Subcontractor include: a) the appointment will not allow the *Contractor* to Provide the Service; b) there are grounds which are akin to the mandatory or discretionary grounds for excluding the Subcontractor under regulation 57 of the PCR 2015; c) the Subcontractor is a self-employed individual."
	21.6	Add new clause: "The *Contractor* does not appoint a proposed Subcontractor until the *Client* has

		• accepted the Subcontractor and, to the extent these *conditions of contract* require, • accepted the subcontract documents."
	21.7	Add new clause: "Unless agreed otherwise with the *Client*: (a) prior to appointing a Subcontractor, the *Contractor* submits the proposed subcontract documents, except any pricing information, for each subcontract to the *Client* for acceptance; (b) the proposed subcontract is an NEC contract and complies with the requirements of clause 21.9 and the Scope."
	21.8	Add new clause: "Reasons the *Client* may not accept the subcontract documents include: (a) they do not comply with the requirements of clause 21.9; (b) their use will not allow the *Contractor* to Provide the Service; or (c) they do not include a statement that the parties to the subcontract act in a spirit of mutual trust and co-operation."
	21.9	Add new clause: "Unless otherwise agreed with the *Client*, the *Contractor* ensures the following requirements are included in any subcontract: (a) the subcontract is to be executed as a deed; (b) all provisions in this contract are stepped down to the Subcontractor (*mutatis mutandis*) including, but without limitation, the provisions relating to payment, record keeping and auditing, security, Security Aspect Letters, and a requirement to provide any information required by the *Contractor* from the Subcontractor for the Information Security Management Plans, and BIM Execution Plans; (c) where applicable, the Subcontractor is to provide any executed Subcontractor warranties in favour of any Beneficiary in the form of the draft contained in the Scope within the timescales required under clause AC3.3 of this contract; (d) the *Client* may step-in to the subcontract in place of the *Contractor* if the *Contractor* becomes insolvent or its equivalent;

		(c) where applicable, the Subcontractor ensures that provisions to the same effect as the requirements of this clause 21.9 are included in any sub-subcontract it awards for works or services required by its subcontract."
	21.10	Add new clause: "Within 14 days after the appointment of a Subcontractor, the *Contractor* supplies a certified copy of the executed and delivered subcontract to the *Client*."
	21.11	Add new clause: "If the *Contractor* breaches clause 21.10, the *Client* may notify the *Contractor* of the breach. If such breach is not rectified within 14 days from the date of such notice, the *Client* is entitled to withhold 10% of the amount due to the *Contractor* for services or work related to the Subcontractor from whom the subcontract is outstanding while such breach remains to be rectified. This is in addition to any other right the *Client* may have to withhold sums under the contract and on a cumulative basis."
Assignment and novation	22	Add clause: "Assignment and novation 22.1 The *Contractor* may not novate, assign or charge the benefit of this contract or any right arising under it without the written consent of the *Client* except that the *Contractor* may assign the debt arising under the contract to a factor or invoice discounter without the *Client*'s prior approval. 22.2 The *Client* is entitled to novate or assign any or all its rights under the contract to any Public Sector Entity from time to time without the consent of the *Contractor*, provided that any such assignment does not materially increase the burden of the *Contractor*'s obligations under the contract. 22.3 Upon the novation of this contract, the *Contractor* executes a collateral warranty in respect of this contract in favour of the *Client* in terms of the draft contained in the Scope. 22.4 In this contract, references to the *Client* include where the context admits its permitted assignees and transferees."
Confidentiality, Information	23	Add clause heading:

Management and Freedom of Information		"Confidentiality, Information Management and Freedom of Information"
	23.1	Add new clause: <u>"Confidentiality</u> The *Contractor* • treats any Information derived from or obtained in the course of the contract, or received from the *Client* prior to the Contract Date, as confidential; • complies with any obligations it may have to the *Client* under a non-disclosure agreement and/or a Security Aspects Letter related to this contract."
	23.2	Add new clause: "Except with the *Client*'s prior approval, the *Contractor* does not: disclose the contract or any provision thereof to any person other than a person engaged by the *Contractor* for the provision of the contract or any other person concerned with the same; take, use, publish, circulate (or authorise the taking, using, publishing or circulating) of any photograph or drawing or other depiction of the *service* or any part of the *service* or of the Parliamentary Estate for publicity purposes or in any annual report or accounts or otherwise for any purpose other than in connection with the performance of the *Contractor*'s obligations under this contract; make any public statement relating to the existence or performance of this contract. This includes the issue of publicity material or press announcement relating to this contract. If the *Client*'s prior approval is sought, the precise wording of the statement must be approved. If the *Client*'s approval is given in accordance with this clause, any disclosure is made in confidence and extends only so far as may be necessary for the purposes of the contract."
	23.3	Add new clause: <u>"Information Management</u> The *Contractor*: ensures that any Information will be managed in accordance with the *Client*'s Information Management Policy; ensures that any Information is not transferred or stored on IT systems physically located outside of the United Kingdom without the *Client*'s express permission; is accountable for all Information held by it or its Subcontractors in relation to this contract;

		enables the *Client* to carry out information security audit checks from time to time and provides, or ensure the provision of, the necessary information requested by the *Client* to support such audits; uses an email service that is able to support encrypted main connections to current standards (TLS 1.2); ensures that it continues to comply with and meet the *Client*'s mandatory security requirements as set out in the "Non-Functional Security Requirements" document issued and responded to as part of the procurement process; ensures, at the end of the *service period* or early termination (howsoever arising), if requested under clause 94.1(d) that: (i) hard copy Information is destroyed in line with the *Client*'s Authorised Retention and Disposal Policy by shredding and disposing of it in confidential waste and (ii) electronic Information is destroyed in line with the *Client*'s Authorised Retention and Disposal Policy, whether held on hard disks of computers, laptops, and tablets; external storage, such as USB drives, CDs, or external hard drives; or network and back-up systems; h) ensures it provides the *Client* with confirmation that all Information referred to above has been destroyed in line with the *Client*'s Authorised Retention and Disposal Policy, including filenames, the dates disposed of, destruction certificates, and such other information that the Client reasonably requires. In the event the *Contractor* considers it is not able to comply with the *Client*'s Authorised Retention and Disposal Policy, it informs the *Client* of the reason and keeps the *Client* informed on a regular basis of the status of the Information."
	23.4	Add new clause: "The *Contractor* notifies the *Client* of any loss or disclosure (whether accidental or otherwise) of Information as soon as such loss or disclosure becomes known to the *Contractor*."
	23.5	Add new clause: "The *Contractor* takes all necessary precautions to ensure that its staff and Subcontractors (including all people engaged directly or indirectly by it who undertake any work in relation to this contract) are bound by and adhere to the same duties of confidentiality and information management obligations as set out in this clause 27."

	23.6	Add new clause: "Freedom of Information and Environmental Information Regulations The House of Commons and the House of Lords are public authorities within the meaning of the Freedom of Information Act 2000 ("**FOIA**") and the Environmental Information Regulations 2004 ("**EI Regulations**"). All information received by the *Client* under or in relation to this contract may be subject to a request under the FOIA or the EI Regulations and all such requests are dealt with by the House of Commons and/or the House of Lords at its or their discretion. The Clerk of the Parliaments or the Speaker of the House of Commons may consider that disclosure of the requested information infringes the rights and privileges of Parliament."
	23.7	Add new clause: "When considering a request under the FOIA or the EI Regulations, the House in question will carefully consider releasing any information it holds or is held by the *Contractor* on its behalf, giving protection to confidential information and any other relevant exemptions where appropriate. Where the *Contractor* provides information to the *Client* that it regards as confidential, it identifies clearly the confidential elements and explains why it considers each element to be of a confidential nature. Routine marking of the documents as being confidential is not accepted; the *Contractor* provides justification for why it considers its information should not be disclosed. Receipt by the *Client* of information marked as confidential, or marked in any other way, does not imply that the *Client* accepts any duty of confidence by virtue of that marking nor any obligation not to disclose that information when required by the FOIA or EI Regulations."
	23.8	Add new clause: "Where required by the *Client*, the *Contractor* assists the *Client* to enable the *Client* to comply with its obligation under FOIA or EI Regulations. Where the *Client* receives a request for information under the FOIA or EI Regulations or any other applicable legislation governing access to information and requires the *Contractor*'s assistance in obtaining all or any such information, the *Contractor* responds to any such request for assistance promptly and in any event within 10 days of receiving the *Client*'s request (or other reasonable time period specified by the *Client* when making the request)."
	23.9	Add new clause:

		"Primary responsibility for decisions to disclose information in response to a request under the FOIA or EI Regulations rests with the House in question. However, decisions on disclosure under the FOIA and EI Regulations are subject to the jurisdiction of the Information Commissioner, the First-tier Tribunal (General Regulatory Chamber) and the Courts."
	23.10	Add new clause: "The *Client* is not liable to the *Contractor* for any loss, damage, harm or other detriment however caused arising from the disclosure of any information relating to this contract under FOIA or EI Regulations."
	23.11	Add new clause: "The *Client* reserves the right to disclose all details of contractual documentation, processes, prices, performances and outcomes arising under or in relation to this contract in order to meet legal, regulatory and public policy requirements, and to comply with any other duty it may have to provide information to the House of Commons and/or the House of Lords and/or any representatives of the Houses either individually or by the formation of committees or working groups."
Access	32.1	Add new clause: (a) "Any access granted to the *Contractor* under the contract may be suspended or amended at any time at the sole discretion of the *Client* as part of the House of Commons' or House of Lords' response to a significant risk, threat, or instance of disruption from external events, agencies, or persons, or any other emergency, or as a result of a change to the business of either House, for example in the event of a recall of Parliament, or because of a significant ceremonial or similar event. (b) The decision of the *Client* under clause 32.1(a) will be final and no prior notice need be given. The *Contractor* vacates the Parliamentary Estate together with all its staff and Subcontractors (including all people engaged directly or indirectly by it who undertake any work in relation to this contract) and (where requested by the *Client*) all or any of its Equipment, Plant and Materials (as set out in the Scope) by the time specified. (c) The *Client* endeavours, but cannot guarantee, to provide 4

		hours' notice to the *Contractor* under clause 32.1(a). Notice under that clause can be given orally or in writing and no discussion about the reason(s) for the notice is entered into. If the Equipment, Plant and Materials (which are required to be removed) have not been removed by the time specified in the notice or by another time agreed by the Parties, the *Client* may arrange for them to be removed by contractors appointed by the *Client*, and then for them to be stored by such contractors until they are collected by the *Contractor*. The *Contractor* indemnifies the *Client* against the costs of such removal and storage. (d) Any suspension or amendment to the *Contractor*'s access under clause 32.1(a) is treated as a compensation event under clause 60.1(4)."
	32.2	Add new clause: (a) "Subject to clause 32.2(b), when vacating the Parliamentary Estate in accordance with clause 32.1, the *Contracto*r ensures the property affected by the *Contractor*'s work and the *service* are secured and left in a safe condition. (b) In the absence of any instruction from the *Client*, the *Contractor* complies with its obligations under health and safety legislation and exercises its professional expertise and judgment in deciding whether the circumstances of the situation allow for it to make the property affected by the *Contractor*'s work and the *service* secure and safe and/or the extent of such making secure and safe that can reasonably be done."
	32.3	Add new clause: (a) Any land or premises (including temporary accommodation) made available to the *Contractor* by the *Client* in connection with the contract is made available to the *Contractor* free of charge (unless stated elsewhere in the contract), on a non-exclusive licence basis, and is used by the *Contractor* solely for the purpose of performing the contract. (e) The *Contractor* ensures that access to the property affected by the *Contractor*'s work is limited to such people as is necessary for the purpose of performing the contract."

Payment	51.4	Add new clause: "A properly prepared invoice should: a) be a true and accurate reflection of the notified sum or the amount stated in a Pay Less Notice (whichever is relevant); b) contain a reference to any appropriate contract references and titles (including the relevant purchase order number and the *Client's* certificate); and c) include any details required by His Majesty's Revenue and Customs."
Compensation events	60.1(19)	Add as new clause 60.1(19): "An event which • stops the *Contractor* completing the *service* or • stops the *Contractor* completing the *service* by the end of the *service period* or • stops the *Contractor* completing a Task Order by the Task Completion Date and which • neither Party could prevent, • an experienced contractor would have judged at the Contract Date to have such a small chance of occurring that it would have been unreasonable to have allowed for it and • is not one of the other compensation events stated in this contract.
Reasons for termination	90.7	Add as new clause 90.7: "The *Client* may terminate if an event occurs which • stops the *Contractor* completing the *service* or • stops the *Contractor* completing the *service* by the end of the *service period* and is forecast to delay completion of the whole of the *service* by more than thirteen weeks or • stops the *Contractor* completing a Task Order by Task Completion Date and is forecast to delay completion of the Task Order by more than thirteen weeks,

		and which • neither Party could prevent, • an experienced contractor would have judged at the Contract Date to have such a small chance of occurring that it would have been unreasonable to have allowed for it and • is not one of the other compensation events stated in this contract (Reason 9)."
Procedures on termination	91.1	After the word "termination", add "(including partial termination)". After the words "the *service*" add "itself or may appoint any other contractor to complete the *service*".
Following Completion or termination	94	Add new clause 94 with heading "Following Completion or termination"
	94.1	Add in new clause 94.1: (a) Following the end of the *service period* or early termination (howsoever arising), the *Contractor* co-operates with the *Client* and, where relevant, any new contractor appointed by the *Client* to continue or take over the performance of the contract in order to ensure an effective handover of all work then in progress and reduce to a minimum any interruption to the provision of the *service*. (b) The *Client* is not liable to reimburse the *Contractor*'s costs associated with clause 94.1(a) but may in its discretion choose to reimburse the *Contractor* for any reasonable cost incurred during the transition to the new contract. (c) Termination of the contract (howsoever arising): • is without prejudice to any other rights or remedies a Party may be entitled to under the contract or at law; • does not affect any accrued rights or liabilities of either Party; • does not affect the coming into force or continuance of any provision of the contract which is expressly or by implication intended to come into force or continue on or after termination; and

		• is without prejudice to the *Client*'s right to appoint any other person to carry out the *service* at any time. (d) Without prejudice to clause 94.1(g), following the end of the *service period* or early termination (howsoever arising), the *Contractor* seeks instructions from the *Client* as to what it do~~es~~ with the Information it holds relating to the contract that is in its possession or under its control. The *Client* may require the Information, or some of it, to: (i) be transferred to the *Client*; or (ii) be kept and maintained by the *Contractor* for a specified period of time (not exceeding 12 years after the earlier of the end of the *service period* or early termination (howsoever arising)) and then destroyed in accordance with Clause 23.3. (e) Any request under clause 94.1(d)(i) : • is complied with within 10 working days. The *Contractor* is responsible for ensuring that any computerised filing, recording, and documenting Information is transferred free of any charges to the *Client* (or person designated by the *Client*) in a usable format to facilitate a smooth hand-over of work at expiration or termination of the contract; • does not prevent the *Contractor* from being entitled to retain one copy of the same for insurance and/or legal purposes and/or for such other purposes as the *Client* may agree (acting reasonably) unless the *Client* notifies the *Contractor* that in the *Client*'s reasonable opinion any or all of it is so sensitive that the *Contractor* may not retain any copies. (f) In the event of the *Contractor*'s failure to comply with clauses 94.1(d)(i) and/or 94.1(e), the *Client* may nevertheless recover possession of any materials covered by this clause and the *Contractor* grants licence to the *Client* or its appointed agents to execute recovery from any premises of the *Contractor* or its Subcontractors where any such materials may be held.

		(g) In the event the *Contractor* is requested to keep and maintain any of the Information for a specified period of time in accordance with clause 94.1(d)(ii), it affords the *Client* (or any representative of the *Client*) such access to those records as may be required in connection with the contract upon request and from time to time.
United Kingdom Housing Grants, Construction and Regeneration Act 1996 (page CC 17)		Delete 1.1 and substitute: "1.1(1) The *Client* is not bound by the Housing Grants, Construction and Regeneration Act 1996 as amended by the Local Democracy, Economic Development and Construction Act 2009 (hereinafter referred to as the "**Act**") but elects to voluntarily incorporate the provisions of the Act into this contract. 1.1(2) A period of time stated in days is a period calculated in accordance with section 116 of the Act. 1.1(3) The date on which a payment becomes due is **7 days** after the date an invoice is submitted. 1.1(4) The final date for payment is **23 days** after the date on which payment becomes due." Clause 1.4 at the end of the first sentence of the replacement text after "final date for payment" add "by stating the amount considered to be due at the date this notice is given and the basis on which that sum is calculated (the "**Pay Less Notice**")" Clause 1.4 add at the end of the final sentence "by means of a Pay Less Notice" Add as clause 1.4A: "1.4A The *Contractor* submits to the *Client* a valid invoice in accordance with clause 50.7 for the notified sum or, where appropriate, the amount stated in a Pay Less Notice notified under clause 1.4. If necessary, the *Contractor* issues a credit note to correct a difference between the notified sum and the amount stated as due in a Pay Less Notice."

Additional clauses

AC2 *Contractor*'s warranties

AC2.1 The *Contractor,* whenever instructed to do so by the *Client,* executes and delivers a deed or deeds of warranty in respect of the *Contractor*'s duties under this contract in favour of any Beneficiary in the terms of the draft *Contractor 's* warranty contained in the Scope**.** The executed and delivered deed or deeds of warranty are provided to the *Client* within **14 days** of the *Client's* instruction (or any other period of time as the *Client* and *Contractor* may reasonably agree).

AC2.2 If the *Contractor* fails to provide the *Client* with a deed of warranty referred to and instructed in accordance with clause AC2.1 within the requisite time period, the *Client* may notify the *Contractor* of the breach. If such breach is not rectified by the *Contractor* within **14 days** from the date of such notice, the *Client* is entitled to withhold 10% of the amount due to the *Contractor* under any invoice while such breach remains to be rectified. This is in addition to any other right the *Client* may have to withhold sums under the contract and on a cumulative basis.

AC3 Subcontractor warranties

AC3.1 Whenever the *Client* from time to time requires, the *Contractor* ensures that each Subcontractor executes and delivers collateral warranties in favour of any or all the Beneficiaries substantially in the form of the draft contained in the Scope.

AC3.2 Unless the *Client* otherwise instructs, the *Contractor* ensures that each Subcontractor immediately upon its appointment executes and delivers a Subcontractor warranty in favour of the *Client* substantially in the form of the draft contained in the Scope, ensuring that the deed includes step-in rights for the *Client* in respect of the Subcontractor's deed of appointment. Such an instruction is not a compensation event.

AC3.3 The *Contractor* complies with this clause AC3 (and ensures any relevant Subcontractor complies):

(a) immediately upon the appointment of a Subcontractor (where applicable);
(b) where (a) is not applicable, within **14 days** of the *Client*'s instruction to provide the requisite warranties; or
(c) within any other period of time as the *Client* and *Contractor* may reasonably agree.

AC3.4 If the *Contractor* breaches clauses AC3.1, AC3.2 or AC3.3, the *Client* may notify the *Contractor* of the breach. If such breach is not rectified by the *Contractor* within **14 days** from the date of such notice, the *Client* is entitled to withhold 10% of the amount due to the *Contractor* for services related to the Subcontractor from whom the subcontract and/or warranty is outstanding while such breach remains to be rectified. This is in addition to any other right the *Client* may have to withhold sums under the contract and on a cumulative basis

AC3.4 Notwithstanding any other provision of this contract, the *Contractor* does not appoint a Subcontractor if there are compulsory grounds for excluding them under regulation 57 of the PCR 2015. If there are non-compulsory grounds for exclusion under that regulation, the *Client* reserves the right to require the *Contractor* to replace or not to appoint the relevant Subcontractor.

AC4 – AC6 NOT USED

AC7 Security

AC7.1 The *Contractor* complies with all security requirements set out in the Scope. Matters of security are at the sole discretion of the *Client*. While working for or with the *Client* and when on the Parliamentary Estate, the *Contractor* complies with all security measures implemented by the *Client* and/or the *Client*'s security contractors. The *Client* may carry out any search of the *Contractor*'s staff and Subcontractors (including all people engaged directly or indirectly by it who undertake any work in relation to this contract) or of vehicles used by the *Contractor* (or its Subcontractors) on the Parliamentary Estate.

AC7.2 All personnel requiring access to the Parliamentary Estate or the *Client*'s IT network in order to perform this contract are required to have received prior security clearance. This must be issued before access is granted. The issuing of a security pass cannot be guaranteed, and a security pass may be withdrawn by the *Client* at its absolute discretion at any time. Should a security pass be refused or withdrawn, the decision shall be final and conclusive.

AC7.3 The *Contractor* is responsible for providing adequate security cleared people. The *Contractor* is deemed to have allowed and included in its Prices for all costs associated with obtaining security passes, including attending the induction and any changes to the timings or content of the induction. No claim will be considered for loss, delay or inconvenience as a result of refusal or withdrawal of labour on security grounds.

AC8 Data Protection

AC8.1 Each Party complies with all applicable requirements of the Data Protection Legislation which arise in relation to this contract. This clause AC8 is in addition to, and does not relieve, remove or replace, a Party's obligations under the Data Protection Legislation.

AC8.2 The *Contractor* only uses Personal Data which is given or made available to it by the *Client* under this contract for the purpose of fulfilling its obligations under this contract and for no other purpose whatsoever.

AC8.3 The *Contractor* compensates the *Client* for any Data Loss Event suffered by the *Client* arising in any way from the *Contractor*'s performance or purported performance of the contract.

AC8.4 To the extent the *Contractor* is able to show that the Data Loss Event was not caused nor contributed to by its neglect or wrongful act, its liability under this clause is reduced.

AC8.5 If the *Contractor* shows that the neglect or wrongful act of any person (not being its staff or Subcontractor) was in part responsible for the Data Loss Event, the *Contractor*'s liability

under this clause does not extend to the share in the responsibility attributed to the neglect or wrongful act of that person.

AC8.6 Where as part of the Parties' obligations under this contract, the Parties are sharing Personal Data as independent Controllers, the Parties agree that, for the purposes of Data Protection Legislation, each Party processes Personal Data as an independent Controller in its own right. For the avoidance of doubt, nothing in this contract is intended to construe either Party as the Processor of the other Party or as joint Controllers with one another with respect to Personal Data.

AC8.7 Each Party:

(a) processes Personal Data in compliance with its obligations under the Data Protection Legislation and this contract;

(b) ensures that it has all necessary notices and consents in place to enable lawful transfer of the Personal Data;

(c) does not disclose or allow access to the Personal Data to anyone other than the personnel directly connected with provision of this contract and only in accordance with the Data Protection Legislation;

(d) ensures that all personnel are subject to written contractual obligations concerning the Personal Data (including obligations of confidentiality) which are no less onerous than those imposed by this contract;

(e) ensures that it has in place appropriate Protective Measures, reviewed and approved by the other Party, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data. Any such approval is subject to regular review by the *Client*;

(f) does not transfer any Personal Data to a third party located outside the UK unless the prior written consent of the other Party has been obtained and the transferor:

a. complies with the provisions of Articles 26 of the UK GDPR (in the event the third party is a joint Controller); and

b. ensures that (i) the transfer is to a country recognised by the UK government as providing adequate protection pursuant to Article 45 of the UK GDPR; (ii) there are appropriate safeguards in place pursuant to Article 46 UK GDPR; or (iii) one of the derogations for specific situations in Article 49 UK GDPR applies to the transfer.

AC8.8 Each Party assists the other in complying with all applicable requirements of the Data Protection Legislation. In particular, the *Contractor*, whilst complying with its own Data Protection Legislation obligations and in relation to Personal Data processed under the terms of this contract:

(a) consults with the *Client* about any notices given to Data Subjects in relation to the

Personal Data;

(b) promptly informs the *Client* about the receipt of any Data Subject Access Request (or purported Data Subject Request);

(c) provides the *Client* with reasonable assistance in complying with any Data Subject Access Request;

(d) does not disclose or release any Personal Data in response to a Data Subject Access Request without first consulting the *Client* wherever possible;

(e) assists the *Client*, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, Personal Data Breach notifications, Data Protection Impact Assessments and consultations with supervisory authorities or regulators;

(f) immediately informs the *Client* about any actual or suspected Data Loss Event, including any Personal Data Breach, in relation to the Personal Data shared under this contract;

(g) at the written direction of the *Client*, deletes or returns Personal Data and copies thereof to the *Client* on expiry or termination of this contract unless required by law to store the Personal Data;

(h) uses compatible technology to ensure that there is no lack of accuracy resulting from Personal Data transfers;

(i) maintains complete and accurate records and information to demonstrate its compliance with this clause and allow for audits by the *Client* or its designated auditor; and

(j) promptly notifies the *Client* upon receipt of any communication from the Information Commissioner's Office or any other regulatory authority in connection with Personal Data shared under this contract.

AC8.9 If the *Contractor* appoints a third-party Sub-Processor to process the Personal Data it receives from the *Client* under this contract, it complies with Article 28 and Article 30 of the UK GDPR and remains liable to the *Client* for the acts and/or omissions of the third-party Sub-Processor.

AC8.10 If the designation of the relationship between the Parties under Data Protection Legislation changes, the Parties will work together to ensure compliance with that legislation, including, for example, variations to a contract to meet the requirements of Article 28 of the UK GDPR by inclusion of the *Client*'s standard form terms and conditions and related appendix.

AC9 Malicious Software

AC9.1 The *Contractor* uses the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor to check for and delete malicious software from the *Client*'s IT systems.

AC9.2 If malicious software is identified by either Party, the Parties co-operate to reduce the effect of the malicious software. If malicious software causes loss of operational efficiency to the *Client*'s IT systems or loss or corruption of *Client* data, the Parties assist each other to mitigate any such loss and to restore the *Client*'s IT systems to full operating efficiency.

AC9.3 Any cost to the Parties arising from compliance with the provisions of clause AC9.2 is borne by:

(a) the *Contractor* where the malicious software originates from *Contractor* software and/or systems operated by the *Contractor*, any third-party software used by the *Contractor* in Providing the Service or processing *Client* data (whilst the *Client* data was under the control of the *Contractor*); and

(b) the *Client* if the malicious software originates from *Client* software and/or systems operated by the *Client* or the *Client* data (whilst the *Client* data was under the control of the *Client*).

AC10 Living Wage

AC10.1 The *Client* is accredited by Citizens UK as London Living Wage employers. The *Contractor* pays all staff and Subcontractors (including all people engaged directly or indirectly by it who undertake any work in relation to this contract) assigned to this contract, as a minimum:

(a) the London Living Wage:

(i) where the *Contractor* has Dedicated Personnel working on the Parliamentary Estate; or

(ii) where services are provided to the *Client* by Dedicated Personnel to this contract, but not carried out on the Parliamentary Estate, and the office from where Dedicated Personnel are supplying services is based in Greater London; or

(b) the Living Wage - where services are provided to the *Client* by Dedicated Personnel to this contract, but not carried out on the Parliamentary Estate and the office from where Dedicated Personnel are supplying services is based outside Greater London.

AC10.2 The *Contractor* pays to all Dedicated Personnel any increase in respect of the living wage rates throughout the performance of this contract.

AC10.3 The *Contractor* provides evidence, information and/or records at regular intervals as reasonably required by the *Client* to demonstrate that the working conditions of staff and Subcontractors (including all people engaged directly or indirectly by it who undertake any work in relation to this contract) are such as to secure the welfare of the workforce and the maintenance of stable and skilled teams. This obligation includes the salaries paid to each

such person and evidence that this is sufficient to maintain such a workforce, training and other workforce matters.

AC11 Enquiries relating to tax arrangements

AC11.1 Where the *Contractor* is liable to be taxed in the UK in respect of consideration received under this contract, it complies with all legislation relating to corporation tax and income tax, and must account to His Majesty's Revenue and Customs (HMRC) for pay as you earn (PAYE) deducted from employees' pay in respect of that consideration.

AC11.2 The *Contractor* must account to HMRC for all national insurance contributions in respect of employees working on the contract.

AC11.3 The *Client* may at any time during the term of this contract request the *Contractor* to provide information which demonstrates how the *Contractor* complies with clauses AC11.1 and AC11.2 above or why those clauses do not apply to it.

AC11.4 A request under clause AC11.3 specifies the information which the *Contractor* provides and the period within which that information is provided.

AC11.5 The *Client* may supply any information which it receives under this clause AC11 to the Commissioners of His Majesty's Revenue and Customs for the purpose of the collection and management of revenue for which they are responsible.

AC12 Accounts and Records

AC12.1 In carrying out all work under and associated with the contract, the *Contractor* completes timesheets and identifies the activities and time spent on each activity and allows the *Client* to inspect the timesheets (whether physically or by electronic transmission). The *Contractor* complies with this clause AC12.1 as part of the compensation event process.

AC12.2 The *Client* reserves the right from time to time to audit, or to nominate a reputable accounting firm to audit, the *Contractor*'s records relating to amounts claimed under the contract. This includes providing the *Client* with evidence that it has complied with this clause AC12. The *Contractor* complies with any such request and co-operates in relation to any audit. Such request may include providing the *Client* and/or the auditor access to sites controlled by the *Contractor*, equipment used in the provision of the contract, documents evidencing compliance with the contract (whether physically or by electronic transmission), and/or access to the *Contractor*'s staff and Subcontractors (including all people engaged directly or indirectly by it who undertake any work in relation to this contract).

AC12.3 The *Client* uses reasonable endeavours to ensure that the conduct of any audit does not unreasonably disrupt the *Contractor* save insofar as the *Contractor* accepts and acknowledges that control over the conduct of audits carried out by an auditor may be outside of the control of the *Client*.

AC12.4 The Parties agree that they bear their own respective costs and expenses incurred in respect of compliance with their obligations under this clause AC12, unless the audit reveals a

material default or fraud by the *Contractor.* In which case, the *Contractor* reimburses the *Client* for the *Client*'s reasonable costs incurred in relation to the audit.

AC12.5 The *Contractor* ensures that the *Client* is afforded access to all the Subcontractors accounts and records in the same way as it is to the *Contractor*'s accounts and records.

AC12.6 Audits carried out by the *Client* shall include, but not be limited to, the *Contractor* and Subcontractor accounts and records set out in the Scope.

AC13 Bribery Act 2010, prevention of corruption and whistleblowing

AC13.1 The *Contractor* warrants that no offence under the Bribery Act 2010 ("**Bribery Act"**) has been or will be committed by:

(a) the *Contractor*; or

(b) any associated person of the *Contractor*,

in connection with the procurement or implementation of this contract or any other contract between the *Client* and the *Contractor*.

AC13.2 For the purposes of clause AC13.1(b), the definition of "associated person" in section 8 of the Bribery Act applies.

AC13.3 If at any time the *Contractor* has knowledge of, or has reasonable grounds to suspect the occurrence of, a breach of the warranty in clause AC13.1, the *Contractor* promptly notifies the *Client* of such matters within its knowledge, or of such grounds for suspicion, and co-operates with the *Client* in the investigation of such breach or suspected breach of warranty.

AC13.4 The *Contractor* does not enter into this contract or any other contract with the *Client* in connection with which commission has been paid or agreed to be paid by it or on its behalf or to its knowledge unless, before any such contract is made, particulars of any such commission, and of the terms and conditions of any agreement for the payment thereof, have been disclosed in writing to the *Client*.

AC13.5 If the *Contractor* is approached by a member of staff or someone representing themselves as acting on behalf of the *Client* who seeks to persuade him to take any steps that would constitute a breach of this clause or of the Bribery Act 2010, the *Contractor* must immediately contact the Director of Finance at the *Client*.

AC13.6 In exercising its rights and remedies in relation to this clause, the *Client* acts in a reasonable and proportionate manner having regard to such matters as the gravity of and the identity of the person performing the prohibited act and give all due consideration, where appropriate, to action other than termination of the contract.

AC14 Modern Slavery Act 2015

AC14.1 In this clause AC14:

(a) **2015 Act** means the Modern Slavery Act 2015;

(b) **Specified Offence** means an offence under Part 1 of the 2015 Act;

(c) **Prevention Order** means an order under Part 2 of the 2015 Act;

(d) **Transparency Statement** means the statement of a commercial organisation under Part 6 of the 2015 Act;

(e) **Supply Chain** means:

a. the *Contractor*; and

b. any Subcontractor of the *Contractor* supplying goods or services to be used for the purposes of the *service*; and

(f) **Subcontractor of the Contractor** includes any sub-sub-contractor or consultant of any tier.

(g) **Modern Slavery Policy** means the *Client's* Modern Slavery and Human Trafficking Policy as may be provided to the *Contractor* from time to time.

AC14.2 The *Contractor* warrants and undertakes that:

(a) it will, and will procure that the Supply Chain will, comply with the 2015 Act and the Modern Slavery Policy throughout the contract term;

(b) throughout the period of this contract, if it is a relevant commercial organisation as defined by section 54 of the 2015 Act, it is compliant with the annual reporting requirements contained within that section;

(c) it has not been convicted of any Specified Offence or any slavery or human trafficking offences equivalent to any Specified Offence anywhere in the world;

(d) it has notified the *Client* of all past and current investigations, inquiries or enforcement proceedings by any governmental, administrative or regulatory body regarding any offence regarding slavery and trafficking involving the *Contractor*, the *Contractor*'s employees or Officers, or the Supply Chain;

(e) none of its employees or Officers, and no part of the Supply Chain has been convicted of any Specified Offence or any slavery or human trafficking offences equivalent to any Specified Offence anywhere in the world;

(f) it will not, during the period in which any of its obligations under this contract remain to be performed, commit any Specified Offence, nor by any wrongful act or omission give cause for any Prevention Order to be made against it; and

(g) if and as required to do so by the 2015 Act, it has made and published and/or will make and publish a Transparency Statement and that in doing so it has not wilfully made and

will not wilfully make any false statement, and has not concealed and will not conceal any facts or circumstances within its knowledge tending to incriminate itself in the commission of a Specified Offence.

(h) it will implement appropriate due diligence procedures to ensure that there is no slavery or human trafficking in any part of the Supply Chain including maintaining records to trace all parts of the Supply Chain providing the *service* to the *Client* under the contract.

AC14.3 The *Contractor* shall notify the *Client* immediately if it becomes aware of any actual or suspected breach of the 2015 Act or the Modern Slavery Policy by the Supply Chain.

AC14.4 The *Contractor* shall, within two weeks of being requested to do so or such other period as required by the *Client*, provide to the *Client* any information, records or assistance within its power or possession which the *Client*:

(a) requests to assist in the investigation of any reasonable suspicion that a Specified Offence has been or is being committed by any member of the Supply Chain, directly or indirectly in connection to the performance of this contract; or

(b) might reasonably wish to include in any Transparency Statement it proposes to make.

AC14.5 If for the purposes of any investigation referred to in clause AC14.4(a) the *Client* requests the *Contractor* provide access to any permanent or temporary place of work of, or to any person working for, any member of the Supply Chain, the *Contractor* shall provide such access and ensure that such access is provided within the timescales specified by the *Client*. Access for the *Client* shall include access for any third party experts instructed by the *Client* in connection with any investigation.

AC14.6 If, following any investigation referred to in clause AC14.4(a), any issues are identified (and without prejudice to the *Client*'s rights under clause AC14.12), the *Contractor* will, within two weeks of a request from the *Client* or such other period as required by the *Client*, submit an action plan to the *Client* for approval. Once approved, the *Contractor* will deliver the action plan to remedy any such issues. For the avoidance of doubt, this contract may be varied in accordance with any agreed action plan where such variation is in accordance with the terms of the contract.

AC14.7 A failure by the *Contractor* to submit or deliver an action plan in accordance with AC14.6 will entitle the *Client* to the remedies available in AC18.

AC14.8 The *Contractor* will, within two weeks of a request from the *Client* or such other period as required by the *Client*, provide to the *Client* information to demonstrate its approach to modern slavery and human trafficking. This information may include, but is not limited to:

(a) workforce conditions

(b) details of supply chain monitoring

(c) updates on any action plans in place with the Supply Chain

(d) working/employment practices

(e) risk management and monitoring processes

(f) recruitment practices.

AC14.9 The *Client* requires the *Contractor* to complete the Home Office Modern Slavery Assessment Tool questionnaire ('MSAT') or any other relevant questionnaire or assessment as specified by the *Client*, unless the *Client* instructs the *Contractor* otherwise. The *Contractor* will

(a) complete the MSAT or any other questionnaire or assessment immediately upon request from the *Client* and in all cases within 8 weeks of the Contract Date;

(b) provide a copy of any previously completed MSAT to the *Client* within 2 weeks of the Contract Date if the *Contractor* has previously completed the MSAT for a public sector body within the year prior to the Contract Date;

(c) review and update the MSAT or any other questionnaire or assessment at any time during the contract term immediately upon request by the *Client*;

(d) ensure that all responses to the MSAT or any other questionnaire or assessment are complete and accurate.

AC14.10 The *Client* and the *Contractor* will both monitor compliance with the 2015 Act and the Modern Slavery Policy throughout the period of the contract. To enable such monitoring the *Client* may

(a) (in addition to clause AC14.5) carry out site visits, to be arranged with the *Contractor* at a mutually convenient time but not to be unreasonably delayed following the *Client*'s request;

(b) set key performance indicators or performance targets to ensure full compliance and that such compliance is being maintained;

(c) require the *Contractor* to prepare and deliver to the *Client* upon each anniversary of the Contract Date and updated on a frequency defined by the *Client*, a slavery and human trafficking report setting out the steps it has taken to ensure that slavery and human trafficking is not taking place in the Supply Chain or in any part of its business.

AC14.11 The *Contractor* shall include in any contract by which it appoints another Supply Chain member, provisions imposing on that person obligations, warranties and undertakings in favour of the *Contractor* equivalent to those imposed on the *Contractor* under this clause Z14.

AC14.12 When assessing any breach or potential breach under this clause, the *Client* is entitled to use and have regard to information relating to modern slavery issues from third party organisations including but not limited to local NGOs, trade unions, researchers or experts.

AC14.13 Breach of this clause AC14 entitles the *Client* to require the *Contractor* to terminate a Subcontract and/or remove from performance of the contract any Subcontractor, employee or other persons associated with it whose acts or omissions have caused the breach.

AC15 Discrimination, human rights and safeguarding

AC15.1 The *Contractor* does not unlawfully discriminate within the meaning and scope of the provisions of or made under the Equality Act 2010 or any other legislation relating to discrimination in employment or in the provision of services/goods in relation to this contract or any other contract it has entered into with the *Client*.

AC15.2 The *Contractor* recognises the obligations imposed upon the *Client* by the Human Rights Act 1998 and does not do anything when performing this contract which may cause the *Client* to be in breach of that Act.

AC15.3 The *Contractor* takes all reasonable steps to secure the observance of these provisions by its Subcontractors engaged in the carrying out of this contract.

AC15.4 The *Contractor* complies with the *Client*'s policy on Safeguarding Children and Vulnerable Adults (as required under the Protection of Freedoms Act 2012). The policy may be accessed from the following website:

https://www.parliament.uk/visiting/access/safeguarding-on-the-parliamentary-estate/

AC16 Soliciting work and/or personnel / recommending additional work

AC16.1 The *Contractor* does not solicit work for any part of its organisation, including partners, associate or parent companies, or to make recommendations or tender advice that directly leads to additional work with the *Client* for the *Contractor* either as a variation or extension to this contract or by the award of a separate non-competitive contract.

AC16.2 The Parties agree not to offer employment to or solicit the other's personnel who within 6 months of such action has been involved directly or otherwise connected to this contract (except where an individual responds directly to a general recruitment campaign) nor use the services of any such personnel, either independently or via a third party, for a period of 6 months from the date that the individual concerned ceases to be permanently involved with this contract.

AC16.3 The *Client* may recover from the *Contractor* any loss sustained in consequence of any breach of clause AC16.2, whether or not the contract has been terminated.

AC17 Behaviour and conduct

AC17.1 In performance of this contract and when working on the *Client*'s Premises and/or when interacting with any of the *Client*'s staff, the *Contractor* complies with the same standards of behaviour and conduct expected of the *Client*'s staff (as set out in the Scope).

AC17.2 Breach of any part of the *Client*'s Independent Complaints and Grievance Scheme (as set out in the Scope) is a reason for the *Client* to request the removal of a person from the contract.

AC18 Remedies, non-waiver and set-off

AC18.1 All remedies available to the *Client* under this contract are without prejudice to any common law rights including termination by consent and shall survive the expiry or termination of the contract.

AC18.2 Except as otherwise expressly provided by this contract, all remedies available to either Party for breach of this contract are cumulative and may be exercised concurrently or separately, and the exercise of any one remedy is not deemed an election of such remedy to the exclusion of other remedies.

AC18.3 If the *Contractor* breaches the terms of a Security Aspects Letter or a non-disclosure agreement, the *Client* is entitled to apply any remedy as set out in the Security Aspects Letter or non-disclosure agreement.

AC18.4 A failure to exercise any right or remedy does not constitute a waiver of that right or remedy.

AC18.5 A waiver is not effective unless it is communicated to the other Party in writing.

AC18.6 A waiver of any right or remedy arising from a breach of this contract does not constitute a waiver of any right or remedy arising from any other breach.

AC18.7 Without prejudice to any of the *Client*'s other rights and remedies under this contract or otherwise, the *Client* is entitled to set off all or any of its liabilities to the *Contractor* against all or any of the *Contractor*'s liabilities to it whether such liabilities arise under this contract or any other contract between the *Contractor* and the *Client* (or between the *Contractor* and (i) the Corporate Officer of the House of Lords, if not the *Client*, (ii) the Corporate Officer of the House of Commons, if not the *Client*, or (iii) both the Corporate Officers acting jointly, if not the *Client*) and whether such liabilities are present or future, liquidated or unliquidated.

AC19 Conduct / handling of claims

AC19.1 The *Client* notifies the *Contractor* as soon as reasonably practicable of any claim or proceedings for which the *Contractor* may be liable under this contract.

AC19.2 Where the *Contractor* is or may be liable to indemnify the *Client* in respect of any claim or proceeding by a third party, it or, if it so wishes, its insurer, is responsible (subject to the rest of this clause) for dealing with or settling that claim or proceeding.

AC19.3 The *Client* deals with any claim which involves a Government Provision or which is made by or against a member of the *Client*'s staff, or a member of either House of Parliament, or a

member of staff of a member of either House of Parliament and clause AC19.2 does not apply to any such claim.

AC19.4 When the *Contractor* or its insurers are dealing with any claim or proceeding, if a matter or issue arises which involves, or may involve, any privilege or special right of the *Client* (including a matter relating to the discovery or production of documents), the *Contractor* or its insurers consults the *Client* before taking any further action on the matter and acts in relation thereto as may be required by the *Client*. If either the *Contractor* or its insurers fail to comply with this clause AC19.4, clause AC19.2 ceases to apply.

AC19.5 The *Contractor* shall maintain a register of all claims under all the insurances in connection with this contract and shall allow the *Client* to review such register at any time.

AC19.6 Except where the *Client* is the claimant party, the *Contractor* shall give the *Client* notice within 20 working days after any insurance claim in excess of £100,000 relating to or arising out of the provision of this contract on any of the insurances required by this contract or which, but for the application of the applicable policy excess, would be made on any of those insurances and (if required by the *Client*) full details of the incident giving rise to the claim.

AC20 Additional reasons for termination

AC20.1 In addition to the *Client*'s termination rights set out elsewhere in this contract, the *Client* may terminate the *Contractor*'s obligation To Provide the Service in any of the following circumstances:

(a) the contract has been subject to a substantial modification which would have required a new procurement procedure in accordance with regulation 72(9) of the PCR 2015;

(b) the *Contractor* has, at the time of contract award, been in one of the situations referred to in regulation 57(1) of the PCR 2015, including as a result of the application of regulation 57(2) of the PCR 2015, and should therefore have been excluded from the procurement procedure or it becomes known to the *Client* after contract award that the *Contractor* or its representatives have been in one of the situations referred to in regulation 57(1) of the PCR 2015;

(c) a change of control of the *Contractor* (and/or parent company if relevant) occurs within the meaning of sections 450, 451 and 1124 of the Corporation Tax Act 2010;

(d) the *Contractor* (and/or the parent company if relevant) is an unincorporated joint venture or a partnership and a change of control occurs of any company which is a party to the joint venture or partnership or any change in the composition of the joint venture or partnership occurs which in the reasonable opinion of the *Client* (having taken reasonable steps to consult with the *Contractor*) represents a material change (having regard, without limitation, to its financial standing, ability to meet its obligations and liabilities, any actual or potential reputational damage to the *Client* in continuing to contract with the *Contractor,* and any other matters prejudicial to the *Client*);

(e) the *Contractor* commits a cyber or physical security violation by reference to the *Client*'s security requirements;

(f) the *Contractor* fails to comply with clauses 12.10, AC14.2 – AC14.12, AC15.1 – AC15.4, AC16.2 and AC22.1;

(g) the *Contractor* (i) fails to provide the necessary information in response to a request under clause AC11.3 or AC11.4 within the timescales specified or, where not specified, within a reasonable time or (ii) provides information which is inadequate to demonstrate either how it complies with clauses AC11.1 and AC11.2 or why those clauses do not apply to it;

(h) the *Client* receives information which demonstrates that, at any time when clauses AC11.1 and AC11.2 apply to the *Contractor*, the *Contractor* is not complying with those clauses;

(i) the *Contractor* breaches the terms of a Security Aspects Letter or a non-disclosure agreement;

(j) the *Contractor* or anyone employed by it or acting on its behalf (whether with or without its knowledge)

a. is in breach of clause AC13, in relation to this or any other contract with the *Client*;

b. is convicted of any offence under the Bribery Act 2010 in relation to this contract or any other contract with the *Client.*

AC20.2 If the *Client* terminates under:

(a) clause AC20.1(a), or

(b) clause AC20.1(b) in any circumstances other than as a result of information not disclosed by the *Contractor*

the procedures and amounts due on termination are the same as those set out at clause AC20.7. If it is not practicable in the circumstances for the *Client* to give the *Contractor* 30 days' written notice of the termination, the *Client* gives the *Contractor* as much written notice as possible.

AC20.3 If the *Client* terminates under:

(a) clause AC20.1(b) as a result of information not disclosed by the *Contractor*, or

(b) clause AC20.1(g), (h) or (i)

the procedures and amounts due on termination are the same as if the *Contractor* has substantially failed to comply with its obligations (as per clause 90.3 Reason 2) save that the *Contractor* is not entitled to any amount due to it under clause 92.1. The *Client* may recover from the *Contractor* the amount of any loss resulting from the termination.

AC20.4 If the *Client* terminates under clause AC20.1(c) to (f) and (j), the procedures and amounts due on termination are the same as if the *Contractor* has substantially failed to comply with its obligations (as per clause 90.3 Reason 2) save that the *Client* is not required to give the *Contractor* four weeks' notice to rectify the default prior to the termination, the *Contractor* is not entitled to any amount due to it under clause 92.1 and the *Client* may recover from the *Contractor* the amount of any loss resulting from the termination.

AC20.5 Clauses AC20.1(c) or (d) are only available to the *Client* within 6 months after a change of control occurs and is not available where it has agreed in advance with the *Contractor* to the particular change of control that happens.

AC20.6 If the *Client* terminates under clause AC20.1(j), in addition to AC20.4 the *Client* is entitled to recover from the *Contractor* the value of any gift, consideration or commission and/or any other loss sustained in consequence of any breach of clause AC13.

AC20.7 The *Client* may terminate the contract, or any part of it, at any time by giving a minimum of 30 days written notice to the *Contractor*. The *Client* may extend the period of notice at any time before it expires. The procedures and amounts due are:

(a) the *Client* is not liable to pay the *Contractor* in accordance with clause 9, but compensates the *Contractor* for any commitments, liabilities or expenditure which would otherwise represent an unavoidable loss by the *Contractor* by reason of the termination of the contract, provided that the *Contractor* takes all reasonable steps to mitigate such loss. Where the *Contractor* holds insurance, it reduces its unavoidable costs by any insurance sums available. The *Contractor* submits to the *Client* a fully itemised and cost list, with supporting evidence, of such losses reasonably and actually incurred by it as a result of termination.

(b) the *Client* is not liable under this clause AC20.7 to pay any sum to the *Contractor*:

- which was claimable under insurance held by the *Contractor*, and the *Contractor* has failed to make a claim on its insurance, or has failed to make a claim in accordance with the procedural requirements of the insurance policy;
- which, when added to any sums paid or due to the *Contractor* under the contract, exceeds the total sum that would have been payable to it if the contract had not been terminated prior to Completion;
- for any indirect or consequential loss arising under or in connection with the contract; or
- when the contract has reached Completion, except where the sum has already been expressly agreed prior to the date of Completion.

AC21 CDM 2015

AC21.1 Each Party undertakes to the other that it has complied and will comply with its statutory duties under the Construction (Design and Management) Regulations 2015 ("**CDM Regulations**") in relation to the *service* and any duties and obligations set out in the Scope.

AC22 Health and safety

AC22.1 The *Contractor* carries out the *service* and its obligations under this contract in accordance with the requirements of the Health and Safety at Work etc. Act 1974, CDM Regulations, any other applicable health and safety law, the *Client*'s and any other health and safety requirements identified in the Scope. Notwithstanding the foregoing, the *Contractor* remains responsible for the health and safety of, and takes all necessary measures to protect, its employees (including all people engaged directly or indirectly by the *Contractor* (or any Subcontractor) who undertake any work in relation to this contract), suppliers, Subcontractors, the *Client*'s staff and Others whilst working on or adjacent to the property affected by the *Contractor*'s work.

AC22.2 Without prejudice to any other clauses in this contract, should the *Contractor* fail to comply with clause AC22.1, the *Client*:

(a) reserves the right to suspend the contract with immediate effect and withhold payments until the issue is resolved by the *Contractor*, who will carry out the necessary health and safety work at its own expenses in order to resume the main contractual duties;

(b) is exempt of any liability arising in connection with the *Contractor*'s failure to comply with any health and safety law or agreed requirement in this contract;

(c) reserves the right to deduct payment or claim compensation from the *Contractor* where (i) the health and safety breach or failure is not rectified by the *Contractor* within a reasonable time following notification of the breach or failure, (ii) it is incapable of being remedied, and/or (iii) the *Client* has to intervene either by carrying out the necessary work or hiring another contractor to do it as a matter of emergency; and/or

AC23 The Transfer of Undertakings (Protection of Employment)

AC23.1 In the event that Transfer of Undertakings (Protection of Employment) Regulations 2006 ("TUPE") applies to the contract, the *Contractor* shall comply with its obligations under TUPE and (if applicable) New Fair Deal.

AC23.2 At least 12 months prior to the expiry of the contract (or any extension), or after the *Client* has given notice to terminate the contract, or at any time upon request from the *Client*, the *Contractor* shall provide the *Client* (within 28 days of the *Client*'s request) with all employee information including, but not limited to, the total number of employees assigned for the purposes of TUPE to Provide the Service. For each person identified, the *Contractor* must provide the TUPE Information.

AC23.3 The *Contractor* warrants the accuracy of the information provided under this clause Z23 and will notify the *Client* of any changes to the information as soon as reasonably possible. The *Contractor* will permit the *Client* to use and disclose the information to a contractor during

any tender process.

AC23.4 The *Contractor* does not make any changes to its permanent personnel establishment or terms and conditions of employment within 12 months of the end of the *service period* without the written permission of the *Client*.

AC23.5 The *Contractor* responds within 5 working days to any questions or requests for supplementary information required during the tender process unless such requests are commercially sensitive.

AC23.6 This clause does not indicate that the *Client* is making any declaration about the application of TUPE; the *Contractor* should take its own legal advice.

AC23.7 In the event of any change of contractor, any discussions with regards to the application of TUPE will be between contractors. The *Client* only becomes involved if there is any breach, or potential breach, of the tendering or contract terms and conditions.

AC23.8 The *Contractor* will indemnify the *Client*, any new contractor and/or any former contractor for all losses arising from:

(a) its failure to comply with its obligations under TUPE;

(b) its failure to comply with the provisions of this clause AC23; and

(c) any claim by any employee or person claiming to be an employee (or their employee representative) of the *Contractor* which arises or is alleged to arise from any act or omission by the *Contractor* on or before the date of the Relevant Transfer (as defined in TUPE).

AC23.9 The provisions of this clause AC23 apply during the contract term and for the limitation period specified in Clause AC24.

AC24 Limitation Act 1980

Irrespective of the manner in which this contract is executed or made, for the purposes of the Limitation Act 1980, all claims arising under this contract have the same limitation period as applies to claims pursuant to deeds. Neither Party relies on any limitation defence which might otherwise be available to defeat any claim any earlier.

AC25 Counterparts

This contract may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one contract.

AC26 Intellectual Property Rights

AC26.1 The *Client* owns the *Contractor*'s rights over material prepared for the design of the *service*

except as stated otherwise in the Scope. The *Contractor* obtains other rights for the *Client* as stated in the Scope and obtains from a Subcontractor equivalent rights for the *Client* over the material prepared by the Subcontractor. The *Contractor* provides to the *Client* the documents which transfer these rights to the *Client*.

AC26.2 It is a condition of the contract that, except to the extent that materials may incorporate designs provided by either the House of Commons or the House of Lords or the *Client*, and subject to clause AC26.3, the *Contractor:*

- does not infringe any Intellectual Property Rights of any third party; and
- indemnifies the *Client* against all actions, suits, claims, demands, losses, charges, costs and expenses which the *Client* may suffer or incur as a result of, or in connection with, any breach of this clause.

AC26.3 The Crowned Portcullis is a royal badge and its use by the Houses of Parliament has been formally authorised by licence granted by the Sovereign, who is the owner of all Intellectual Property Rights in the badge. It must not be used except under the express direction and control of the House of Commons or the House of Lords.

AC26.4 Pursuant to section 165 of the Copyright, Designs and Patents Act 1988 (as amended), the House of Commons or the House of Lords, separately or jointly, are the first owner(s) of copyright in work made by them or under their direction or control, which includes any work made in preparation for or as part of the requirements of this contract, and that copyright is referred to as "**Parliamentary Copyright**".

AC26.5 Where the *Client* provides or makes available to the *Contractor* any materials:

(a) in which Parliamentary Copyright subsists, that copyright remains the property of the House of Commons or the House of Lords or both jointly;

(b) in relation to which the *Client* is the owner of any other Intellectual Property Rights, those rights remain the property of the *Client*;

(c) the *Contractor* has the right to use those materials only to Provide the Service. The *Contractor* may make this right available to its Subcontractors, where necessary to Provide the Service;

the *Contractor* returns those materials to the *Client* at the end of the *service period* or termination of the contract (howsoever arising).

AC26.6 Where any materials are prepared by or for the *Contractor* for use, or intended use, in relation to the performance of this contract, all Intellectual Property Rights in that material belong to the *Client*. The *Contractor* may not use those materials for work other than for the *Client*.

AC26.7 Insofar as Parliamentary Copyright does not subsist in any material or works which are the subject matter of this contract (including any preparatory materials created for or as part of the requirements of this contract) or AC26.6 does not apply, the *Contractor* assigns to the *Client* with full title guarantee and free from all third-party rights, the Intellectual Property Rights and all other

rights in that material or works.

AC26.8 Where the *Contractor* is not the legal owner of the Intellectual Property Rights in any such material or works (including any work completed in preparation for or as part of this contract), it procures an irrevocable, non-exclusive licence in favour of the *Client*. The cost of any such assignment or licence is deemed to be included within the offered total of the Prices from the Price List. The *Contractor* indemnifies the *Client* against all actions, suits, claims, demands, losses, charges, costs and expenses which the *Client* may suffer or incur as a result of, or in connection with, any breach of this clause.

AC26.9 All royalties, licence fees or similar expenses for the supply or use of any invention, process, drawing, model, plan or information in connection with the contract are deemed included in the offered total of the Prices from the Price List.

AC26.10 The *Contractor* indemnifies the *Client* from and against all demands, actions, claims and proceedings which may be made or brought against the *Client*, and any damages, cost and expenses incurred by the *Client* in respect of the supply or use of those matters referred to in clause AC26.9.

ANNEX 5: Price List

1. The prices and rates entered in the Pricing Schedule shall include all the costs that the *Client* will pay in order for the *Contractor* to fully provide the requirements of the Contract, including all incidental and travel/accommodation expenses. All costs associated with each activity should be included. No other costs will be paid by the *Client.* The rates and costs submitted shall be Firm Price and for the duration of the contract.

2. The prices provided shall be exclusive of VAT and in GBP.

3. People Rates are to be inserted for ALL roles in the People Rates tab, please ensure that this is carried out otherwise the *Client* will not be able to evaluate your tender as all the rates listed are needed to allow for evaluation. The rates supplied shall include all incidental and travel/accommodation expenses. All costs associated with each role should be included, no other costs will be paid by the *Client*. The rates shall be for the duration of the contract.

Pricing Schedule - STC1173(A)

Item	Year 1 GBP (ex. VAT)	Year 2 GBP (ex. VAT)	Year 3 GBP (ex. VAT)	Year 4 GBP (ex. VAT)	Year 5 GBP (ex. VAT)	Total (ex. VAT)
Activity 1- Validation of Exisitng Designs and Build Schedules (Please see the Scope for a full breakdown of the activities)						
1. Cost per design review						
1. Cost per new design						

1. Cost per venue visit and survey						
Activity 2 – Storage and Logistics(Please see the Scope for a full breakdown of the activities)						
2. Cost 190m3 climate controlled storage for year (1/12th per month)						
2. Cost 350m3 non-climate controlled storage (1/12th per month)						
Activity 3 – Potential Rehearsals of build with existing supply chain (Please see Annex A, B and C of the Scope for details on requirements of each scenario)						
3. Delivery of elements described in 'Scenario 1, Annex A'						
3. Delivery of elements described in 'Scenario 2, Annex A'						
3. Delivery of elements described in 'Scenario 3, Annex A'						
3. Delivery of elements						

described in 'Scenario 4, Annex A'						
3. Provision of Welfare Facilities for *Contractor* personnel **per rehearsal**						
3. Weekly Scaffold Safety Inspection (required during rehearsals)						
Activity 4 - Ongoing Contract Management						
4. Contract Management (1/12th per month)						
4. Please breakdown any headline costs by adding lines below if needed but please ensure that the value total matches the line above that is broken down)						
Activity 5 – Set up and ongoing management of arrangements to allow real life activation (Please see Annex A, B and C of the Scope for details on requirements of each scenario)						
5. Delivery of elements described in 'Scenario 1,						

Annex A' (including up to 12 months maintenance and support of structure and de-rig)						
5. Delivery of elements described in 'Scenario 2, Annex A' (including up to 12 months maintenance and support of the structure)						
5. Delivery of elements described in 'Scenario 3, Annex A' (including up to three weeks maintenance and support and de-rig)						
5. Weekly Scaffold Safety Inspection (required during Activation)						
5. Provision of Welfare Facilities for *Contractor* personnel **per Activation**						
Please breakdown any of the additional costs from the headline costs in this section 5 below but ensure the value totals the line item above that is being broken down.						

STC1173(A) People Rates
Please provide a list of hourly rates for the different trades that will be involved in the contract as below. All trade costs are expected to have been included within the Pricing Schedule above. The hourly rates will be used as the People Rates in any future contract for Compensation Events in accordance with the contract.

Role	£ per hour (Ecl. VAT)
Design Director	
Designer	
Design Assistant	
Administration	
Contract Manager	
Surveyor	
Project Manager	
Programme Manager	
Contractor Equipment Coordinator	
Safety Manager	
Logistics Manager	
Supervisor	
Labourer	
Rigger	
Carpenter	
Electrician	
Scaffolder	
Scaffold Safety Inspector	

ANNEX 6: Not Used

ANNEX 7: Security Aspects Letter, Schedules, PSMP and Principal Contractor and Principal Designer Appointment Letter.

The following documents are incorporated into this Contract:

Security Aspects Letter

Security Aspects Letter in Respect of PHD Modular Access Services Limited

Date of Issue: 5th March 2024

1. This document is a Security Aspects Letter ("SAL") and comprises this Letter and three Schedules:

Schedule 1 – Classification Table;
Schedule 2 – Parliamentary Protective Marking Scheme (PPMS);
Schedule 3 – Detailed Information Security Assessment (DISA).

2. The parties to this SAL are:
   a. The Corporate Officer of the House of Lords and Corporate Officer of the House of Commons, acting jointly of Westminster, London SW1A 0PW (the **"Authority"**); and
   b. PHD Modular Access Services Limited with:
      - company number: 02690003,
      - 54 Oxford Road, Denham, Uxbridge, Middlesex UB9 4DN (the **"Contractor")** together the "parties".

3. The Authority and the Contractor are parties to a contract (the "Contract") for construction services in relation to the UK Parliament called Principal Contractor: Events, Contract ref. STC1173(A). The parties agree that:
   a. this SAL forms part of the Contract (and any entire agreement or similar such clause shall have no effect upon this SAL); and
   b. in consideration of the Authority entering into the Contract, the Contractor shall comply with this SAL in relation to the Contract.
   c. The SAL supersedes and replaces any previous SAL in relation to the Contract.

Note:
For the avoidance of doubt, for these purposes references to the Contract include both the framework agreement between the Authority and the Contractor and all call-off orders issued under it.

4. This SAL identifies and defines the information security requirements issued by the Authority to be applied by the Contractor to accessing, processing, holding, generating of, or any other dealing with, Classified information assets as part of the Contract. These requirements are effective from the Date of Issue of this SAL. In this SAL the definition of "Classified" is as stated in the PPMS (Schedule 2).

5. In this SAL the definition of "sub-contract" or "sub-contractor" includes sub-consultancy and sub-consultants, and any other form or designation of agreement for

the contracting of work for the purposes of this Contract, including any further sub-contracting of any sub-contracted portions of the Contract (i.e. sub-sub-contracts and below).

6. This SAL is in addition to actions taken and responses provided by the Contractor before and during its procurement process regarding how it will meet the Authority's data security and protection requirements; this information may have been set out within a Non-Functional Security Requirements, Non-Disclosure Agreement or similar document received by or completed during the tender process.

7. The Contractor agrees that its work will involve it holding and generating information assets, and that it will:

a. protect the confidentiality of the Authority's security Classified information assets;

b. complete and comply with this SAL;

c. incorporate essential security requirements and protections in all relevant sub-contracts so that they are back-to-back with this SAL, and ensure compliance with it;

d. apply the sensitivity levels as set out in the Classification Table (Schedule 1), which will be supplied completed by the Authority, and notify the Authority if additional descriptions of information need to be added to the Classification Table, for example for contractor generated information assets.]

e. mark any unmarked information assets with a security protective marking that follows the PPMS (Schedule 2);

f. generate, hold and mark information assets in accordance with the PPMS; and

g. comply with the DISA (Schedule 3).

8. In the event of a conflict between this Letter and the Schedules, this Letter shall prevail. In the event of a conflict between each or any of the Schedules, the Schedules shall have the following order of precedence:

1. Schedule 1 – Classification Table;
2. Schedule 2 – PPMS;
3. Schedule 3 – DISA.

In the event of any conflict between this SAL and the provisions of the Contract, this SAL shall prevail.

Applying the SAL

9. Whilst the SAL applies only to Classified information assets (except where the contrary is stated), nonetheless the Contractor should apply good business sense and practice to all information assets connected to the Contract regardless of their level of sensitivity.

10. In addition to or compliance with the requirements at paragraph 7 above, the Contractor will:

a. bring the levels of protective marking required by this SAL to the attention of

a. the person in the company directly responsible for the security aspects of the Contract and

b. any sub-contractor (who must be sub-contracted in writing) working on the project (as described in the Contract) where it is envisaged they will receive access to Classified information assets;

b. implement security controls to safeguard Classified information assets in accordance with the SAL;

c. regardless of its unmarked status, use its reasonable endeavors to protect UNRESTRICTED information (designated as such in accordance with the Classification Table at Schedule 1); and

d. transmit Classified information assets created by the Contractor and/or its Sub-contractors to the Authority in accordance with this SAL and PPMS.

Schedules to this SAL

11. The Classification Table (Schedule 1) identifies the different types of information within a particular contract which are Classified information assets requiring protection over and above that stipulated (i) in the specific contract, (ii) by legal requirements, or (iii) pursuant to good business sense and practice; for example, information about the existence of the contract itself, BIM data, or correspondence.

12. The first column in the Classification Table identifies the different types of Classified information asset that a contractor is likely to be managing during the particular contract. The second column specifies the Classification to be applied to each type of information asset. Contractors can then refer to the PPMS (Schedule 2) for details about how the material should be handled in accordance with the Classification. The Authority will complete the Classification Table once a preferred bidder has been identified, and the classifications set out in the table will apply to all Classified information relating to the Contract.

13. The originator of Classified information assets may be the Authority, the Contractor or a third party contracted to the Authority. The originator is responsible for ensuring that the Classified information assets bear a protective marking in accordance with the PPMS (Schedule 2) or, where this is not required or practical, of making any recipient aware of the degree of sensitivity of the information in another way. This will be completed for Classified information assets in accordance with this SAL. The Contractor must communicate the level of sensitivity of the information asset and the security controls associated with it to all those who will receive, generate or be exposed to that information.

14. The DISA (Schedule 3) contains information provided by the Contractor as part of their bid to demonstrate their information security capabilities, supported by relevant information security certification.

Security certification

15. The Contractor and its sub-contractors must hold proportionate information security certifications that meet the approval of the Authority such as Cyber Essentials or ISO 27001 or equivalents.

16. If (a) Cyber Essentials or ISO 27001 certification is for some reason unachievable; or (b) the Contractor and its sub-contractor is working towards Cyber Essentials or ISO 27001 certification, then (at the Authority's discretion) the Contractor and its Sub-contractor undertakes to work towards certification in a time frame agreed with the Authority or to provide evidence in the DISA (Schedule 3) equivalent to a formal certification.

Audit

17. The Authority reserves the right to: (a) ask further questions; and/or (b) undertake an audit and/or physical review of the Contractor's and its sub-contractors' facilities (including without limitation its IT systems); and/or (c) take any and all necessary action (as the Authority deems fit in its sole discretion) to ensure the security and integrity of its information, which may include (without limitation) suspending or limiting the transfer of any information to the Contractor and its sub-contractor and/or any other third party until any and all identified issues are resolved to the satisfaction of the Authority.

18. The Authority may audit the Contractor's processes relating to compliance with this SAL and the protection of information concerning the Contract at any time on giving reasonable notice to the Contractor. The areas liable to audit include, but not exclusively:

a. Premises where information assets are processed, stored or accessed;
b. Electronic systems that process, store or transmit information assets;

c. Physical locations, such as cupboards or cabinets where information is stored; and/or

d. Other locations, facilities or sites that process, store or have access to information.

It is a condition of this SAL that the Authority will be granted access to the areas that are subject to audit for the purpose of completing an audit and any related follow-up audit.

Sub-contracts

19. The Contractor is liable for any breach of this SAL by its Sub-contractors. The Contractor has responsibility for ensuring and auditing the compliance of its Sub-contractors with the SAL and for reporting on such audits to the Authority as the Authority requires.

Breach and miscellaneous

20. Breach of the terms of this SAL by the Contractor, its agents, employees, designers and any sub-contractor will amount to a breach of the Contract entitling the Authority in its discretion to terminate the Contract, apply the relevant provisions of this SAL, or apply any other remedy provided for in the Contract or at common law. Notwithstanding that right to terminate or its rights at common law, the Authority may in its absolute discretion choose to:

a. Assess the breach;

b. Hold an investigation; and/or

c. Take appropriate action which may in the Authority's discretion fall into three categories:

i. Informal warning. A verbal warning given with a written record confirming subject discussed, time and location;

ii. Formal warning to the company in question; or

iii. Terminate contract.

All rights or remedies listed within this SAL are within the Authority's discretion, are cumulative, and may be exercised concurrently or separately. The exercise of any one remedy shall not be deemed an election of such remedy to the exclusion of other remedies.

21. The failure of the Authority to exercise any right or remedy shall not constitute a waiver of that right or remedy. No waiver shall be effective unless it is communicated expressly to the other party in writing. A waiver of any right or remedy arising from a breach of contract shall not constitute a waiver of any right or remedy arising from any other breach of the Contract.

22. The parties acknowledge that the Authority shall be entitled (without prejudice to this SAL or any claim for damages) to apply for and obtain injunctive or equitable relief in respect of any actual or threatened breach of this SAL.

23. If changes to the information security requirements emerge during the performance of the Contract, the Contract or this SAL may be amended or terminated.

24. If the Contractor has any difficulty in interpreting the meaning of this SAL and/or its Schedules or in safeguarding the Authority's security Classified assets in accordance with it, the Contractor should contact the Authority's representative immediately who will work collaboratively and in good faith with the Contractor to agree a solution.

Signed for and on behalf of the **AUTHORITY**

Signature:

Name:

Position:

Date:

We acknowledge receipt of and our agreement to the Security Aspects Letter and its Schedules.
Signed for and on behalf of the **CONTRACTOR**

Signature:

Name:

Position:

Date:

SCHEDULE 1
Contract Specific: Information Classification Table

Description of Information	Classification
The existence of the Contract.	
Association of the Contract with Houses of Parliament.	
Information relating to any subcontractor's involvement in the Contract.	
Employee Contact Information that is openly commercially available.	
Subcontracting documentation issued by Houses of Parliament.	
Any correspondence, response or query relating only to commercial aspects of subcontracting.	
Any correspondence, response or query relating to technical aspects of the services to be provided, as described in the subcontract.	
Any correspondence, response or query relating to technical aspects of the services to be provided based on information gleaned from Houses of Parliament.	
Completed forms relating to Security Clearance	
Any document that relates only to the subcontractor's own facilities, corporate IT environment etc.	
Any document the bidder creates forming part of their response to this subcontract.	
Unrestricted	
Restricted	
Highly Restricted	
Parliament Secret	

SCHEDULE 2 TO SECURITY ASPECTS LETTER
Parliamentary Protective Marking Scheme (PPMS)

Parliamentary Protective Marking Scheme – Strategic Estates & Programmes

UK Parliament

	Unrestricted	Restricted	Highly Restricted	Parliament Secret (PS)
Definition	Information that is easily accessible by staff across Parliament. Unmarked information is considered **Unrestricted**	Information that needs controls on access and handling. A **Restricted** marking is a signal to staff to use discretion. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. **Note:** The aggregation of Restricted information should also be considered i.e., sometimes more than two Restricted documents together *may* require them to be classified as **Highly Restricted**.	**Highly Restricted** information needs strict, managed access controls. This marking should be used to identify highly sensitive information related to personal data, commercial' and security information that can be held on the Parliamentary network. **Note:** The aggregation of Highly Restricted information should also be considered i.e., more than two Highly Restricted documents together *may* require them to be classified as **Secret**.	Parliament Secret is information of a highly sensitive nature. It needs the highest level of protection available in Parliament. This marking should not be used or stored on Parliament's network (e.g., SharePoint, Outlook email, Aconex or our HR, finance, or other databases). **Note:** Most staff will not use this marking
Sharing and Access	• Open permissions (internally) are encouraged for Parl staff. Please refer to Information Sharing Model • Please refer to the External Sharing Principles and/or the External Sharing Guidance for more details • Sending information via links is best practice. Please refrain, where possible, from sending attachments Some **Unrestricted** information may be appropriate for public release and sharing but the default position is that any Parliamentary documents should not be shared beyond the work environment	• Restricted information has a select audience such as a project team, chosen individuals or groups • It is not created to actively share with the public • This information can be shared externally if there is a business need and these handling instructions are followed For Parliament staff please refer to the External Sharing Principles and/or the External Sharing Guidance for more details For external suppliers please refer to the Client's Information Requirements, Standards, Methods, and Procedures	• Sharing of Highly Restricted information is limited to individuals on a need-to-know basis • It is not created to actively share with the public and should only be shared externally with the consent of the Information Asset Owner and these handling instructions are followed Please refer to the External Sharing Principles and/or the External Sharing Guidance for more details For external suppliers please refer to the Client's Information Requirements, Standards, Methods, and Procedures	Parliament Secret information must **NOT** be shared from Parliament's network or any digital commercial network **Note:** If you believe that you have created, need to create or are in possession of any PS content, please contact eimteam@parliament.uk.
Examples	• **Internal training syllabuses** • Floor plans displaying publicly known locations • Association of the Contract with HoP • Job descriptions/ roles and responsibilities • Heritage Collections data* • Some designs (intended)* • Retention schedule • Guidance • Standards and Policies (published) • FOI responses • Comms/marketing • Academic outputs • Publicly available specifications adhered to by Parliament, eg: PAS/BS/ISOs – BIM19650 Standards * You may need to check with your Information Asset Owner (IAO) first as these are not always unrestricted	• **Resourcing** Documentation ○ Recruitment docs • **Designs** and Design Reports ○ technical aspects of the services to be provided, as described in the subcontract • Contractual and commercial **communications including** ○ Information relating to suppliers' involvement ○ Subcontracting documentation ○ Documents that relate only to the subcontractor's own facilities, corporate IT environment etc. ○ Any document the bidder creates forming part of their response to subcontracts Procurement information e.g. tenders • Other ○ **Standards**, Policies, and/ or Strategies (Unpublished) eg: BIM Information Requirements and Standards – only released for tendering ○ Minutes* ○ Process **documentation** ○ Information Asset Registers ○ Asbestos information ○ Managem ○ O & M ma	• Secondary Distribution Points (SDPs) • HR information that refers to Grievances, Bullying and Harassment, Medical referrals • Legal advice e.g., an employment dispute or advice from Speakers Counsel or on contracts • Completed pass applications • Floorplans revealing sensitive locations on the Parliamentary Estate and/ or operational control point locations, systems and connectivity including server rooms and Building Management Systems (BMS), Security Equipment Rooms (SER) and Pass Offices • Detailed asset designs including metadata on security functions (such as CCTV / Access control sensor locations, fabric and Safety & Security Systems) • Business Continuity Plans • Health & Safety – Near Miss and Incident reporting • Schematic plan of a location • Personnel management systems with locations and movements of Parliamentary personnel, including detailed preparations for VIP visits, • Maintenance systems with information on assets or level of support containing security information	• Detailed plans for sensitive security operations • Documents which would significantly increase the risk of harm or the bypassing of Parliamentary security measures • Network design architecture (if protective controls are breached) e.g., for broadcast, engineering, infrastructure etc • Occupancy and floorplans information / location e.g., Prime Minister or Cabinet Members' Offices • Personnel & Physical Security Audits which may contain highly sensitive personal info and/or Physical Security reviews • Security asset and functional information on drawings, specification, reports, schedules, diagrams, schematics, COBie and 3D Models etc • Technical details and detailed schematics of Security Projects • O&M Manuals containing security information • Degree of connectivity of building systems to systems (such as Building Management System - BMS) • Details of Mechanical, Electrical and Plumbing for Proprietary Plant and Equipment (such as facility locations, utility management points, system vulnerabilities) • Space IDs when associated with system functions,

1 / 2

	Unrestricted	Restricted	Highly Restricted	Parliament Secret (PS)
		information ○ Timesheets * Check with your Information Asset Owner (IAO) as some items (including meeting minutes) may vary in protective marking	• Completed Business Cases • Risk registers • Evacuation areas and routes • Survey information with photographs and details of sensitive locations (such as server room, security functions)	organisational roles, or personnel • Information about location of IT servers and systems, data centres and data cabling
Impact if information compromised	• Minor, short-term disruption or loss of confidence to a service, individual, or team • Minor embarrassment to an individual, service or project only • No risk to any party's personal safety	• Distress, minor reputational damage, or embarrassment to an individual, team, service, or the Administration(s) • Minor, short-term disruption to critical business platforms or systems • Minor breach of contractual obligations with some damage to working relationships • Minor financial losses or penalties for Parliament, a client or a third party • Disruption of current or future commercial operations for the Administration(s) or a third party	• Severe distress and damage to an individual and the Administration(s) • Disruption to the workings of Parliament including digital services and physical Estate restrictions over a long period of time which could lead to a loss of confidence in Parliament as an institution • Assist in the planning of a crime or obstruct investigations • Significant breach of contractual obligations leading to potential legal action • Significant financial losses or penalties for Parliament, a client or a third party • Shut down or otherwise substantially disrupt significant Parliament operations, or seriously impede the development or operation of Parliament policies.	• Significant disruption to the workings of Parliament over a long period of time which could lead to a loss of confidence in Parliament as an institution • Endanger individuals, Parliamentary assets, property, or the security of the Parliamentary Estate • Assist in the planning of a crime or obstruct investigations
Handling – SharePoint and email (Office365)	**Documents and email** • Share **internally** using links instead of attachments. • Hold in a SharePoint site or library that is open to all staff in Parliament. • Unmarked information in Office365 will default to **Unrestricted**. **Email** Always check before emailing information externally. Not all **Unrestricted** information is open to the public.	**Documents and email** • Share **internally** using links instead of attachments. • Hold in a closed SharePoint site or library that is visible to members of an Office, group or network. **Email** • Check the distribution list of emails you send and receive. • Challenge the marking if you do not agree. Add if it is unmarked. • Share only with work email addresses and do not share information with freeware (Gmail, Hotmail, etc.) accounts	**Documents and email** • Share **internally** using links instead of attachments. • Hold in a closed SharePoint site or library that is visible to a small, select audience. Such as closed programmes working on security operations or sensitive Committee groups. • Maintain a register of those with access and review regularly. **Email** • Check the distribution list of emails you send and receive. • Challenge the marking if you do not agree. • Share only with work email addresses and do not share information with freeware (Gmail, Hotmail, etc.) accounts	Parliament Secret information requires the highest level of protection available in Parliament. This marking should not be used or stored on Parliament's network (e.g., SharePoint, Outlook email, Aconex or our HR, finance or other databases). Note: If you believe that you have created, need to create or are in possession of any PS content, please contact eimteam@parliament.uk.
Handling - Hardcopy	Unmarked information is considered **Unrestricted**. **Unrestricted** information does not normally require a marking. Information such as posters and newsletters do not need a marking. Unrestricted markings do not need to be applied when shared externally.	The marking to be displayed in the header of the document and the front cover of the paper file. Lock away **Restricted** information when it is not in use.	The marking to be displayed in the header of the document and the front cover of the paper file. Information containing **Highly Restricted** information should be locked away while not in use. Access to the storage must be regularly reviewed and updated.	Parliament Secret information can currently only be held in hard copy and strict guidelines are in place for handling, disposal and sharing. Please familiarise yourself with these guidelines if you are working at this tier.

Other platforms, formats, and media

Strategic Estates and Programmes work across several platforms and formats e.g. CAD drawings, video, images, modelling etc. The format of a document does not determine its marking e.g. not all CAD drawings are considered Highly Restricted. It is still the information or content of the document that determines the marking. Please refer to the table above or the Quick Reference Guide to help you choose the appropriate marking. Specific instructions and guidance for marking databases and platforms will be prepared and shared in due course.

EIM; PSD; IRMS - August 2023

SCHEDULE 3 TO SECURITY ASPECTS LETTER
Detailed Information Security Assessment Template (DISA)

Detailed Information Security Assessment (DISA)

High Level Security Principles

1. We require that any of Parliament's information that you gain access to, while delivering services, will be protected appropriately.
2. We require written assertions, and where possible, evidence, that appropriate information security measures are in place for Parliamentary information that is to be stored, processed, and managed on your internal company systems, or that there are suitable commercial obligations with a subcontractor or a 3rd party company such as cloud providers/Common Data Environments (CDEs).
3. The scope comprises the personnel, procedures, IT systems and devices used to deliver the services:
    - If you are the prime contractor (referred to in ISO 19650 as "*Lead Appointed Party*"), we expect that you will be responsible for notifying Parliament of all subcontractors or 3rd party companies (referred to in ISO 19650 as "*Appointed Party organisations*") are to be involved in service delivery and would have access to Parliament's data;

You will be responsible for the security of any our information that you pass to other companies and should have a commercial process in place to demonstrate effective management of the risks and the flow down of security obligations to subcontractors with access to Parliamentary data.

Guidance

To assist with effectively answering the questions listed in the Detailed Information Security Assessment (DISA) (formerly known as the Information Security Management Plan - ISMP) additional guidance has been included that should be referred to in your response.

- "Points to consider" highlight some examples of what a good response should include.
    - For example, providing a copy of a corporate policy which sets out the security controls to be applied; and/or
    - where an appropriate third party has audited the internal process to confirm compliance.
- The National Cyber Security Centre (NCSC) provides advice and support for the public and private sector in how to avoid computer security threats, and these are included here too where relevant.
- The NCSC glossary - a set of straightforward definitions for common cyber security terms – see link here.

Document History

Version	Status	Date of Update or Approved	Author	Approved By	Summary of Change
1.0	Final	21/12/2022	Information Management Security Integrity Coordinator & Parliamentary Accreditor	Parliamentary Accreditor	Name Change; Alignment with ISA (formerly NFSR) & PSMP (formerly BASIR)

All sections must be completed by the nominated individual who handles information security for, or on behalf of, your organisation.

Please note that 'Points to consider' offer suggestions on how to successfully respond to each section.

The Appendix Inventory is important to assist Parliament with monitoring and compliance.

Revision History (Contractor to complete)

Version Number	Date Approved	Approved By	Brief Description

1.	**Overview** Identify and list any current information security **certifications**.	
1.1.	**Certification examples (not exhaustive) include evidence of at least one of the following:** • Cyber Essentials as a minimum • Cyber Essentials PLUS - preferrable • ISO/IEC 27001 • SSAE-16 with SOC 2 report made available • PCI DSS plus appropriate SAQ • Information Assurance for Small & Medium Enterprises (IASME) **Respondent's must attach the relevant certifications to provide independently assured, against a recognised industry standard, evidence of the effective implementation of security controls being used to deliver the service to Parliament.** **In addition, you must provide a written assertion from any subcontractors processing Parliament information have been assured under the commercial arrangements.** **Company Security Policy can also be included to compliment examples above.**	
1.2.	**Respondent's must provide an identified, and named:** • **Board representative (or a person with the direct delegated authority)** **who is responsible for:** • **(information) security management for your organization and that of the subcontractors?** Provide name, role, and contact details.	
1.3	**Information Systems:** **Outline the solutions you will use to process and store Parliamentary information**	

	Points to consider: • Any SaaS (eg: O365) used by main contractor • The functions of the SaaS and the associated security aspects of that function • SaaS provider has external security certification and published security compliance documentation (See PSMP section 10.3.1 & 10.3.2 for more details)	
2.	**Subcontractor Information Management** If Parliamentary information were to be passed to subcontractors during the delivery of services, describe how information security will be managed across the supply chain *(See PSMP section 10.4.10 for more details)*	
2.1.	**Information Security Management across Supply Chain:** **Respondent's must provide a written assertion on how they ensure any Subcontractor processing Parliamentary information shall comply with requirements set out in the commercial agreement.** Points to consider: • Have key subcontractors completed ISA? • Written statement of assertion of contractual compliance for each subcontractor • Does the process include checks on their information security competence such as relevant certifications? • Supplier Security Assessment Questionnaire (provide as evidence)	
2.2.	**Subcontractor security requirements** **Describe how your security requirements will be covered and monitored in arrangements with subcontractors.** Points to consider: • Summarize how Parliamentary information will be managed down the supply chain	

	• Details of how Parliamentary information will be handled down the supply chain?	
2.3.	**Demonstrate how secure sharing of Parliamentary information complies with Parliament's External Sharing Principles for all suppliers, with a particular emphasis on sharing with sub-contractors.** Points to consider: • Secure File Transfer Protocols • Common Data Environment? • Other mechanisms (e.g. SharePoint, email etc.) • Assertion of testing of external sharing solution on annual basis	
3.	**Company Technical Security Measures** The following areas must be answered fully including providing relevant **evidence.** *(See PSMP section 10.3 for more details)*	
3.1.	**Describe the Protective Monitoring you have in place to protect IT systems from threats and describe how is this managed.** Points to consider: • Outline how digital service(s) are monitored • The management processes in place to provide alerts and reports • Key security enforcing components e.g. Firewalls • Comprehensive event generation across all security relevant devices/components • Centralised service which automatically correlation events • Relevant section of company Security Policy can also be included to compliment examples above. *(See PSMP section 10.3.5 for more details)*	
3.2.	**Network systems scanned for vulnerabilities**	

	Describe and provide a written assertion: • How security vulnerabilities on internal infrastructure are undertaken, and • That there are commercial obligations in place for any subcontractor processing Parliamentary information to have suitable commercial obligations to performs this action. <u>Points to consider:</u> • Outline how scanning for vulnerabilities is performed and frequency e.g. deployment of industry recognised scanning tool • Sub-contractors are required to implement vulnerability scanning tool • Automatic (non-human) processes in place to update signature (vulnerability patterns) updates to vulnerability tools • Details/certs of who performs testing (internal/external) • Relevant section of Company Security Policy can also be included to compliment examples above *(See PSMP section 10.3.3 for more details)*	
3.3.	**Describe what mechanisms you have in place to manage risks from <u>malware</u> in communications and on all IT systems?** <u>Points to consider:</u> • Use/deployment of anti-virus protection • Malware protection of mobile devices • Details of (potential) mechanisms, eg: Intrusion Prevention Systems (IPS) or Deep Packet Inspection (DPI) • Relevant section of company Security Policy can also be included to compliment examples above *(See PSMP section 10.3.3 for more details)*	

3.4.	**Respondent's must provide a written assertion that all internal and external transfer of information is protected using encryption or other technical control providing a similar level of protection.** **Where information is transmitted over public network the Supplier must encrypt the data using the TLS1.2 or a later version or other comparable and established cryptographic protocol.** Points to consider: • Outline how all databases holding Parliamentary information are encrypted • NCSC recommended encryption (AES 256) • External communications are encrypted (eg: ○ TSL1.2; ○ SFTP – Secure File Transfer Protocol) • Components used to encrypt in transit are externally certified or have been peer reviewed • Relevant section of company Security Policy can also be included to compliment examples above *(See PSMP section 10.3.4 & 10.3.7 for more details)*	
3.5.	**Describe the data encryption (ie: data at rest) on your systems.** Points to consider: • NCSC recommended encryption (AES 256) • Components used to encrypt at rest are externally certified or have been peer reviewed • Relevant section of company Security Policy can also be included to compliment examples above *(See PSMP section 10.3.4 & 10.3.7 for more details)*	
3.6.	**Outline your Mobile Device Management (MDM) process and where applicable include your Bring Your Own Device (BOYD).** Points to consider:	

	• Is BYOD permitted? • Mobile application management (MAM) outline • Do laptops have full disk encryption? • Application of NCSC mobile device guidance • Relevant section of company Security Policy can also be included to compliment examples above	
3.7.	**Describe how IT systems (operating systems and applications) are <u>patched</u> and updated.** <u>Points to consider:</u> • Policy around patching/patch testing? Highlighting prioritising patches according to criticality • Outline of patching process including automatic deployment of patching to all devices • How quickly are security patches applied? • Are updates and patches tested prior to deployment? • Defined SLA with SaaS or subcontractors for patching services • Relevant section of company Security Policy can also be included to compliment examples above *(See PSMP section 10.3.10 for more details)*	
3.8.	**Respondent's must provide a written assertion of robust User authentication to any services which must use at least two independent factors to verify a user's identity** <u>Points to consider:</u> • Details of 2FA/MFA for access to all systems storing Parliamentary data • Password complexity defined • Relevant section of company Security Policy can also be included to compliment examples above *(See PSMP section 10.2.2 & 10.3.7 for more details)*	

3.9.	**Respondent must provide a written assertion on how <u>access is controlled to Parliamentary Information</u> by only authorized personnel.** <u>Points to consider:</u> • Configurable technical controls to be used to manage access to project data on a 'need to know' basis • How is account management conducted? • Is the principle of least privilege employed for user accounts? • User access managed and revoked through joiners, movers, and leavers (JML) package • Relevant section of company Security Policy can also be included to compliment examples above *(See PSMP section 10.2.2 & 10.3.7 for more details)*	
3.10.	**Data backup:** Details of data backup procedure being used to provide offsite storage. <u>Points to consider:</u> • How data is extracted and transported to offsite location • Timelines – periodicity of often data is extracted (backed up) • In-built geographic resilience of the data back-up storage • Relevant section of company Security Policy can also be included to compliment examples above *(See PSMP section 10.3.6 for more details)*	
4	**Physical Security** This section cover how Parliamentary data will be protected at your and subcontractors' locations such as offices and work sites. For physical locations in scope briefly describe the **<u>measures in place to control and manage access</u>** to offices (including visitors) and to sensitive areas (server rooms*). (See PSMP section 10.5 for more details)*	

4.1	**Respondent's must provide a written assertion of how they comply with the HMG physical security requirements** **https://www.gov.uk/government/publications/crowded-places-guidance/physical-security.** Points to consider: • Site and building barriers to include how keys are managed; • CCTV and alarms; • Guard force; • Protection for sensitive areas (e.g. plant and IT equipment rooms). • Process for managing visitor access to your locations • Access Controlled entry • Building reception • Relevant section of company Policy can also be included to compliment examples above	
5	**Personnel Security** This section covers the security measures in place to **identify and verify staff**. NOTE: Those personnel with direct and frequent unsupervised access to Parliamentary data will be expected to hold Parliamentary security clearance, even if a site access pass is not required. *(See PSMP section 10.2 for more details)*	
5.1	**Summarise or provide a written assertion of your Staff identification/Verification process;** Points to consider: ➢ Does this include checking the identity, right to work and references of staff and subcontractors? ➢ Statement on roles requiring enhanced clearances (eg: CTC) ➢ Relevant section of company Policy can also be included to compliment examples above *(See PSMP section 10.2.1 for more details)*	

5.2	**What standard does your policy conform to?** (E.g.: BS 7858 or the Government Baseline Personnel Security Standard) *(See PSMP section 10.2.1 for more details)*	
5.3	**Outline any staff training on information security awareness and its regularity.** Points to consider: • Security awareness training including details of training process for staff regarding information security and information management • Social Media Policy and staff awareness of the risks of social media • Relevant section of company Policy can also be included to compliment examples above *(See PSMP section 10.2.4 for more details)*	
6	**Business Continuity** Describe what measures relevant to the contract are in place for **incident management, disaster recovery and business continuity**. *(See PSMP section 10.3.10 & 10.3.11 for more details)*	
6.1	**Respondent's must provide a written assertion that there is a robust Business Continuity and Resilience policy in place which protects against:** • **a cyber and physical compromise and** • **which has been tested in the last 12 months** **Briefly describe the key features.**	
6.2	**Respondent's must provide a written assertion that they have an approved incident management policy and briefly describe the key features** Points to consider: ➢ Do you **test** your own business continuity policies?	
6.3	**Where the service is going to process personnel Parliamentary information, Respondent's must provide a**	

	written assertion that relevant Data Protection Polices and Privacy Notices are in place?	
6.4	**Respondent's must provide a written assertion that <u>Data storage</u> is hosted in a location which is within the EEA?** Points to consider • Provide Certificates for any data centres used • Relevant section of company Policy can also be included (Preference for data held in UK data centres; for more sensitive data)	
7	**Data Return and Retention** At the end of a contract/s you will be expected to **<u>return or securely delete the data and information</u>** used to deliver the contract/s. If you require to retain any material for insurance or legal reasons this must be agreed with Parliament. *(See PSMP section 8.1.3 for more details)*	
7.1	**<u>Retention and Disposal:</u>** **Respondent's must provide a written assertion that confirms the return of Parliamentary data upon project completion:** <u>Points to consider:</u> ➢ Identify what tools / process are used to return data ➢ Identify how this will be applied to subcontractors ➢ Relevant section of company Policy can also be included to compliment examples above	
7.2	**Respondent's must provide a written assertion that confirms the secure disposal of Parliamentary data upon project completion:** <u>Points to consider:</u> • Details and evidence of policy around management and/or disposal of Parliamentary data upon project completion	

	• Identify what tools / process are used to destroy data • Identify how this will be applied to subcontractors	
7.3	**Retention of Parliamentary data:** **What types and what volume of data will be retained, why (i.e. Limitation Act 1980) and for how long?** <u>Points to consider:</u> • Details of legal/regulatory reasons why Parliamentary data is retained • What types and what volume of data will be retained? • Secure destruction policy?	

Appendix - Inventory:

Systems & Applications (and Software)

List all Systems, Applications and key Software to be used by the contractor, and where possible, by sub-contractors during the lifecycle of the contract

Corporate Evidence

List all **approved policies and corporate documents** used in evidence to support all contractor assertions made completing the DISA and include **'Review/Renew Date'.**

Document Title	'Review/Renew Date'

Strategic Estates

Parliamentary Security Management Plan (PSMP)

00ESW-XXXX-HOP-99-XX-K-XX-DO-00003 P01

PM_80_10_79 : Security Management Plan

Estates Information Management (EIM) team

1. Executive Summary

The Parliamentary Security Management Plan (PSMP) outlines the information security framework that Strategic Estates will apply to protect its systems and information from threats.

The purpose of the PSMP is to identify and assess the risks that Strategic Estates faces, and to advise on controls to mitigate those risks. This can involve a range of measures, such as installing security systems, establishing security policies and procedures, training employees on security protocols, and conducting regular security assessments.

The intended audience for the PSMP is all Strategic staff and all Lead Appointed Parties or Appointed Party organisations (Suppliers) who are implementing works and services for Parliament.

Principles-Based Assurance

The PSMP is a principles-based assurance (PBA) document. Principles-based assurance refers to an approach to derive assurance by focusing on the underlying principles and objectives of the information security framework, rather than on specific rules and guidelines. The goal of PBA is to assist Lead Appointed Parties or Appointed Party organisations (Suppliers) to provide assurance that they can securely and competently handle and manage Parliament's information, whilst offering a professional service to Parliament.

In contrast to a rules-based approach, which relies on strict adherence to specific rules and guidelines, a principles-based approach allows for more flexibility and judgment in the assurance process. This approach is based on the idea that the principles underlying the information security framework are more important than the specific rules and guidelines.

The PSMP principles are listed in *Appendix B - Information Risk Management Principles performance indicators*.

Security Considerations

The PSMP principles also form the basis for *Section 10 – Security Considerations*. For Strategic Estates' projects and programmes these security considerations will be adhered to by all roles – internal staff and external contractors - to ensure that Parliamentary information is protected and secure, at all Royal Institute of British Architects (RIBA) Plan of Work stages.

The PSMP provides guidance to Parliamentary works services programmes and supply chain partners on the information security measures required when delivering a refurbishment work package on the Parliamentary estate.

The security considerations and the principles within them cover all aspects of security: personnel, process, physical, and technical.

2. Table of Contents

2.1. Table of Figures

3. Introduction

3.1.1 The Parliamentary Security Management Plan (PSMP) is part of the portfolio of documents that support Parliament's implementation of the standard(s) for information security within Strategic Estates (SE).

3.1.2 Conceived originally from PAS1192 and BS EN ISO 19650[1] Building Information Management (BIM) maturity Level 2 regulatory standards, the PSMP has broadened its scope to include all aspects of information security within SE. This includes projects delivered in BIM environments and those delivered outside BIM environments. This also includes pre-contract work (e.g.: Feasibility studies).

3.1.3 In line with BIM standards, this document was previously entitled the *Built Asset Security Information Requirements* (BASIR). The term BASIR has been withdrawn in BS EN ISO 19650-5 and replaced with *Security Management Plan*.

3.1.4 The current policy structure is based on the *Centre for the Protection of National Infrastructure* (CPNI)[2] Security Considerations Assessment (SCA) process which ensures security-related vulnerabilities are considered across a range of activities and processes within an organisation. This includes physical, personnel, technical and process security measures.

3.1.5 It also builds on the CPNI's guidance document *Ongoing operation, management, and maintenance of an existing built asset (including buildings and infrastructure)* as well as PAS1192 BIM Level 2 and BS EN ISO 19650 Building Information Management (BIM) maturity regulatory standards.

3.1.6 The PSMP sits strategically within Parliament's Information Security Accreditation Process. The process of accreditation within both Houses of Parliament provides Parliament's Information Authority[3] with assurance that technical solutions, storing or processing Parliamentary data, are meeting appropriate security standards.

3.1.7 The PSMP principles align with the four key Information Risk Management Principles as set out in Parliament's Bicameral Risk Appetite Statement.

- Physical
- Personnel
- Technical
- Process

3.1.8 The PSMP is part of the contract documentation provided to Lead Appointed Parties or Appointed Party organisations (Suppliers) implementing works and services for Parliament, so they are aware of their information security obligations[4].

---

[1] The ISO 19650 standard is an international standard for managing information over the whole life cycle of a built asset using building information modelling (BIM). It contains all the same principles and high-level requirements as UK BIM Framework and is closely aligned with the current UK 1192 standards.

[2] CPNI protects national security by providing advice to the organisations that make up the UK's national infrastructure covering physical, personnel and cyber security.

[3] The Information Authority is a sub-committee of the House of Commons Executive Board and the House of Lords Management Board. Its objective is to deliver increased benefits from Parliamentary information for members of both Houses, staff and the public, while containing the risk of inappropriate access to that information. The Information Authority provides a focus for informed decision making about the effective management and security of our information.

[4] For more details, please refer to 13.5 "1192 Series General Terms relationship to BSEN ISO19650"

- Until late 2022, at the time of writing this document, the documentation used by Strategic Estates (Parliament) in the supplier due diligence process had different titles and layout.
- These changes were part of an update on each document to ensure that Parliament gets relevant assurances that its information is managed securely, protected adequately, and shared appropriately with those who need it while fulfilling any contractual obligations
-

Previous Title	New Title
NFSR – Non-Functional Security Requirements	ISA - Information Security Assessment
ISMP - Information Security Management Plan	DISA - Detailed Information Security Assessment

Figure 1 – Due Diligence Document Title Changes

- The title ISA follows the wording in section 6.2 "Assessing the security risks" of 19650-5. The DISA naturally follows sequentially from the ISA as it looks for greater detail
- The ISA allows respondents to answer 'Yes' or 'No' (or where applicable 'N/A') to broadly assert their technical infrastructure without providing evidence to support their claims at this stage.
- The DISA requires written assertions, and where possible, evidence, that appropriate information security measures are in place for Parliamentary information that is to be stored, processed, and managed on external company systems, or that there are suitable commercial obligations with a subcontractor or a 3rd party company such as Software as a Service (SaaS) providers/Common Data Environments (CDEs).

3.1.9 For BIM projects the PSMP requirements are reflected in the Appointing Parties Employer's Information Requirements (EIR) which underpin NEC3/NEC4[5] and BS EN ISO 19650-2 BIM Information Protocol contracts.

3.1.10 The PSMP is relevant to all roles and individuals within Strategic Estates (SE) that generate, handle, manage or process Parliamentary information. This includes (but is not limited to) Parliamentary and supplier roles from Lead or Appointed Party, Project Managers, Designers, Specialist Designers, Cost Consultants, Logistics, external organisations (such as local planning dept), Contractors, Sub-contractors, Suppliers and Manufacturers, who provide services to Parliament through construction, new works, refurbishment, and maintenance contracts.

3.1.11 The aim of the PSMP is to define the information and security requirements that shall be followed by all roles to ensure that sensitive Parliamentary information is protected and secure. For projects delivered in a BIM environment, this applies to all Royal Institute of British Architects (RIBA) Plan of Work stages[6].

3.1.12 The PSMP provides guidance to Parliamentary works services programmes and supply chain partners on the information security measures required when delivering refurbishment and other work packages on the Parliamentary estate. It is an interpretation of existing policy and good practice covering all aspects of security, including personnel, procedural, physical, and technical.

---

[5] The New Engineering Contract (NEC), or NEC Engineering and Construction Contract, is a formalised system created by the UK Institution of Civil Engineers that guides the drafting of documents on civil engineering, construction and maintenance projects for the purpose of obtaining tenders, awarding and administering contracts

[6] The RIBA Plan of Work organises the process of briefing, designing, constructing and operating building projects into eight stages and explains the stage outcomes, core tasks and information exchanges required at each stage.

3.1.13 The PSMP, where applicable, uses industry standard terminology taken from the CPNI, the National Cyber Security Centre (NCSC)[7], as well as PAS1192 BIM Level 2 and BS EN ISO 19650 Building Information Management (BIM) maturity regulatory standards.

3.1.14 The Uniclass code[8] for this document is *PM_80_10_79 : Security Management Plan*.

3.1.15 This document is *unmarked* therefore denoting an 'Unrestricted' Protective Marking.

4. Scope

4.1.1 The PSMP is owned by Strategic Estates (SE) and is applicable to all SE programmes and projects. It is also directly relevant to estate infrastructure maintenance activities.

4.1.2 This policy is also applicable to third-party solution or service providers which process, host, manage or create Parliament protectively marked information.

4.1.3 Should there be any conflict between this policy, other Parliamentary policies/standards or other referenced documents, the most stringent requirement shall be applied unless otherwise agreed. Identified conflicts will be raised with the appropriate Project Manager or Senior Project Lead, and an appropriate approach agreed.

4.1.4 Any words following the terms "including", "include", "in particular" or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase, or term preceding those terms.

4.1.5 All relevant Codes of Practice, Standards, Regulations, and local Building Codes, together with relevant Statutory Rules, Regulations, Byelaws, and other applicable enforceable instruments shall be complied with.

4.1.6 This policy must not be altered in any way without prior written agreement of the owner.

5. Principles

5.1.1 The PSMP is a principles-based assurance (PBA) document. Principles-based assurance refers to an approach to derive assurance by focusing on the underlying principles and objectives of the information security framework, rather than on specific rules and guidelines.

5.1.2 Collaborative digital work methods and technologies generally involve the collaborative sharing of information across a broad range of independent organisations, especially within the built environment sector.

5.1.3 Parliament requires the adoption of principles and requirements for the security-minded management of protectively marked information prior to a solution/service processing, storing, or accessing of Parliament's protectively marked information.

5.1.4 The implementation of the Confidentiality, Integrity, and Availability (CIA) principles helps to ensure that Parliament's systems/applications and data/information are not compromised in any way when critical issues arise.

---

[7] The NCSC is an organisation of the United Kingdom Government that provides advice and support for the public and private sector in how to avoid computer security threats. Its parent organisation is GCHQ.

[8] Uniclass 2015 is a unified classification system for all sectors of the UK construction industry. Uniclass is a way to organize everything required for built environment assets and provide a logical code for each general item, which can be used by anyone to identify and refer to it.

5.1.5 To do this, the PSMP will align with the following four key Information Security Risk Management Principles as set out in Accreditation Standard[9] that forms part of Parliament's Bicameral Risk Appetite Statement:

- Principle 1: Govern

  Identifying and managing information risks during all phases of lifecycle. Solution Owners must develop an understanding of the threats and vulnerabilities to manage information risk to systems, assets, data, and capabilities.

- Principle 2: Protect

  Assurance of the implementation of security controls to reduce risks. Solution/Service Owners must develop and implement the appropriate safeguards or controls to limit or contain the impact of a potential information security event. This principle will ensure that solutions are assured against Parliament's cyber security standards, controls and policies and information management controls and policies

- Principle 3: Detect

  Assurance of the ability to detect and understand information security events. Solution/Service Owners must implement the appropriate measures to quickly identify information security events.

- Principle 4: Respond

  Assurance of the ability to respond to and recover from information security incidents. Solution/Service Owners must develop and implement effective activities to restore any capabilities or services that were impaired due to an information security event.

In support of handling information (and assuring solutions) against these Principles a set of performance indicators have been developed to inform the assurance process (see Appendix B) and form the basis of the expected outcomes for the security considerations in Section 11 below.

6. Information Management - Legal & Commercial Considerations

6.1.1 All Lead Appointed Parties or Appointed Party organisations (Suppliers) shall only use project information produced under the permitted purpose as set out in the contractual obligations.

6.1.2 Information obligations should be devised and implemented for supply chains' contractual agreements to understand and flow down their legal and commercial responsibilities for information sharing within a supply chain.

6.1.3 An example of an information protocol in existence for BS EN ISO19650 projects is the "*Information protocol to support BS EN ISO 19650-2 the delivery phase of assets*".

6.1.4 Another example is the *NEC4 Secondary Clause X10 Particulars* for all projects. X10 has been designed to inject information management and BIM particulars into contracts. X10

[9] The Accreditation Standard lends heavily from the Australian Cyber Security Centre (ACSC) 'Information Security Manual' (ISM). The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and data from cyber threats.

needs to reference the key documents to support the information management clauses written for the project. X10 is optional so may not be included in every contract currently.

6.1.5 BS EN ISO 19650-2 Information Protocol references the legal, commercial, security, supply chain responsibilities and information management standards for the built environment to be provided with new engineer contracts. The Information protocol references the need for a Security Management Plan (SMP) document. If no such plan/document exists, then the secondary clause X10 can be used to introduce specific clauses for NEC contracts.

7. Parliamentary Protective Marking Scheme (PPMS)

7.1.1 Protective marking schemes are designed to assist staff in determining the level of protection required when creating, sharing, and re-using information. They include any special handling that is required and appropriate to the relevant marking.

7.1.2 Adding protective markings is the method employed by the originator of information which indicates to others the levels of protection required when handling the information in question, in terms of its sensitivity, security, storage, movement both within and outside an organisation (Parliament) and its ultimate method of disposal.

7.1.3 The protective marking scheme applies to all staff, contractors, and all others who work or volunteer for the Parliamentary Administrations. It applies to whomever uses Parliamentary information in the course of their work or volunteering.

7.1.4 Use of a protective marking does not prevent disclosure under the Freedom of Information Act.

7.2. The Markings

7.2.1 Parliament's protective marking scheme has four tiers that reflect the range of sensitivities in its information. The markings are:

Figure 2 - PPMS (Parliamentary Protective Marking Scheme)

7.2.2 Examples for each protective marking for Strategic Estates can be found in Appendix C.

7.2.3 Parliament requests that where possible, descriptors are to be used to accompany the markings. Descriptors should not be used for Unrestricted information. The use of descriptors to accompany your marking is intended to provide an indication of the type of information contained.

7.2.4 Parliament has a set of approved descriptors that may be applied in conjunction with Restricted and Highly Restricted. Descriptors should not be used for Unrestricted information.

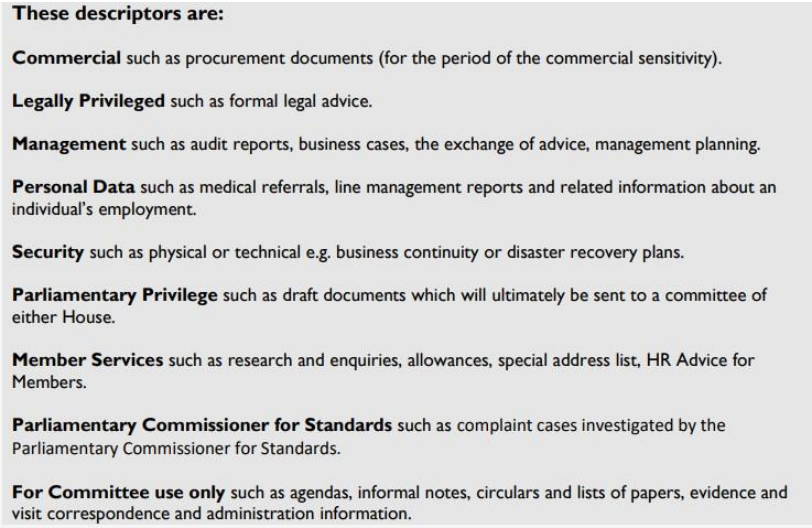

Figure 3 - PPMS Descriptors

7.2.5 The PPMS user guide for Strategic Estates – entitled PPMS Guidance - SE Sch2 - SAL V2.0 (internal link only) – is included with the Invitation to Tender (ITT) package. It offers some practical examples to users for applying protective markings.

7.2.6 For Parliamentary staff who manage sensitive or security-related projects, or require more information, please seek additional advice from Estates Information Management (EIM) Team.

7.3. Comparisons with the Government protective marking scheme

7.3.1 Prior to the approval of the protective markings, work was completed to assess whether the Government scheme would be appropriate for Parliament.

7.3.2 For the following reasons it was decided that Parliament should have its own marking scheme:

- The Government scheme is the 'property of HMG' and applies to their information assets. This denotes ownership and would not have allowed the flexibility in application we require for Parliament.
- Requirements from the organisation were clear and steered our decision to create a four-tier scheme.
- The government scheme would require significant adaptation to work in Parliament, as it does not provide the level of granularity required.

Note: An assessment of how Parliament's chosen markings align to the Government scheme will be completed in 2023 and a high-level mapping table will be included in revised versions of this document.

8. Monitoring and Compliance

8.1. Data and Information Storage Requirements

8.1.1 Lead Appointed Parties or Appointed Party organisations (Suppliers) must have a retention schedule that states the length of retention of all project records and artefacts they hold

that were generated during the working relationship with Parliament and which comply with legal or other regulatory requirements.

8.1.2 Parliament retains the right to audit its models, data and information stored in supply chain members' IT environments. The audit may inspect contractors' facilities, processes, and other security arrangements to ensure compliance with Parliamentary requirements.

8.1.3 If requested, Lead Appointed Parties or Appointed Party organisations (Suppliers) must confirm the return, and/or secure deletion of, Parliament's data at the end of the contract period. CPNI and NCSC have produced guidance on best practices[10] including the secure deletion and/or destruction of project or asset information held by those organisations, and/ or removal of access to that information.

8.2. Management and Monitoring

8.2.1 Where models, data and/or information are held at off-site storage facilities, the Lead Appointed Parties or Appointed Party organisations (Suppliers) shall manage and enforce access and monitor individuals accessing data.

8.2.2 Implementation shall be monitored and audited by:

- The programme Information Manager and/or delegated person within Parliament's Estates Information Management (EIM) team

8.2.3 Lead Appointed Parties or Appointed Party organisations (Suppliers) will collaborate with and support the monitoring and auditing process which may include site inspections and reviews of security controls.

8.2.4 If security deficiencies are identified in Lead Appointed Parties or Appointed Party organisations' (Suppliers) security measures, a corrective action plan will be developed by the project manager in consultation with SE's information security specialists. If not implemented effectively and in a timely manner this may result in action under the contract.

8.3. Security Incident Management and Reporting

8.3.1 Lead Appointed Parties or Appointed Party organisations (Suppliers) must be contractually obliged to implement their own security incident processes and to report any incident which affects Parliamentary services or information to their Parliamentary contract manager. This must be done as soon as practicable with appropriate action agreed and implemented within a timely fashion.

8.4. Compliance

8.4.1 In 2023 Strategic Estates plan to review the contractual obligations related to information management and where appropriate, insert an information management compliance checklist into the contract management plan.
Note: Any changes will be included in revised versions of this document.

[10] NCSC - Destruction and disposal. Available from: www.ncsc.gov.uk/topics/destruction-and-disposal CPNI - Secure destruction. Available from: http://www.cpni.gov.uk/secure-destruction

8.4.2 The information management compliance checklist will be based on the expectations set out in the Information Security Assessment and will also be based on the level of risk appetite associated with the service provided.

9. Information Handling

9.1. External Sharing

9.1.1 External Sharing is the direct sharing of Parliamentary information and/or systems with external users. Anyone who is not a direct employee of Parliament (either House of Commons, House of Lords or Parliament Digital Service [PDS] is an external user (e.g., Members, Members' Staff, Contractors), even if they have security clearance, a security pass, access to Parliamentary IT, or a Parliamentary network account (eg: parliament.uk).

9.1.2 Parliamentary staff must read and adhere to the *External Sharing Principles* before sharing Parliamentary information and/or systems with external users. They can then use the *External Sharing Guidance* which is a 'how to' guide on the approved ways of sharing Parliamentary information externally.

9.1.3 Lead Appointed Parties or Appointed Party organisations (Suppliers) should, where available, use the appropriate Parliamentary systems to share information and ensure that they have robust and secure means to share information with their supply chains.

9.1.4 For Parliamentary staff who require more information, please seek additional advice from Estates Information Management (EIM) Team in SE; and the Information and Records Management Service (IRMS).

9.2. Sharing information on Parliamentary approved systems

9.2.1 There are accredited systems which we can use for sharing information with Lead Appointed Parties or Appointed Party organisations (Suppliers). Formal details on what can be shared on In-Tend, Aconex and SharePoint are available in the *External Sharing Guidance*. This is summarised below:

Tool	Notes/Used For
SharePoint	External sharing can be activated to share links to parliamentary information with users who do not have parliamentary accounts. See below.
Aconex	To exchange built asset information up to Highly Restricted with external third parties engaged to deliver building projects across the parliamentary estate
In-Tend	To share information as part of tendering processes. Information up to Restricted can be shared using the tool where appropriate.

Figure 4 - Sharing via Approved Systems

9.2.2 Aconex secure mailing boxes & distribution lists

There is a function within Parliament's Common Data Environment (CDE) - Aconex - to allow for sharing of more sensitive documents with discrete groups of individuals. This will ensure that documentation is only shared with those who should receive it rather than their full organisation/ project. It is important that this function is utilised where appropriate, and more guidance can be obtained from the CDE Administrator.

9.2.3 Restricted Access accounts on Intend are required to be set up for those tenders which require the sharing of certain restricted material to specific security cleared individuals. Please review the PPMS guidance to clarify exactly when this applies, additionally you can seek advice from the Information Asset Owner (IAO) or Information Manager in Strategic Estates. Generic email addresses used in standard Intend supplier registrations such as *sales@supplier.com* are not accepted for Restricted Access accounts and thus this solution provides an additional level of reassurance.

9.2.4 For Parliamentary staff who require more information or require a new supplier account set up, please contact the PPCS 'Policy and Compliance' team.

9.3. Information Handling in Programmes and Projects

9.3.1 Guidance on handling information in programmes and projects is given in PPMS documents. Sensitive Parliamentary information should be accessed only by appropriately Parliamentary cleared personnel operating authorised equipment from approved and assured technology such as the encryption of data in transit over all communications methods. (For more information re security clearance see Section 10.2 below.)

9.3.2 The protection of personal data is to be compliant with the standard Parliamentary contractual terms and conditions which meet the requirements of the Data Protection Act 2018.

9.3.3 Information should be stored and managed in a manner to ensure that it can be accessed only by those with the appropriate business requirement and Parliamentary security clearance and need to know. This can be achieved in several ways such as volumes segregated according to classification or a single volume with strong role-based access controls.

9.3.4 Whichever approach is chosen assurance is required through the accreditation or supplier assurance strategy that an appropriate mechanism is in place and is effective.

9.3.5 Advice on the interpretation of the guidance is available from

- the Estates Information Management (EIM) team;
- the Information and Records Management (IRMS) team;
- the Information Compliance (IC) team; and
- the Security Projects (Physical Security) team within Parliamentary Security Department (PSD).

9.4. Handling of Models, Data, and Information – Sensitive Assets and Systems

9.4.1 Any CDE used shall be configured and organised, based on the appropriate strategies for the project, so that:

- Individual files and groups of files are organised and separated by Project/Location, and space/feature;
- It is possible to link Project and/or Location strategy codes to security levels within the system to obscure the presence of files, data and codes associated with the strategy from those with inappropriate security access;
- It shall be possible to assign and manage individual users' access to different levels of sensitive models, data, and information in accordance with the classification and grading;

- Access to information is managed on a role and user basis, with need-to-know principles being applied to the grant of access.

9.5. Models, Drawings, Specifications and Other Design Artefacts

9.5.1 In general, models, drawings, specifications, and other design artefacts shall be classified in accordance with the PPMS and Grading Guide. Where practicable they should be redacted to reduce protective marking Compliance with each of the following is required.

- Location reference numbers are used in place of the combination of room name and either occupier role or name (e.g.: need to avoid *PM is in room 34*).
- Where a specific asset is sensitive:
  - No annotation which explicitly states its function is included;
  - The LOD and LOI[11] does not exceed that specified in the Model Production Delivery Table (MPDT) or Detailed Responsibility Matrix.

9.5.2 Models, drawings, specifications and other design artefacts detailing:

- Systems providing an emergency or safety critical function shall be classified as Restricted as a minimum;
- Telecommunication and IT links, particularly access points into buildings, control centres, etc. shall be classified Restricted as a minimum;
- Alarms and related security systems shall be classified as Highly Restricted as a minimum.

9.6. Conducting Surveys

9.6.1 Surveys shall be conducted in accordance with the GMP – Geospatial Management Plan[12]. This includes the capture of remotely sensed data, including laser scanning and photography.

9.6.2 Prior to any survey:

- The survey requestor shall determine whether the survey will cover any sensitive assets or systems;
- The organisation undertaking the survey shall meet with the Parliamentary Estates' Physical Security Team (PSD) team to discuss and agree equipment; methodology; software; format and any other project-specific requirements to ensure compliance with Parliamentary Estate survey, GMP and security documentation;
- It is important that surveys of internal areas are conducted with no occupants and with a clear desk policy. This is essential to avoid collecting occupant personal data in photographs or other pictures in the area;
- Surveys should avoid photographing security features such as alarm sensors, access control points, security barriers or CCTV cameras unless specifically agreed in advance.

---

[11] LOD: Level of Detail, demonstrates the graphical content of models
LOI: Level of Information, demonstrates the non-graphical content of models

[12] Survey procurement, level of detail, accuracy and methodology guidance required across the estate.

9.6.3 A record of the outcome from these actions shall be recorded by the Project Lead and a formal record kept and retained by the project.

9.6.4 Contractor survey equipment to be reused for other customers must be capable of securely deleting Parliamentary information once it has been transferred for processing.

9.6.5 Information gathered from surveys must be classified appropriately and then be transferred and processed securely (e.g., the use of encrypted USB device and accredited IT systems). For full specification of appropriate USB devices, please refer to the Parliamentary Secret Handling Protocol.

9.6.6 Detailed surveys of sensitive areas of the estate should consider the effects of aggregation.

9.6.7 These procedures shall be followed regardless of whether the survey is being undertaken using internal or external survey teams.

9.6.8 Any information that has been determined to be Parliament Secret shall be masked or redacted where possible. Such information shall be handled and stored in line with the requirements of the Parliament Secret Handling Instructions.

9.6.9 All components of the supply chain (including the main contractor's subcontractors) will collaborate with, and support, the Information Manager in the monitoring and auditing process.

9.6.10 Implementation of the agreed requirements will be monitored and audited by the programme Information Manager and/or delegated person within the Estates Information Management (EIM) team.

9.7. Level of Information – Sensitive Assets and Systems

9.7.1 Each individual component within a model Level of Information Need requires two components that form part of the Levels of Definition:

- Graphical: Level of Detail (LOD)
- Non-graphical: Level of Information (LOI)

9.7.2 The LOD and LOI for any sensitive asset shall not exceed that specified in the Model Production Delivery Table[13] (MPDT) or Detailed Responsibility Matrix[14].

9.7.3 Within any Unrestricted model or database, the Level of Definition associated with any sensitive asset or system shall not exceed that required for Level of Definition 2 (Conceptual), as set out in the MPDT, Lead or Appointed Party Detailed Responsibility Matrix and LOD/LOI. Doc Ref: 00ESW-XXXX-HOP-XX-XX-Z-XX-SH-00002

9.7.4 Where a higher Level of Definition is required, these attributes shall be held in a partitioned, access-controlled storage, with access managed on a need-to-know basis.

[13] A Model Production Delivery Table defines who produces what, when and to what level of detail, in a BIM project.
[14] The Responsibility Matrix clearly sets out the responsibility for the production of information and models for each defined project stage, and to what Level of Definition.

10. Security Considerations

10.1.1 The security considerations listed here draw heavily from both ISO 19650-5:2020, the NCSC, and the CPNI Security Considerations Assessment (SCA) process. This includes security measures for:

- Physical
- Personnel
- Technical
- Process

The security considerations are structured along these four measures with each containing the expected outcome from the 'Information Risk Management Principles performance indicators' as set out in Accreditation Standard that forms part of Parliament's Bicameral Risk Appetite Statement.

10.1.2 This section explains the security considerations to achieve the expected outcomes. The Information Risk Management Principles performance indicators are listed in Appendix B. These are derived from the Accreditation Standard in Parliament's Bicameral Risk Appetite Statement as the expected outcomes required to achieve the principles. These are noted in the considerations below as the G, P, D, & R points.

10.1.3 BS EN ISO 19650-5:2020 is a specification for security-minded information management. It provides a framework for organisations to understand key vulnerabilities and the controls needed to manage their security risks.

10.1.4 The CPNI Security Considerations Assessment (SCA) process ensures security-related vulnerabilities are considered across a range of activities and processes within an organisation.

10.1.5 Parliament's Bicameral Risk Appetite Statement enables the Senior Information Risk Owners (SIRO) for both Houses to be confident that their information risk exposure are being managed.

10.1.6 The Parliamentary Protective Marking Scheme (PPMS) is applied to all security considerations. See Section 7 above for more details.

10.2. *Personnel Security Considerations*

10.2.1 P10 - Only trusted and vetted personnel are granted access to systems, applications, and data repositories

- Security screening and vetting policy/requirements
  - The Parliamentary Security Vetting (PSV) service has streamlined the way to apply for security clearance and pass renewals online. Staff and new starters will be able to fill out a digital form which will automatically be sent to the Security Vetting Team to process.
  - Both internal and external 'new starters' need an internal sponsor to send "*all the required information; and support you through the process to complete your security clearance*".
  - Numerous relevant user guides are available from the Security Vetting & Pass Office team.

- Depending on the level of risk appetite it may be only appropriate for BPSS to gain access to parliamentary information. This might occur if the business risk appetite level is 'Hungry' or 'Open'.
- For Parliamentary staff who require more information about vetting requirements, please seek additional advice from
  - The Security Vetting Unit in the Parliamentary Security Department (PSD).

Parliamentary Network Accounts

- Contractors, consultants, and Lead Appointed Parties or Appointed Party organisations (Suppliers) may be issued with a Parliamentary network account which provides them with access to relevant Parliamentary systems and information where there is a business need and this is approved by the Information Asset Owner (IAO).
- For Parliamentary staff who require more information, please seek additional advice from
  - The External Sharing Guidance
  - Parliament's Account Management Policy
  - the Information and Records Management Service (IRMS) team
  - the Parliamentary Security Department (PSD).

- Any clearance requirements need to be determined from the understanding of the business impact should the solution be compromised
  - This is determined though the **risk appetite level** within the Bicameral Risk Appetite Statement

Clearance	Description	Parliamentary use & application
Baseline Personnel Security Standard (BPSS)	A BPSS acts as a pre-employment check, signalling good recruitment and employment practice in general. The check is carried out by screening identity documents and references. The check include: • identity • employment history (past 3 years) • national and immigration (right to work) status • unspent criminal record.	This check is conducted during the on-boarding of Parliamentary staff. For contractors (and sub-contractors) Parliament relies upon the internal checks of said suppliers.

Counter Terrorist Check (CTC) **or (CTC Cleared)**	A CTC will normally take up to six months to complete and is usually valid for 3 years. It includes: • identity • employment history (past 3 years) • national and immigration (right to work) status • unspent criminal record.	Parliamentary Policy requires all staff with access to the Parliamentary Estate and/or Parliamentary Network to be CTC cleared. Parliament also performs an extra financial credit check for 'Parliamentary clearance' Parliament's staff renew their CTC/Parliamentary Clearance every three years
Security Check (SC) **or (SC Cleared)**	To gain (SC) clearance you will normally need to have been a UK resident for a minimum of 5 years, and will need to successfully complete all stages of the vetting process which includes: • Baseline Personnel Security Standard • Departmental/Company Records Check • Security Questionnaire • Criminal Record Check • Credit Reference Check • Security Service Check	This is needed if required to handle Parliamentary Secret (PS) information * PS was formerly known as Grade 4 information

Figure 5 - Types of Security Clearance used in Parliament

10.2.2 P11 - Personnel are granted the minimum access to systems, applications and data repositories required for their duties.

When assuring the delivery of this outcome the following principles should be considered:

Any access decision by the IAO is recorded

- Any decision for enabling external user access to data shall be recorded
- Where the information is stored digitally the solution must be able to consume the business approved access right.
- Only designated and privileged users must be able to amend access rights
- The modification or update of access right shall be recorded, and any record be immutable
- Any access control decision for user shall use a managed and trusted identity service
- Where the users identity is not managed by Parliament the IAO is responsible for ensuring revocation of any user access rights.

The IAO must review the access decisions on a regular basis.

➢ Appropriate **procedural/technical controls** are put in place to control access to information which is appropriate for the technical implementation.

- There are too many controls to list – every system will be different with different controls expected - but an example of this in practice are SharePoint groups which permit different levels of access to different groups in different locations

- Information assets are identified and any '**need to know'** constraints are identified
  - An example of identifying the different levels of information assets is the Schedule 1 of the Security Aspects Letter (SAL) which identifies the (sensitive) information which the Lead Appointed Parties or Appointed Party organisations (Suppliers) will manage and protect during the life of the contract.

Note: An assessment of the Schedules within Parliament's Security Aspects Letter (SAL) will be completed in 2023. Any alterations will be included in revised versions of this document.

10.2.3 P12 - Multiple methods are used to identify and authenticate personnel to systems, applications, and data repositories

- **Joiners & Leavers** process should consider access to applications and data
  - Parliament's New Joiners process contains a *'Line Managers' - Preparation for New Joiners' Checklist* that includes a request for Parliamentary Network (PN) Account and access to shared drives & mailboxes.
  - Lead Appointed Parties or Appointed Party organisations (Suppliers) must evidence their ongoing management of personnel clearances/access, including ongoing revalidate clearance + process to revoke access

- User Authentication Process
  - Parliamentary staff must be aware of, and comply with, responsibilities expected of users of Parliamentary digital systems, such as:
    - Acceptable use user responsibilities document
    - The password user responsibilities document
  - Lead Appointed Parties or Appointed Party organisations (Suppliers) must understand and articulate their User Authentication to any services which

should be using at least two independent factors to authenticate access to any solution being used to transmit, process and store Parliament protectively marked information.

10.2.4 P13 - Personnel are provided with ongoing information security awareness training

- Both Parliamentary staff and staff from Lead Appointed Parties or Appointed Party organisations (Suppliers) must partake of **staff training** on information security awareness at least annually.

10.3. *Technical Security Considerations*

10.3.1 P1 - Systems and applications are designed, deployed, maintained, and decommissioned according to their value and their confidentiality, integrity, and availability requirements

- All **security risks** must be identified, considered and appropriate controls defined to keep all systems secure. This applies to all solutions, systems and process which Parliamentary staff and Lead Appointed Parties or Appointed Party organisations (Suppliers) use to handle Parliamentary information.
- Security controls must be in place to mitigate security risks. Lead Appointed Parties or Appointed Party organisations (Suppliers) shall assess all identified security risks and put in place a plan to reduce the level of risk exposure to that which is acceptable to Parliament.
- For more general information please refer to the latest guidance from the National Cyber Security Centre (NCSC) regarding Risk Management Guidance.

10.3.2 P3 - Systems and applications are configured to reduce their attack surface

- All solutions must be **configured** in accordance with supplier/industry best practice. This applies to all solutions which process Parliament information irrespective as to whether they are provisioned for use by Parliamentary staff and/or Lead Appointed Parties or Appointed Party organisations (Suppliers).
- This will include best practice from NCSC/NIST on various topics as monitoring vulnerabilities, segmenting your network, using strong encryption policies, and training employees.

10.3.3 Where applications are provisioned or developed and deployed to process Parliamentary information then an appropriate testing framework shall be used to identify any inherent vulnerabilities e.g. OWASP ASVS**P5 - Security vulnerabilities in systems and applications are identified and mitigated in a timely manner**

- Regular security **vulnerabilities scanning** must be undertaken on internal infrastructure, preferably with automatic (non-human) processes in place to update signature (vulnerability patterns) updates to vulnerability tools.
- Vulnerability assessments must be conducted in conformance with the guidance set out in NCSC Vulnerability Scanning Tools and Services
- Lead Appointed Parties or Appointed Party organisations (Suppliers) shall monitor both vendor websites for publication of vulnerability reports including the UK CiSP[15] for wider vulnerability awareness. Should a vulnerability be relevant to component used in any part of the Supply Chain then the risk shall be recorded any corrective action shall be taken.
- There are commercial obligations in place for any Lead Appointed Parties or Appointed Party organisations (Suppliers) processing Parliamentary information to performs these actions.

10.3.4 P7 - Data is encrypted at rest and in transit between different systems

- **Encryption** must comply with the NCSC cryptographic standards and guidance such as "Using TLS to protect data".
- Appropriate security controls shall be in place to ensure the confidentiality of any stored Parliamentary aggregated dataset is protected. Where assured encryption is the method chosen to implement this control then all data at rest shall be cryptographically configured in accordance with NIST guidance.
- Where Parliament information is shared between systems then it shall be protected using a cryptographic solution which has been assured for use with the UK public sector by the National Cyber Security Centre or via an international security standards certification body. This security outcome shall be assured for all service/solutions processing Parliament protectively marked information.

10.3.5 P8 - Data communicated between different systems is controlled, inspectable and auditable

- The use of a **protective monitoring solution** must conform with the steps to implementation set out in the NCSC (National Cyber Security Centre) "Logging and monitoring" guidance. The solution at the gateway, or boundary of the service should be able, to decryption, inspect and apply policy controls to data/information being passed to, or received from, other systems.
- Where it is not possible to inspect data or information then internal security enforcing controls shall be applied e.g., network segmentation and end point control capabilities on client or server
- This applies to Parliamentary staff and Lead Appointed Parties or Appointed Party organisations (Suppliers).

10.3.6 P9 - Data, applications and configuration settings are backed up in a secure and proven manner on a regular basis

- **Geographic resilience** must be in-built into the data back-up storage.
- The **regularity** of the back-up will be proportionate and appropriate to the business impact/risk appetite level for the solution.
- This applies to Parliamentary staff and Lead Appointed Parties or Appointed Party organisations (Suppliers).

---

[15] The Cyber Security Information Sharing Partnership (CISP) is a joint industry and government digital service to allow UK organisations to share cyber threat information in a secure and confidential environment. For more details see the NCSC website

10.3.7 P11 - Personnel are granted the minimum access to systems, applications and data repositories required for their duties

- **Access control** must be enforced such that only approved personnel can access Parliament protectively marked information being processed/stored by the Lead Appointed Parties or Appointed Party organisations (Suppliers).
- This should include a user access policy (or equivalent) which is role based and adopts the principle to least privilege.

Security Model Volumes

- A Security Model is a container showing Geo-Metric representations of a secure asset with associated asset information, e.g.: operational details; manufacturer's make & model etc The Volume relates to the discipline e.g.:
  Electrical; Mechanical etc
- Segregation of Security Model Volumes that may reveal the location of end devices (eg: cameras; access door panels; reinforcements etc).
- Separation of Asset Information from 3D Model geometry pertaining to end devices (camera/ access control panel).

- For Parliamentary staff who require more information, please seek additional advice from the Project BIM Lead representative in the Estates Information Management (EIM) Team in SE.

Redaction

- Redaction of Parliamentary Secret Information for sharing
- Redaction of 2D Drawings (using symbols and separate key sheet)
- Redaction of 3D Surveys (eg: Point clouds containing sensitive asset locations)

- For Parliamentary staff who require more information, please seek additional advice from a specialist security advisor from the Security Projects (Physical Security) team within Parliamentary Security Department (PSD).

Design Coordination

- Coordinating with Engineering disciplines (Telecoms/Electrical) for placement of Security End Devices
- Coordinating with private landowners (eg: free/lease holds) on the location of asset installations (potentially include a redacted set of drawings)

- More details regarding the processes involved can be found in Section 12 below.

10.3.8 P12 - Multiple methods are used to identify and authenticate personnel to systems, applications and data repositories

- Lead Appointed Parties or Appointed Party organisations (Suppliers), SaaS (Software as a Service) or subcontractor system(s) associated with the contract that process Parliament Information have **Multi-Factor Authentication** (Two Factor Authentication) in place and password complexity is defined.
- Any identity which is used to enable a User to be authorised to access a solution or service processing Parliamentary information shall be derived from a Parliamentary Identity Service/source.

- All applications which process Parliamentary information shall be able to directly consume a token or digital certificate to enable a decision to made to allow access to Parliamentary information or services.

10.3.9 D1 - Information security events and anomalous activities are detected, collected, correlated, and analysed in a timely manner

- Lead Appointed Parties or Appointed Party organisations (Suppliers) must ensure their digital service(s) are **automatically monitored** with the management processes in place to provide alerts and reports which are then investigated.

10.3.10 R2 - Information security incidents are contained, eradicated, and recovered from in a timely manner

- Lead Appointed Parties or Appointed Party organisations (Suppliers) must ensure that security alerts are **automatically generated** and reported to their Security Operations Centre (SOC).

10.3.11 R3 - Business continuity and disaster recovery plans are enacted when required

- Lead Appointed Parties or Appointed Party organisations (Suppliers) must ensure they have **alternative technical solutions and capabilities** in place to enable business continuity with loss of primary/main business solution.

10.4. *Process Security Considerations*

10.4.1 G1 – A nominated senior person is responsible for providing leadership and oversight of information security

- Parliament has designated **Departmental Information Risk Officers (DIRO)** who have overall responsibility for information risk assessment, handling and investigating information breaches, monitoring and mitigation and provides assurance that business practices accord with policies and guidance.
- The DIRO answers to the Senior Information Risk Officer (SIRO) who is the senior person responsible for overall information assurance for the House of Commons at Board level. The Head of the Governance Office is the current SIRO.
- Lead Appointed Parties or Appointed Party organisations (Suppliers) must identify and nominate a board representative or a person with the direct delegated authority who is responsible for (information) security management for their organisation, including the management of subcontractors.
- He or she should have the authority to put in place security controls, will be held accountable for any deficiencies in these controls, will investigate breaches of security and will act as the main point of liaison for Parliamentary security officials.

10.4.2 G2 - The identity and value of systems, applications and data is determined and documented

- Parliament maintains an up-to-date **Information Asset Register (IAR)**. This is a document that helps Parliament to identify, understand and manage its information assets and the potential risks to them. IARs help Parliament to:
    - Understand where information is held

- Know who the nominated owner of each asset is
- Identify how long to keep information
- Know who has access to the information and why
- Secure information appropriately
- Identify, understand, and manage risks to the business in relation to the assets
- Provide assurance that information is being managed properly.

- Parliament will also maintain an up-to-date **IT asset register** which is a tool to log and monitor all IT hardware, PCs and equipment.
- Lead Appointed Parties or Appointed Party organisations (Suppliers) should also have processes in place to identify and document the value of their systems, application, and data.
- For built asset (BIM) projects the Lead Appointed Parties or Appointed Party organisations (Suppliers) must comply with the requirements of the appointing party and will document the methodology of compliance in the **BIM Execution Plan**. This will consist of:
  - Personnel (security vetting; background checks; NDA etc)
  - Physical (site logistics & planning etc)
  - Information Technology (secure systems; information security etc)
- For Parliamentary staff who require more information, please seek additional advice from Estates Information Management (EIM) Team in SE; and the Information and Records Management Service (IRMS).

10.4.3 G3 – The Confidentiality, Integrity, and Availability (CIA) requirements of systems, applications and data is determined and documented

- Both Parliament and Lead Appointed Parties or Appointed Party organisations (Suppliers), should be confident when doing risk assessments on any solution that they look at the confidentiality, integrity, and availability requirements (CIA) that it is attempting to protect, and should know the **importance of the characteristics** of the systems, applications, and data.
- The implementation of the CIA requirements helps to ensure that systems/applications and data/information are not compromised in any way when critical issues arise.

10.4.4 G4 - Information risk management processes are embedded into organisational risk management frameworks

- The Parliamentary Bicameral Risk Appetite Statement sets out Parliament's approach to information risk management and the relationship to the wider delivery processes. The approach shows how the setting the Solution **Risk Appetite Level** to determines the assurance process which identifies residual risks which informs the Accreditation decision.
- The "Information Risk Management Activities" diagram within the Bicameral Risk Appetite Statement, visualises Parliament's approach information risk management. The Bicameral Risk Appetite Statement does not stand in isolation and is informed by activities which are outside of its scope, but which are included in the diagram for completeness.

10.4.5 G5 - Information risks are identified, documented, managed, and accepted by the Solution Owner both before systems and applications are authorised for use, and continuously throughout their operational life

- Parliament's internal Information Risk Management Recording and Reporting mechanism is called the **Accreditation Decision Record** (ADR). The outcome of all assurance

processes in Parliament are captured in the ADR. All decisions of the associate treatment of residual risk must be set out in the ADR as time bounded conditions of assurance.

- Lead Appointed Parties or Appointed Party organisations (Suppliers) should also have processes in place to identify, document, manage and accept information risks.
- Parliament's matrix of information risk levels is visualised in the "Information Risk Levels" diagram (page 14 of the Bicameral Risk Appetite Statement). See figure 6 below.

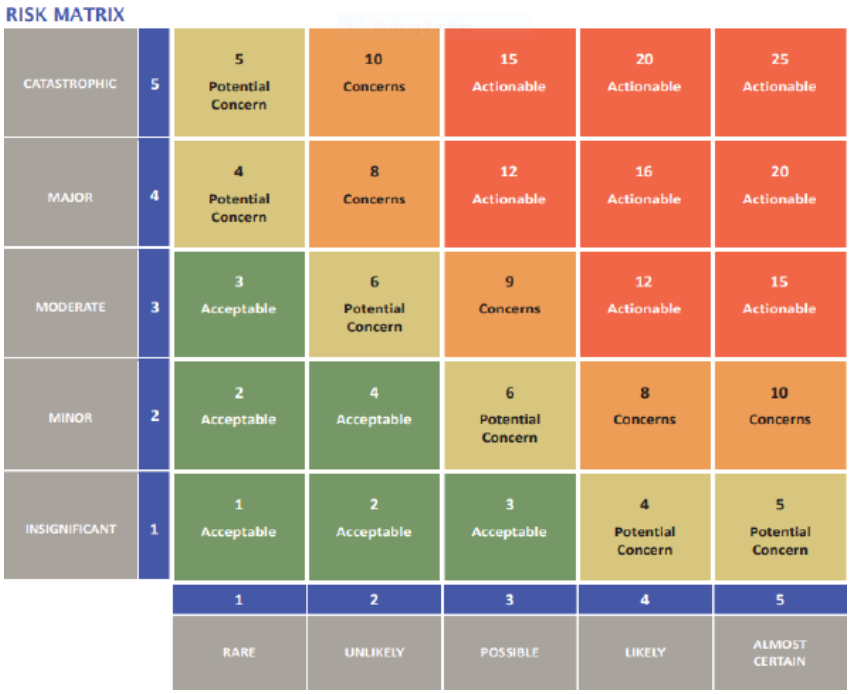

Figure 6 - Information Risk Levels

10.4.6 G6 - The level of information risk exposure is defined and within Parliament's tolerance

- Parliament's Delegated Information Risk Management Authority sets out the Roles which have been authorised to assure exposure is tolerable within Parliament risk tolerance. When a risk management decision is made it must be recorded on the Accreditation Decision Record for the solution.
- If an information risk above Level 7 is identified, then the Information Assurance lead and Service Owner shall jointly prepare a submission to the relevant risk management authority to ascertain whether the information risk within Parliament Risk Tolerance. See figure 7 below.
- Lead Appointed Parties or Appointed Party organisations (Suppliers) should also have processes in place to

ROLE	Risk Management Authority
Solution/Service Owner	Authority to accept information risk that have been assessed as being below Risk Level 3.
Accreditor	Authority to accept information risk that have been assessed as being between Risk Level 3 and Level 7.
Assurance Working Group	Authority to accept information risk that have been assessed to between Risk Level 8 and 10.

Information Authority	Authority to accept information risk that have been assessed above Risk Level 10

Figure 7 - Delegated Information Risk Management Authority

10.4.7 G7 - System and applications information risks are assured in consistent and proportionate manner

10.4.8 The process of **accreditation** within the Houses of Parliament provides the Information Authority with assurance that the information security risk exposure associated with solutions that store or process Parliamentary data, is within the business' risk tolerance. Accreditation aims to ensure security is built into every solution from the beginning rather than it being an afterthought at the end and must be performed in accordance with the Parliament's Accreditation Standard.

10.4.9 Assurance processes shall be performed in accordance with the Parliament Accreditation Standard and associated guidelines/procedures.

- **Note** – Parliament does not currently have a process for 'external accreditation'.

10.4.10 P2 - Systems and applications are delivered and supported by trusted suppliers

- Parliament has processes in place to perform **supply chain due diligence**. Parliament must derive the necessary assurances that Lead Appointed Parties or Appointed Party organisations (Suppliers) can competently and securely manage and process Parliamentary information.
- Lead Appointed Parties or Appointed Party organisations (Suppliers) must
  - undertake a due diligence process to ensure the effectiveness of any security risk management processes prior to onboarding any sub-contractors;
  - ensure the flow down of security requirements (from main contract to sub-contractor contracts;
  - ensure the ongoing and regularity of auditing of sub-contractors is in place throughout the lifetime of the contract.
- Lead Appointed Parties or Appointed Party organisations (Suppliers) shall have processes in place to consume updates and patches from vendors being used to deliver service to Parliament.
- When a vendor does publish a security related patch or update the Lead Appointed Parties or Appointed Party organisations (Suppliers) must have processes and technical measure in place to enable deployment in a timely manner.
- Where vendor product delivers security enforcing controls then security certification in place which demonstrates effective information risk management in the vendor development and deployment processes

10.4.11 P4 - Systems and applications are administered in a secure, accountable, and auditable manner

Lead Appointed Parties or Appointed Party organisations (Suppliers) must ensure they have an up-to-date user access policy (or equivalent) which is role based and adopts the principle to least privilege. This requires robust HR (Human Resources) processes to be in place which will enable and revoke user access on personnel joining or leaving.

- Administration of system, applications and computer code shall only be performed by designated roles which have been granted privileged access rights
- Privileged roles must only be provided with the absolute minimum access rights, permissions they need to fulfil their administrative function.
- There must be a formal authorisation process and policy for User to be granted,

assigned and approved a privileged role.

- Robust user authentication process shall be in place for accessing any privileged roles.
- Any actions performed from a privileged roles shall be record and malicious actions shall be promptly reported.
- Any administrative function exercised shall only be possible from managed devices and within network segments which are only accessible to a privileged role.
- A business continuity process shall be in place to ensure a privileged roles can perform in the event of component failure.

10.4.12 P6 - Only trusted and supported operating systems, applications and computer code can execute on systems

- The Parliamentary process of accreditation provides assurance that solutions, storing or processing Parliamentary protectively marked data, are meeting appropriate Parliamentary security standards.
- Lead Appointed Parties or Appointed Party organisations (Suppliers) should follow NCSC guidance "Secure development and deployment guidance" to help understand the security implications of modern code development and deployment practices.

10.4.13 D1 - Information security events and anomalous activities are detected, collected, correlated and analysed in a timely manner

When assuring the delivery of this outcome the following principles should be considered:

- All aspects of the service which delivery security controls shall be capable of reporting events that might constitute a security incident
- All events reported shall be time stamped using an authoritative and consistent source
- All events shall be communicated securely
- Only authorised personnel shall be able to access any event related information.
- If an event is assessed to be a security incident, then then any such instance shall be reported to a single management report service which is monitored appropriately.

- An information breach is a breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to sensitive information. Breaches may be the result of both accidental and deliberate action.
- Parliamentary staff must report any information breach so advice can be sought on how to not only reduce the consequences of any breach, but to learn lessons and ensure controls have been put in place to avoid any future breaches.
- If Parliamentary staff suspect that information has been lost, accessed inappropriately or misused, make sure that Information Compliance (House of Commons) or the Information Compliance team (House of Lords) are notified straightaway. This can be done via email or through the loss or misuse of information and/or equipment form on Digital Service Online.
- Lead Appointed Parties or Appointed Party organisations (Suppliers) should have:
    - Have an approved Incident Management Policy in place
    - Communicate any cyber and physical compromise/breach of Parliamentary information immediately
    - Have a nominated individual responsible for process management

10.4.14 R1 - Information security incidents are identified and reported both internally and externally to relevant bodies in a timely manner

- See 10.4.11 above
- If anomalous activity is detected and a security alert is raised, then the process needs to be in place to respond to the alert and instigated an appropriate response plan
- If information is destroyed, lost, altered without authorisation, or accidentally disclosed to another party this is classed as an information breach. If personal data is involved, the House Service has 72 hours to report this to the supervisory authority, Information Commissioners Office (ICO), who oversee data protection laws.

10.4.15 R2 - Information security incidents are contained, eradicated, and recovered from in a timely manner

- See 11.4.11 above
- If Parliamentary staff suspect that they have been deceived into giving out sensitive information or infecting their device(s) through emails, texts or social media, it's important that they report it to the Digital Support Desk by calling x2001 immediately.

10.5. *Physical Security Considerations*

10.5.1 P14 - Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel

- The Parliamentary Security Department (PSD) have developed a document entitled "***Known Supplier Guidance Document***" to provide a good practical framework for the designation and on-going oversight of known Lead Appointed Parties or Appointed Party organisations (Suppliers) accessing the Parliamentary Estate. It details the required security processes of known suppliers and should help Parliamentary Suppliers and contractors develop their own procedures that satisfy Parliament's security requirements.
- The key aspects covered include:
    - The Supplier designation process
    - The Supplier validation process
    - Guidance for Known Supplier Security Strategy
        - Details of contract
        - Person responsible for security
        - Employment checks and training
        - Preventing unauthorised access to the premises and Parliamentary Supplies
        - Security Search & Screening/ Site Security Checks and Controls
        - Deliveries
        - Quality assurance
- For Parliamentary staff who require more information, please seek additional advice from a specialist security advisor from the Security Projects (Physical Security) team within Parliamentary Security Department (PSD).
- The "***Strategic Estates Handling Instructions - Parliament Secret"*** protocol describes Strategic Estates (SE) information security requirements for the physical and electronic handling and implementation by staff who are responsible for the receipt, registration, safe custody, distribution, and control of material for information protectively marked as Parliament Secret. This has previously been called RESTRICTED ACCESS SECURITY GRADE 4.

- The protocol is intended to assist teams to determine the correct level of security and put in place the associated controls to protect Parliament Secret material. This will also benefit Parliamentary staff and Lead Appointed Parties or Appointed Party organisations (Suppliers) by outlining how to manage physical documents in their day-to-day roles.
- The key aspects covered include:
    - Production of Parliament Secret Material
    - Use & Disseminate (access & sharing)
    - Delivery or Transfer
    - Appraise & Dispose
    - Incident Management
    - Supply Chain Assurance
    - Secure cabinets

11. Information Handling for Tendering

11.1. Procurement processes

11.1.1 Information provided to supply chain companies (Lead Appointed Parties or Appointed Party organisations) must be protected adequately in accordance with Parliamentary requirements.

11.1.2 The Parliamentary Procurement and Commercial Service ('PPCS') oversees all procurement processes carried out in Parliament and provides procurement services for both House of Lords and House of Commons.

11.1.3 PPCS must be consulted by project leads about the most appropriate procurement route for contracts and will assess the most appropriate procurement procedure to be deployed.

11.1.4 PPCS is structured into three category teams, these are:

- Works (Construction and maintenance)
- Services and Supplies, and
- Information and Communications Technology (ICT).

Each category team can provide advice and the relevant level of expertise

11.2. Framework

11.2.1 Parliament contracts with Lead Appointed Parties or Appointed Party organisations (Suppliers) through a variety of processes.

11.2.2 For high value requirements Parliament follows the (external link) Public Procurement Regulations (PCR 15). These require Parliament to advertise its contract opportunities to suppliers directly in the open marketplace, or through a (external link) Framework Agreement let by an official organisation (for example Crown Commercial Services, or through an internal Parliamentary framework).

11.2.3 For lower value requirements, Parliament advertises its needs directly to the marketplace (or uses a framework agreement, or if approved by waiver, a single tender action). In all cases, the contract ultimately is between the House's Corporate Officer(s) in Parliament and the Lead Appointed Parties or Appointed Party organisations (Supplier). The only difference being where Parliament advertises to the marketplace, it uses its own terms and conditions. Where it employs an external framework agreement it uses the terms of that agreement, with allowed adaptations to ensure they meet Parliament's needs.

11.3. For all tenders

11.3.1 A **Non-disclosure Agreement (NDA)** is a legally binding agreement which sets out how you share

information or ideas in confidence and limits the party's ability to disclose the confidential information of others. An NDA should be used when Parliament is sharing information which may be deemed sensitive, or which is protectively marked as Restricted or above. Additionally, an NDA is used for contracts or projects for which the subject matter may be deemed confidential for commercial reasons.

11.3.2 Non exhaustive examples for an NDA requirement include projects / contracts which:

- May contain information which should not be disclosed outside of Parliament;
- May contain sensitive security information;
- May contain ideas or plans which could be replicated or shared for commercial gain;
- May contain personal data;

11.3.3 For Parliamentary let framework agreements, provided there is an overarching NDA signed by all suppliers named on the framework, an additional NDA is NOT required for each call off.

11.3.4 For Parliamentary staff who are using an externally let framework, (for example Crown Commercial Services - CCS), or who are unsure whether an NDA is required, or what template to use, please contact the Head of Procurement Policy and Compliance in PPCS.

11.4. Expressions of interest (EoI) and current tenders

11.4.1 The Parliamentary Procurement and Commercial Service ('PPCS') uses an *e-tendering portal* (hosted by In-Tend) to manage its procurement processes. Potential suppliers/bidders need to register on the portal before they can express an interest in any opportunities and view the associated tender documents.

11.4.2 The PPCS process for EoI is outlined online on Parliament's website – (external link) see link here.

11.4.3 Occasionally Parliament hosts 'Industry Days' where potential suppliers may come onsite (Parliamentary Estates) to be briefed on a future (sensitive) project or to view the relevant part of the Estate to the project.

11.5. Redaction

11.5.1 Data to be passed to potential bidders should be redacted as far as practicable to reduce its sensitivity, where appropriate.

11.5.2 Internal Parliamentary guidance exists entitled the "*Omission of Sensitive Information in Tender Documentation Guidance*". This was created by the Parliamentary Security Department (PSD) as the definitive guide to the omission of sensitive information in documents being prepared for use during tendering, planning and/or listed building consent application processes.

11.5.3 The basic principle of the guidance requires all such documentation to omit sensitive Parliamentary information prepared for these purposes, creating anonymised artefacts that can be shared with uncleared supply chains and statutory and other authorities processing planning, and/or listed building consent applications.

11.5.4 The principle of omitting sensitive information should be applied wherever possible to all Parliamentary projects and programmes that wish to tender to uncleared supply chains. Broadly speaking, it is both impractical and unnecessary to require prospective Lead Appointed Parties or Appointed Party organisations (Suppliers) to security clear their workforces prior to appointment and could place a high administrative burden on Parliament's Personnel Security Service. That said, it is sometimes necessary for bidders to understand the constraints of where they are working to be able to accurately price works/services, if this is the case then a prior security clearance stage should be used. This would be assessed on a case-by-case basis.

11.5.5 For Parliamentary staff who intend to redact information, or consider doing so, please contact the Parliamentary Security Department (PSD) and the Estates Information Management (EIM) Team for more information and assistance.

11.6. Required Documents in Works team tender processes:

11.6.1 Due diligence is required to on-board Lead Appointed Parties or Appointed Party organisations (Suppliers) and to implement works and services for Parliament. The due diligence aims to derive assurances of suppliers' technical capabilities and competencies to securely handle Parliamentary information. For this purpose, Parliament has several documents for use as follows:

11.6.2 The **Security Aspects Letter (SAL)** is intended as a contractual document which requires Lead Appointed Parties or Appointed Party organisations (Suppliers) to agree to meet Parliamentary information security requirements for their own information systems and those of their subcontractors, where these will hold Parliamentary information. Contract information security levels are identified in the SAL which is intended to be contract (not company) specific.

The SAL user guide (internal link entitled Guidance on Using the Security Aspects Letter (SAL) – is included with the Invitation to Tender - ITT - package) must be read prior to completing a SAL as it clearly details the structure and additional documents and schedules required.

The SAL is sent as a template with SQ/ tender documents – but is only required to be completed and signed by those awarded the contract.

Note: An assessment of the Schedules within Parliament's Security Aspects Letter (SAL) will be completed in 2023. Any alterations will be included in revised versions of this document.

11.6.3 The **Information Security Assessment (ISA)** (formerly known as the Non-Functional Security Requirements - NFSR) asks Lead Appointed Parties or Appointed Party organisations (Suppliers) a series of Yes/No questions to gauge their technical infrastructure with regards to information management. Security accreditation is currently the only evidence requested at this stage.

11.6.4 Dependent on the level of risk associated with the project or programme the ISA is sent with SQ/tender documents and is required to be completed by all bidders and assessed by Parliament (pass / fail) at SQ/Tender stage

11.6.5 The **Detailed Information Security Assessment (DISA)** (formerly entitled the Information Security Management Plan - ISMP) follows the ISA and forms a Schedule to the SAL. It asks Lead Appointed Parties or Appointed Party organisations (Suppliers) to build on the high-level information they have already provided by requesting evidence to support their information management technical infrastructure.

11.6.6 Dependent on the level of risk associated with the project or programme, the DISA is sent as a template with SQ/tender documents – but is only required to be completed by those awarded the contract.

11.6.7 The **Parliamentary Security Management Plan (PSMP** - this document) is the last of the portfolio of documents that support Parliament's implementation of the standard for information security.

The PSMP is sent with SQ/tender documents and is part of the Scope/Specification/Works Information

11.6.8 The documents are required to be used as follows. Please consider the information which will be shared not only at tender stage, but throughout the life of the contract.

Information Classification	NDA	SAL	ISA	DISA	PSMP
Unrestricted	No	No	No	No	No
Restricted	Yes	Yes	Yes	Yes	No

Highly Restricted	Yes	Yes	Yes	Yes	No
Project (Which may be any of the above classifications)	Yes	Yes	Yes	Yes	Yes

Figure 8 - Information Classification

11.6.9 **Note:** At present the ISA and the DISA (formerly the NFSR and ISMP) only occurs on "*Works*" contracts. PPCS are reviewing processes for *Services & Supplies* and *ICT* contract with a view to harmonising.

11.6.10 The approach to be used for information handling and assurance during the procurement of contracted work services is given in the table below:

Procurement of Contracted Work Services	
Soft Market Testing	➢ When bidders are informed about the project so they can determine whether they are interested and for Parliament to ensure there is sufficient market interest, capability and capacity for the proposed route to market
Expression of Interest (EoI)	➢ Supplier Questionnaire with security question requiring written response ➢ Capability Assessments may apply to some procurements
Invitation to Tender (ITT)	➢ Non-Disclosure Agreement (NDA) ➢ Information Security Assessment (ISA/NSFR) ➢ Employer's Information Requirements (EIR) ➢ Template Security Aspects Letter (SAL) and schedules for information, PPMS, Grading Guide, DISA/ISMP (for information only)
Bid Submission	➢ ISA/NFSR response evaluated to feed into Bid review process. (This will happen earlier if using the Selection Questionnaire and/or the Capability Assessment when tendering)
Procurement of Contracted Work Services	
Contract Award	➢ Project Issues Security Aspects Letter (SAL) Schedule 1 completed and signed by the Project Lead (as they own the information) ➢ Suppliers sign Security Aspect Letter (SAL)
Post Contract	➢ Suppliers completes the Detailed Information Security Assessment – DISA (formerly the ISMP)

Figure 9 - Information Security in the Works Procurement Process

11.6.11 At contract award the SAL should be signed by the supplier and the supplier's completed Detailed Information Security Assessment (DISA) endorsed by Parliament.

11.6.12 For Parliamentary staff who manage sensitive security projects, or require more information, please seek additional advice from Estates Information Management (EIM) Team.

12. Review of the PSMP

12.1. Policy

12.1.1 The Parliamentary Security Management Plan (PSMP) shall be subject to annual and ad hoc reviews by the Information Manager or delegated person within the Estates Information Management (EIM) team. This will ensure that it continues to satisfactorily deliver the risk mitigation measures identified in the Bicameral Risk Appetite Statement.

12.2. Role Responsibilities

12.2.1 For full list of roles and responsibilities please refer to

- The Employers/Exchange Information Requirements (EIR) Doc Ref: 00ESW-XXXX- HOP-99-XX-K-XX-DO-00001 (1192 series) and
- 00ESW-XXXX-HOP-99-XX-K-XX-DO-00009 (BS EN ISO 19650 series).

12.3. Supporting Processes

12.3.1 During a project, the Parliamentary Security Management Plan (PSMP) shall be reviewed:

- When moving from design into construction; and
- When moving from construction into operation.
- The action will depend on what is expressed in the contract

12.3.2 A review shall also be undertaken should if any changes in the political, legislative, or regulatory environment that could have an impact on information held in a CDE or asset/facilities management database. This will also include all physical records.

12.3.3 A review shall be completed if any change in the security situation around the built asset which they believe will have a significant impact upon it not otherwise taken into consideration.

12.3.4 Reviews shall be planned and executed so that they do not cause delays in agreed work timetables. If an issue is identified which means that a delay is inevitable to satisfactorily mitigate an unacceptable risk, the matter shall be taken to the Parliamentary Security Working Group to agree a course of action. Under these circumstances, and any other relevant representatives of the parties impacted shall be invited to attend, and participate in, the committee meeting.

13. 1192 & 19650 Alignment

13.1. 1192 Series Documents/Parliament Bespoke Documents

1192 Series Documents/Parliament Bespoke Documents	BS EN ISO 19650 Series Documents
PLQs – Plain Language Questions	PIR – Project Information Requirements
EIR - Employers Information Requirements	EIR -Exchange Information Requirements
Construction Industry Council (CIC) Information Protocol Second Edition	BS EN ISO 19650-2 Information Protocol
MIDP - Master Information Delivery Plan/TIDP Task Information Delivery Plan	Information Delivery Plan

MAL - Managed Asset List Level of Information Need (LOD/LOI) Construction Operations and Building Information Exchange (COBie) Responsibility Matrix Strategic Estates CAD & Document Numbering Guidance AIS – Asset Information Specification RNC - Room Numbering Convention AIR - Asset Information Requirements Section 17 Information Exchanges EIR – Employers/Exchange Information Requirements Section 5.1 Exchange Formats	Project's Information Standards
Project Delivery Handbook	Project Information Delivery Milestones
Computer Aided Design (CAD) Standards DHP – Digital Handover Procedure AIR – Asset Information Requirements BASIR – Built Asset Security Information Requirements (now the PSMP) COBie and Model Variation Guide	Project's Production Methods and Procedures
BS1192:2007 a2 2016 and PAS1192-2:2013 BIM Level 2 Certification	BS EN ISO 19650-2 Certification
As-built Record Information	Project Reference Information
Design Responsibility Matrix (DRM)	High Level Responsibility Matrix
Model Production Delivery Table (MPDT)/BIM Responsibility Matrix (BRM)	Information Model Responsibility Matrix
Pre-Contract BIM Execution Plan (BEP)	Pre-appointment BIM Execution Plan (BEP)
Post-Contract Award BIM Execution Plan (BEP)	Project Delivery BIM Execution Plan (BEP)

Figure 10 - 1192 Series Documents/Parliament Bespoke Documents

13.2. 1192 Series General Terms relationship to BSEN ISO19650

1192 Series General Terms	BS EN ISO 19650 Series General Terms
Suitability	Status
Graphical	Geometrical
BIM Maturity Level	BIM Maturity Stage
Level of Definition (LOD)	Level of Information Need -LOIN
Common Data Environment (CDE): sections, i.e. WIP, Shared, Published, Archive	Common Data Environment CDE: states, i.e. WIP, Shared, Published, Archive
AIM – Asset Information Model	Same
AIR – Asset Information Requirements	Same
BASM – Built Asset Security Management Plan	Security Management Plan
BEP – BIM Execution Plan	Pre-Appointment or Project Delivery BEP
BIM – Building Information Management	Same
BWM – BIM Workgroup Meeting	N/A
CAFM – Computer Aided Facility Management	Same
CDM - The Construction (Design and Management) Regulations 2015	N/A
COBIE – Construction Operations and Building Information Exchange	Same
EAM – Energy Analysis Model	N/A
FM – Facility Management	Same
GSL – Government Soft Landings	Same
IFC – Industry Foundation Class	Same
HoP – Houses of Parliament	N/A
NRM – New Rules of Measurement	N/A
OIR – Organisational Information Requirements	Same
PIC – Project Information Cloud	N/A
PIM – Project Information Model	Same
PIP – Project Implementation Plan	Mobilisation Plan
POE – Post Occupancy Evaluation	Same
PTM – Project Team Member	Same
RM – Responsibility Matrix	Same
SE – Strategic Estates	N/A
SLC – Soft Landings Champion	Same
SMP – Standards Methods and Procedures	Projects Information Standards, Project's Information Production Methods and Procedures
TIM – Task Information Manager	N/A
TTM – Task Team Manager	N/A
WIP – Work in Progress	Same
Pathways	Trigger Event
Data Drop	Information Exchange
Volume Strategy	Federation Strategy'

Figure 11 - 1192 Series General Terms relationship to BSEN ISO19650

13.3. 1192 Series Supply Chain Terms

1192 Series Supply Chain Terms	BS EN ISO 19650 Series Supply Chain Terms
Roles	Actors (Appointing Party, Lead Appointed Party and Appointed Party) or Information Management Functions (Supply Chain Individual Organisations)
Employer	Appointing Party
Lead Consultant/Contractor or Principal Designer/Contractor under CDM 2015	Lead Appointed Party
Sub Consultant/Contractor or Designer under CDM 2015	Appointed Party
Common Data Environment (CDE): sections, i.e. WIP, Shared, Published, Archive	Common Data Environment CDE: states, i.e. WIP, Shared, Published, Archive

Figure 12 - 1192 Series Supply Chain Terms

Note: For the avoidance of doubt the term 'Employer' is deemed fully interchangeable with the term ‘Client’ under **CDM:2015** and Appointing Party under **BS EN ISO 19650- 2:2018.**

13.4. Industry Standards and Guidelines

Title	Description
BS EN ISO 19650-1:2018	Organization and digitization of information about buildings and civil engineering works, including Building Information Management -- Information management using Building Information Management : Concepts and principles.
BS EN ISO 19650-2:2018	Organization and digitization of information about buildings and civil engineering works, including Building Information Management -- Information management using Building Information Management : Delivery phase of the assets.
BS EN ISO 19650-3:2020	Organization and digitization of information about buildings and civil engineering works, including Building Information Management (BIM). Information management using Building Information Management . Operational phase of the assets
BS1192-4:2014	Collaborative production of information. Fulfilling employer’s information exchange requirements using COBie.
BS EN ISO 19650-5:2020	Organization and digitization of information about buildings and civil engineering works, including Building Information Management (BIM). Information management using Building Information Management . Security-minded approach to information management
PAS1192-6:2018	Specification for collaborative sharing and use of structured Health and Safety information using BIM
BS EN ISO 19650-2 Information Protocol	Information protocol to support BS EN ISO 19650-2 the delivery phase of assets
ISO 12006-2:2015	Building construction — Organization of information about construction works — Part 2: Framework for classification

Title	Description
ISO 16739-1:2018	Industry Foundation Classes (IFC) for data sharing in the construction and facility management industries — Part 1: Data schema
ISO 27001:2013	Information Security Management
BS 8536-1:2015	Briefing for design and construction. Code of practice for facilities management (Buildings infrastructure)
BS 8536-2:2016	Briefing for design and construction. Code of practice for asset management (Linear and geographical infrastructure)
Uniclass 2015	Unified classification system for all sectors in the UK construction industry
SFG20	Standard maintenance specification for building engineering services
NRM	Order of cost estimating and cost planning for building maintenance work
CIBSE Guide Table M	Chapter 12 - Table of asset life expectancy
BSRIA BG-1:2007	Consider To be deleted Standard Superseded
BSRIA BG-6:2018	A Design Framework for Building Services
BSRIA BG-79:2020	Handover information and O&M manuals
BSRIA BG-54:2014	Soft Landings Framework 2018 (BG 54/2018)
BS EN 17412-1:2020	Building Information Management . Level of Information Need. Concepts and principles
BS7913: 2013 BIM for Heritage	Guide to the conservation of Historic Buildings Developing the Asset information Model
BS8541-2:2011	Library objects for architecture, engineering and construction. Recommended 2d symbols of building elements for use in Building Information Management
BS 8541-1:2012	Library objects for architecture, engineering and construction. Identification and classification - code of practice

Figure 13 - Industry Standards and Guidelines

14. Appendices

14.1. Appendix A: Bibliography

14.1.1 Parliamentary Documents

- Acceptable use user responsibilities document
- Accreditation Decision Record (ADR)
- Bicameral Risk Appetite Statement
- BIM Execution Plan
- External Sharing Principles
- Information Asset Register
- IT asset register
- Known Supplier Guidance Document
- 'Line Managers' - Preparation for New Joiners' Checklist
- Omission of Sensitive Information in Tender Documentation Guidance
- Parliament's Account Management Policy
- Parliamentary Protective Marking Scheme Guidance
- PPMS Guidance - IHSE Sch2 – SAL
- Security Vetting & Pass Office team User Guidance
- Strategic Estates Handling Instructions - Parliament Secret
- The External Sharing Guidance
- The password user responsibilities document

14.1.2 External Documents

- PAS1192
- BS EN ISO 19650 Building Information Management (BIM) maturity level 2 regulatory standards
- CPNI - Ongoing operation, management, and maintenance of an existing built asset (including buildings and infrastructure)
- CPNI - Secure destruction. Available from: www.cpni.gov.uk/secure-destruction
- CPNI - Security Considerations Assessment (SCA) process
- Data Protection Act 2018
- Detailed Responsibility Matrix
- Employers/Exchange Information Requirements (EIR)
- Geospatial Management Plan
- Information protocol to support BS EN ISO 19650-2 the delivery phase of assets
- Model Production Delivery Table (MPDT)
- NCSC - Destruction and disposal. Available from: www.ncsc. gov.uk/topics/destruction-and-disposal
- NCSC - Logging and monitoring guidance
- NCSC - Risk Management Guidance
- NCSC - Using TLS to protect data
- NCSC - Vulnerability Scanning Tools and Services
- NEC4 Secondary Clause X10 Particulars

14.2. Appendix B - Information Risk Management Principles performance indicators

Govern principal performance indicators

G1: A nominated senior person is responsible for providing leadership and oversight of information security.

G2: The identity and value of systems, applications and data is determined and documented.

G3: The confidentiality, integrity and availability requirements of systems, applications and data is determined and documented.

G4: Information risk management processes are embedded into organisational risk management frameworks.

G5: Information risks are identified, documented, managed, and accepted by the Solution Owner both before systems and applications are authorised for use, and continuously throughout their operational life.

G6: The level of information risk exposure is defined and within Parliament's tolerance.

G7: System and applications information risks are assured in consistent and proportionate manner.

Protect principal performance indicators

P1: Systems and applications are designed, deployed, maintained and decommissioned according to their value and their confidentiality, integrity and availability requirements.

P2: Systems and applications are delivered and supported by trusted suppliers.

P3: Systems and applications are configured to reduce their attack surface.

P4: Systems and applications are administered in a secure, accountable and auditable manner.

P5: Security vulnerabilities in systems and applications are identified and mitigated in a timely manner.

P6: Only trusted and supported operating systems, applications and computer code can execute on systems.

P7: Data is encrypted at rest and in transit between different systems.

P8: Data communicated between different systems is controlled, inspectable and auditable.

P9: Data, applications and configuration settings are backed up in a secure and proven manner on a regular basis.

P10: Only trusted and vetted personnel are granted access to systems, applications and data repositories.

P11: Personnel are granted the minimum access to systems, applications and data repositories required for their duties.

P12: Multiple methods are used to identify and authenticate personnel to systems, applications and data repositories.

P13: Personnel are provided with ongoing information security awareness training.

P14: Physical access to systems, supporting infrastructure and facilities is restricted to authorised personnel.

Detect principal performance indicators

D1: Information security events and anomalous activities are detected, collected, correlated and analysed in a timely manner.

Respond principal performance indicators

R1: Information security incidents are identified and reported both internally and externally to relevant bodies in a timely manner.

R2: Information security incidents are contained, eradicated and recovered from in a timely manner.

R3: Business continuity and disaster recovery plans are enacted when required.

14.3. Appendix C: PPMS Examples for Strategic Estates

Documents

Examples	• Contracts • The existence of the Contract • Association of the Contract with HoP • Employee Contact Information that is openly commercially available. • Job descriptions • Terms of reference • Roles and Responsibilities • Collections data • Designs (intended) • Retention schedule • Guidance • Standards and Policies (published) • FOI responses • File Lists • Comms/marketing • Academic outputs • Internal communications	• Information relating to any supplier's involvement in the Contract • Subcontracting documentation issued by Houses of Parliament • Any document that relates only to the subcontractor's own facilities, corporate IT environment etc • Completed forms relating to Security Clearance • Any document the bidder creates forming part of their response to this subcontract • Collection's data • Designs + Design Reports • Standards + Policies + Strategies (Unpublished) • Accommodation Schedules • Contractual communications • Programmes & Schedules • Recruitment docs • Spreadsheets (on/off site) • Due diligence documentation • Audits • Room data sheets (Revit) • Planning application drawings • internal review and/or redacted • Real estate contractual information and metadata	• Any correspondence, response or query relating only to ○ commercial aspects of subcontracting ○ technical aspects of the services to be provided, as described in the subcontract • Minutes • Contact lists + Parl staff names • Process documentation • Information Asset Registers • Asbestos information • Data Flow Diagrams • User groups – Roles & Permissions on system • Management plans • Business cases • Schematic plan of a location • Procurement data & info • Resource schedules & CVs • Engagement data requirements • Maintenance scheduling • O & M manuals • Risk registers • Incident reporting • Accommodation Schedules • Timesheets • Project plans • Tender information	• Subcontracting documentation issued by Houses of Parliament (if information relates to Parliamentary security systems) • Any correspondence, response or query relating to technical aspects of the services to be provided, as described in the subcontract (if information relates to Parliamentary security systems) • Any document the bidder creates forming part of their response to this subcontract (if information relates to Parliamentary security systems) • Audits e.g. Parliament secretholdings • Occupancy info/location e.g.Location of Prime Minister's office • Certifications – Health & Safety – Safe systems of work • Schematic plan of a location • Pass details referring to high-level security clearance

Activities

	Restricted	Highly Restricted
Activities	The following work activities and the assets and/or systems, types of systems associated with them shall be regarded as **Restricted**: • Details of the location of the built asset and its physical environment; • Profile and attractiveness of the built asset as a target; • Nature of occupiers/users; • Any legal or regulatory requirements; • Complexity and criticality of building systems; • Survey information with photographs and details of sensitive locations (such as server room, security functions); • Degree of connectivity of building systems to systems (such as Building Management System (BMS)); • Details of Mechanical, Electrical and Plumbing for Proprietary Plant and Equipment (such as facility locations, utility management points, system vulnerabilities); • Space IDs when associated with system functions, organisational roles, or personnel; • Information about location of IT servers and systems, data centres, data cabling; • Maintenance systems with information on assets and their functions or level of support.	The following work activities and the assets and/or systems, types of systems associated with them shall be regarded as **Highly Restricted**: • Detailed asset detailed designs and drawing to include metadata on security functions (such as CCTV / Access control sensor locations, fabric; • Operational control point locations, systems, and connectivity; • Evacuation areas and routes; • All details concerning Physical Safety and Security Systems (PSSS); • Survey information with photographs and details of sensitive locations (such as server room, security functions); • Detailed operations and connectivity of BMS; • Personnel management systems with locations and movements of parliamentary personnel; • Details of IT system function and capabilities (such as server rooms, switches, data centres); • Server rooms fit out with details of system connectivity and capability; • Security Equipment Room (SER) fit out; • Security Operations Centre (SOC) fit out; • Pass Office fit out.

14.4. Appendix D: Project Information Standard

Project Information Standards Document References	
Title	Reference
Managed Asset List (MAL) A non-exhaustive list of estate wide maintainable, security and heritage assets aligned to their corresponding SFG20, NRM3, CIBSE Table M and Uniclass 2015 classification codes for the delivery and operation phase of assets.	00ESW-XXXX-HOP-XX-XX-Z-XX-SH-00001
Level of Information Need (LOD/LOI) Shows the graphical and non-graphical detail and information required at each Royal Institute of British Architects (RIBA 2020) plan of work stage, this includes the grading requirements for security assets aligned to the Parliamentary Protective Marking Scheme (PPMS).	00ESW-XXXX-HOP-XX-XX-Z-XX-SH-00002
Strategic Estates CAD & Document Numbering Guidance Document numbering procedures aligned to Project Delivery Common Data Environment (CDE) placeholder number generator tool.	00ESW-XXXX-HOP-99-XX-K-XX-SH-00003
Asset Information Specifications (AIS) Guidance on acquisition and population off space I.D and asset I.D, including QR code generation.	00ESW-XXXX-HOP-99-0X-Z-XX-DO-00006
Room Numbering Conventions (RNC) This document aims to provide a good practice guidance for assigning room numbers.	00ESW-XXXX-HOP-99-XX-Z-XX-DO-00008
Asset Information Requirements (AIR) Asset information aspirations from client including Construction Operations Building Information Exchange (COBie) parameters for security, heritage, and maintenance assets.	00ESW-XXXX-HOP-99-XX-K-XX-DO-00002 (1192 series) and 00ESW-XXXX-HOP-99-XX-K-XX-DO- 00008 (BS EN ISO 19650 series)
Exchange Information Requirements (EIR) Guidance on how to Employ appropriate systems, tools, and procedures to achieve “BS EN ISO 19650” maturity as specified in	00ESW-XXXX-HOP-99-XX-K-XX-DO-00001 (1192 series) and 00ESW-XXXX-HOP-99-XX-K-XX-DO-00009 (BS EN ISO 19650 series)
COBie Responsibility Matrix Supply chain responsibility matrix for populating COBie parameters	00ESW-XXXX-HOP-99-XX-K-XX-SH-10001
Project Information Requirements (PIR) Plain Language Questions for Digital Assurance	00ESW-XXXX-HOP-99-XX-K-XX-DO-00007

Figure 14 - Project Information Standard

Project Information Production Methods and Procedures Document References	
Title	**Reference**
Parliamentary Security Management Plan (PSMP – formerly the BASIR) HOP security standards and procedures for Information Technology (I.T), Human Resource (HR) and Physical security aligned to BS EN 19650-5	00ESW-XXXX-HOP-99-XX-K-XX-DO-00003
Strategic Estates CAD Manual HoP CAD manual that explains industry drawing composition methodologies for Computer Aided Design (CAD) elements such as scale, line types, symbology, text heights, borders etc.	00ESW-XXXX-HOP-99-XX-K-XX-PS-00001
Digital Handover Process (DHP) The purpose of this document is to describe as exhaustively as possible the expected digital output from all parties involved in a construction project for Houses of Parliament so that a smooth, well- communicated, and well-coordinated digital hand- over can take place and understand in relation to the Contractors liability and warranty period.	00ESW-XXXX-HOP-99-0X-Z-XX-DO-00007
Supply Chain Responsibility Matrices BIM (BRM) and Design (DRM) Example BIM (Information Model) and Design (High- Level) Responsibility Matrices following the Responsible, Accountable, Consulted, and Informed (RACI) methodology. The project while need to be examined holistically to determine the design and BIM responsibility for each member of the supply chain during overlaps in RIBA 4 - Technical Design and RIBA 5- Construction to prevent future disputes with project scope and task orders.	00ESW-XXNA-HOP-XX-XX-Z-XX-SH-00001
Master Information Delivery Plan Example An example Master Information Delivery Plan for the supply chain to follow, suppliers can use their own organisational MIDP's	00ESW-XXNA-HOP-99-XX-K-XX-TE-00002
COBie Workbook 2.4 Example Industry standard COBie asset spreadsheet example	00ESW-XXXX-HOP-00-XX-K-XX-PS-10001
Geospatial Management Plan Survey procurement, level of detail, accuracy and methodology guidance required across the estate.	00ESW-XXXX-HOP-99-XX-K-XX-DO-00013
Strategic Estates Model and COBie Validation Manual Estates Information Management (EIM) internal COBie and model validation process	Placeholder

Figure 15 - Project Information Production Methods and Procedures

LETTER OF APPOINTMENT – PRINCIPAL DESIGNER AND PRINCIPAL CONTRACTOR

29/02/2024

PHD Modular Access Services Limited
54 Oxford Road,
Denham,
Uxbridge, Middlesex,
UB9 4DN

Dear Danny Dwyer,

RE: STC1173(A) – Principal Contractor: Events

In accordance with the requirements of Regulation 5(1) of The Construction, Design and Management Regulations 2015 (CDM 2015) in the role of Client Representative, acting on behalf of the Corporate Officer of the House of Lords and the Corporate Officer of the House of Commons (acting jointly) for the Strategic Estates department, I hereby appoint PHD Modular Access Services Limited as Principal Contractor and Principal Designer for the STC1173(A) – Principal Contractor: Events.

Strategic Estates acknowledges its obligations in accordance with CDM 2015. Please confirm in writing, the receipt of this Letter of Appointment and PHD Modular Access Services Limited is aware and has sufficient skills, knowledge, experience and organisational capability to carry out the obligations as detailed in CDM regulations 2015.

Your appointment will remain for the duration of the project or until otherwise notified of any change by ourselves.

If any further assistance is required, please let me know.

Yours sincerely,

EXECUTION

Signed for and on behalf of the **Corporate Officer of the House of Lords and the Corporate Officer of the House of Commons, acting jointly**:

……
Authorised Signatory

……
Name

……
Position/Office

……
Date

Signed for and on behalf of the ***Contractor***:

……
Authorised Signatory

……
Name

……
Position/Office

……
Date