

SHORT FORM CONTRACT FOR THE SUPPLY OF SERVICES

Info-Tech Research Group
345 Ridout North
London
Ontario
N6A 2N8

[REDACTED]
[REDACTED]
Date: 01/09/2023
Our ref: C188245

Dear [REDACTED],

Following your tender/proposal for the supply of Research and Advisory Subscription Service to the Food Standards Agency, we are pleased confirm our intention to award this Contract to you.

The attached Order Form, contract Conditions and the **Annexes** set out the terms of the Contract between the Food Standards Agency and Info-Tech Research Group for the provision of the Deliverables set out in the Order Form.

We thank you for your co-operation to date, and look forward to forging a successful working relationship resulting in a smooth and successful Delivery of the Deliverables. Please confirm your acceptance of this Contract by signing and returning the Order Form to the FSA Commercial team at the following email address: [REDACTED] within 7 days from the date of the Order Form. No other form of acknowledgement will be accepted. Please remember to include the reference number(s) above in any future communications relating to this Contract.

We will then arrange for the Order Form to be countersigned which will create a binding contract between us/You should arrange for the Order Form to be countersigned which will create a binding contract between us.

Yours faithfully,

[REDACTED]
Commercial Category Manager

I. Order Form

1. Contract Reference	C188245	
2. Buyer	Food Standards Agency Foss House, Kingspool, Peasholme Green, York, YO1 7PR	
3. Supplier	Info-Tech Research Group 8 Duncannon Street, London, WC2N 4JF	
4. The Contract	<p>This Contract between the Buyer and the Supplier is for the supply of Deliverables.</p> <p>The Supplier shall supply the Deliverables described below on the terms set out in this Order Form and the attached contract conditions ("Conditions") and Annexes.</p> <p>Unless the context otherwise requires, capitalised expressions used in this Order Form have the same meanings as in the Conditions.</p> <p>In the event of any conflict between this Order Form and the Conditions, this Order Form shall prevail.</p>	
5. Deliverables	Goods	None
	Services	<p>As set out in Annex 2 – Specification and in the Supplier's tender as set out in Annex 4 – Supplier Tender</p> <p>To be performed remotely</p>
6. Specification	The specification of the Deliverables is as set out in Annex 2 – Specification and in the Supplier's tender as set out in [Annex 4 – Supplier Tender .	
7. Start Date	2 nd October 2023	
8. Expiry Date	1 st October 2024	
9. Extension Period	The Buyer may extend the Contract for two period of up to 12 months each by giving not less than 4 weeks notice in writing to the Supplier prior to the Expiry Date. The Conditions of the Contract shall apply throughout any such extended period.	
10. Optional Intellectual Property Rights ("IPR") Clauses	Not applicable	
11. Charges	The Charges for the Deliverables shall be as set out in Annex 3 – Charges .	

12. Payment	<p>Payment of undisputed invoices will be made within 30 days of receipt of invoice, which must be submitted promptly by the Supplier.</p> <p>All invoices must be sent, quoting a valid Purchase Order Number (PO Number), to [REDACTED].</p> <p>Within 10 Working Days of receipt of your countersigned copy of this Order Form, we will send you a unique PO Number. You must be in receipt of a valid PO Number before submitting an invoice.</p> <p>To avoid delay in payment it is important that the invoice is compliant and that it includes a valid PO Number, contract reference number and the details (name, email, and telephone number) of your Buyer contact (i.e. Buyer Authorised Representative). Non-compliant invoices may be sent back to you, which may lead to a delay in payment.</p>		
13. Data Protection Liability Cap	In accordance with clause 12.5 of the Conditions, the Supplier's total aggregate liability under clause 14.7(e) of the Conditions is no more than the Data Protection Liability Cap, being £500,000 .		
14. Progress Meetings and Progress Reports	Not applicable		
15. Buyer Authorised Representative(s)	<p>For general liaison your contact will continue to be</p> <p>[REDACTED] [REDACTED] [REDACTED]</p>		
16. Supplier Authorised Representative(s)	<p>For general liaison your contact will continue to be</p> <p>[REDACTED] [REDACTED] [REDACTED] [REDACTED]</p>		
17. Address for notices	<table border="0"> <tr> <td style="vertical-align: top; width: 50%;"> Buyer: <i>Food Standards Agency</i> Foss House, Kingspool, York, YO1 7PR [REDACTED] [REDACTED] [REDACTED] </td> <td style="vertical-align: top; width: 50%;"> Supplier: <i>Info-Tech Research Group</i> 345 Ridout North London Ontario N6A 2N8 [REDACTED] [REDACTED] [REDACTED] </td> </tr> </table>	Buyer: <i>Food Standards Agency</i> Foss House, Kingspool, York, YO1 7PR [REDACTED] [REDACTED] [REDACTED]	Supplier: <i>Info-Tech Research Group</i> 345 Ridout North London Ontario N6A 2N8 [REDACTED] [REDACTED] [REDACTED]
Buyer: <i>Food Standards Agency</i> Foss House, Kingspool, York, YO1 7PR [REDACTED] [REDACTED] [REDACTED]	Supplier: <i>Info-Tech Research Group</i> 345 Ridout North London Ontario N6A 2N8 [REDACTED] [REDACTED] [REDACTED]		

18. Key Staff	Not Applicable
19. Procedures and Policies	For the purposes of the Contract the buyers policies and procedures are found in Annex 2.
20. Special Terms	<i>Not Applicable</i>
21. Incorporated /terms	<p>The following documents are incorporated into the Contract. If there is any conflict, the following order of precedence applies:</p> <ul style="list-style-type: none"> a) The cover letter from the Buyer to the Supplier dated 01/09/2023 (if used) b) This Order Form c) Any Special Terms (see row 20 (Special Terms) in this Order Form) d) Conditions e) The following Annexes in equal order of precedence: <ul style="list-style-type: none"> i. Annex 1 – Processing Personal Data ii. Annex 2 – Specification iii. Annex 3 – Charges iv. Annex 5 - DPA f) Annex 4 – Supplier Tender, unless any part of the Tender offers a better commercial position for the Buyer (as decided by the Buyer, in its absolute discretion), in which case that part of the Tender will take precedence over the documents above.

Signed for and on behalf of the Supplier	Signed for and on behalf of the Buyer
Name: [Redacted] General Counsel	Name: [Redacted] Commercial Category Manager
Date:	Date:
Supplier Signature:	Buyer Signature:
[Redacted]	

II. Annex 1 – Processing Personal Data
A. Part A - Authorised Processing Template

Contract:	C188245 Research and Advisory Service
Date:	01/09/2023
Description of authorised processing	Details
Identity of Controller and Processor for each category of Personal Data	The Buyer is Controller and the Supplier is Processor The Parties acknowledge that in accordance with Paragraph 2 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor
Subject matter of the processing	Personal data will be processed to facilitate contract management and delivery of advise/guidance from the supplier to the Buyer
Duration of the processing	11 th September 2023 – 10 th September 2024
Nature and purposes of the processing	Staff names and contact information will be used to facilitate contract management and delivery of the contract through meetings, phone calls and correspondence.
Type of Personal Data	Name, Staff email address, Staff telephone number.
Categories of Data Subject	Staff, Suppliers.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under law to preserve that type of data	All data will be returned to the buyer upon the completion of this contract
Locations at which the Supplier and/or its Subcontractors process Personal Data under this Contract	Republic of Ireland, United States of America and Canada.

Protective Measures that the Supplier and, where applicable, its Subcontractors have implemented to protect Personal Data processed under this Contract against a breach of security (insofar as that breach of security relates to data) or a Personal Data Breach	Not applicable
---	----------------

III. Annex 2 – Specification

Specification Reference
<i>C188245</i>
Specification Title
<i>Research & Advisory Subscription Service</i>
Contract Duration
<i>1 + 1 + 1</i>
<i>Budget - £70,000 for year 1</i>

This specification, which forms part of the Invitation to Tender (ITT), comprises of three individual sections:

A. SPECIFICATION: An outline of the requirement

B. PROCUREMENT TIMETABLE: An estimated timetable for the procurement of the proposed requirement

C. TENDER REQUIREMENTS AND EVALUATION CRITERIA: Provides guidance to applicants on the information that should be included within tenders and on the evaluation criteria and weightings used by evaluators when assessing and scoring tenders

Tenders for FSA funded projects must be submitted through the FSA E-sourcing and contract management system, ECMS, using the following link: <https://health-family.force.com/s/Welcome>. Failure to do so may result in the tender response not being processed by the system or the response being automatically disqualified during the evaluation stage of the tender process.

THE SPECIFICATION, INCLUDING PROJECT TIMETABLE AND EVALUATION OF TENDERS

GENERAL INTRODUCTION

The Food Standards Agency is an independent Government department working across England, Wales, and Northern Ireland to protect public health and consumers wider interest in food. We make sure food is safe and what it says it is.

The Agency is committed to openness, transparency, and equality of treatment to all suppliers. As well as these principles, for science projects the final project report will be published on the Food Standards Agency website (www.food.gov.uk).

The Food Standards Agency is a non-ministerial government department of over 1500 people, with a big vision – to drive change in the food system so that it delivers “food we can trust”. As the country has now left the EU, the scale of this challenge cannot be underestimated. More than 90% of food and feed law in the UK currently comes from Europe and our primary goal is to continue to protect public health and UK consumers’ wider interest in food.

The context in which we operate has transformed and continues to change at an unprecedented rate. Digital is the primary way we carry out our work, it is key to achieving our ambitions and transforming the way we do business, and we continually strive to provide better online services to external stakeholders and internal customers to achieve faster and more effective models of delivery at optimal cost.

FSA Transparency

In line with the Government’s Transparency Agenda which aims to encourage more direct access to data held by government, the Agency is developing a policy on the release of underpinning data from all its science- and evidence-gathering projects. Underpinning data should also be published in an open, accessible, and re-usable format, such that the data can be made available to future researchers and the maximum benefit is derived from it. The Agency has established the key principles for release of

underpinning data that will be applied to all new science- and evidence-gathering projects which we would expect support partners to comply with. These can be found at <http://www.food.gov.uk/about-us/data-and-policies/underpinning-data>.



A. THE SPECIFICATION

Background

To support the FSA's commitment to provide and improve secure, modern digital and data services, the Department are looking to engage with an organisation who can provide research and advisory services to help continually improve the FSA's Digital, Data and Technology team performance, help us ensure our strategy and approach fully aligns with industry best practice and help us work better with our technology partners.

This year we have significant resource constraints and access to an advisory service will help alleviate the pressure we face and reduce the risk we carry in terms of skills & capability gaps and knowledge base.

The Specification

Provision of a digital, data and technology (DDaT) best practice advisory service providing:

- Support from dedicated expert resource for the FSA's DDaT leadership to guide strategic decision making, risk management, validation, and recommendations on best practice.
- Guidance on creating a department that operates effectively despite any change in economic circumstance.
- Opportunities for the DDaT leadership team to discuss specific problems and overall strategy direction with mentors who have worked at a high level in the DDaT field.
- Online access to resources and onsite access to resources where required.
- Access to an expert for one to one advice for the Chief Information Officer, access to an analyst for deeper dives one to one advice and five roles to have access reference material.
- Over the life of the contract the FSA may choose to extend access to the services provided to additional roles. Any such change would be agreed through a variation to contract.

The specification must:

- Provide access to benchmarking intelligence on major technology contracts (for example: Microsoft Azure, O365, Workday).
- Provide access to resources that will support spend optimisation, providing guidance on potential cost savings, including benchmarks. Suppliers should also provide suggested technical roadmaps with milestones.
- Provide a service to review current contract specifications, performance and Service Level Agreements/KPI's and suggest improvements
- Provide unlimited access on demand to subject matter experts who can guide the DDaT team through complex project delivery. Practical and tactical guidance required and validation of approaches in place will be requested. This needs to cover all the DDaT functions including but not limited to, data architecture, cyber security, service management, cloud optimisation and product management.
- Provide access to expertise on identifying user needs for software.

- Provide access to industry trends, industry benchmarks and resources that will enable Food Standards Agency to optimise practice in alignment with sector.
- Provide a service to help the FSA identify appropriate technology and software options to meet user needs.
- Provide unlimited and unrestricted access to all content including
 - project and process research
 - technology reviews
 - blueprints
 - tools
 - off the shelf, reusable templates
 - diagnostic programmes

The specification should:

- Provide access to on-demand learning resources for the DDaT team, including but not limited to Security, Data, Risk Management, Infrastructure etc.

The specification nice to have:

- Give access to industry events and conferences that provide the DDaT team with opportunities to network, share and develop relationships.
- Provide tools and content that can be used for awareness raising and communicating key messages to FSA staff.
- Provide access to a community of other organisations undergoing or have been through similar DDaT improvement initiatives.

Compliance with UK GDPR regulation

Please outline in your tender how you will comply with the GDPR, recognising the commissioning authority's role as the 'data controller' and the contractor's role as the 'data processor,' and responding to the sections below. If successful you may also be asked to carry out a Privacy Impact Assessment (PIA), and a privacy notice may be required, which will be reviewed by the FSA data security team.

Data security

Please confirm in your tender that you have in place, or that you will have in place by contract award, the human and technical resources to perform the contract to ensure compliance with the General Data Protection Regulation and to ensure the protection of the rights of data subjects.

Please provide details of the technical facilities and measures (including systems and processes) you have in place, or will have in place by contract award, to ensure compliance with the General Data Protection Regulation and to ensure the protection of the rights of data subjects. Your response should include, but should not be limited to facilities and measures:

- to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- to comply with the rights of data subjects in respect of receiving privacy information, and access, rectification, deletion, and portability of personal data;
- to ensure that any consent-based processing meets standards of active, informed consent, and that such consents are recorded and auditable;
- to ensure legal safeguards are in place to legitimise transfers of personal data outside the EU (if such transfers will take place);
- to maintain records of personal data processing activities; and
- to regularly test, assess and evaluate the effectiveness of the above measures.'

Security

The supplier will comply with the following requirements.

Background Checks: supplier shall conduct appropriate background checks on all new employees based on the sensitivity of the role that they are being hired for.

Information Security Awareness: supplier shall develop and implement an information security awareness program designed to ensure that all employees and contractors receive security education as relevant to their job function.

Security in Supplier Agreements: supplier shall ensure that agreements with suppliers who may impact the security of the services or products being supplied contain appropriate security requirements.

Information Security Policy: supplier shall develop, implement, and maintain an information security policy and shall communicate the policy to all staff and contractors.

Risk Management: supplier shall employ a formal risk assessment process to identify security risks that may impact the products or services being supplied, and mitigate risks in a timely manner commensurate with the risk.

Breach reporting If the Supplier becomes aware of a Breach of Security covering FSA data (including a Personal data breach) the Supplier will inform the FSA at the earliest opportunity

Accreditation – supplier will have Cyber Essentials

Technical Security - The supplier will follow the NCSC [Cloud Security Principles](#)

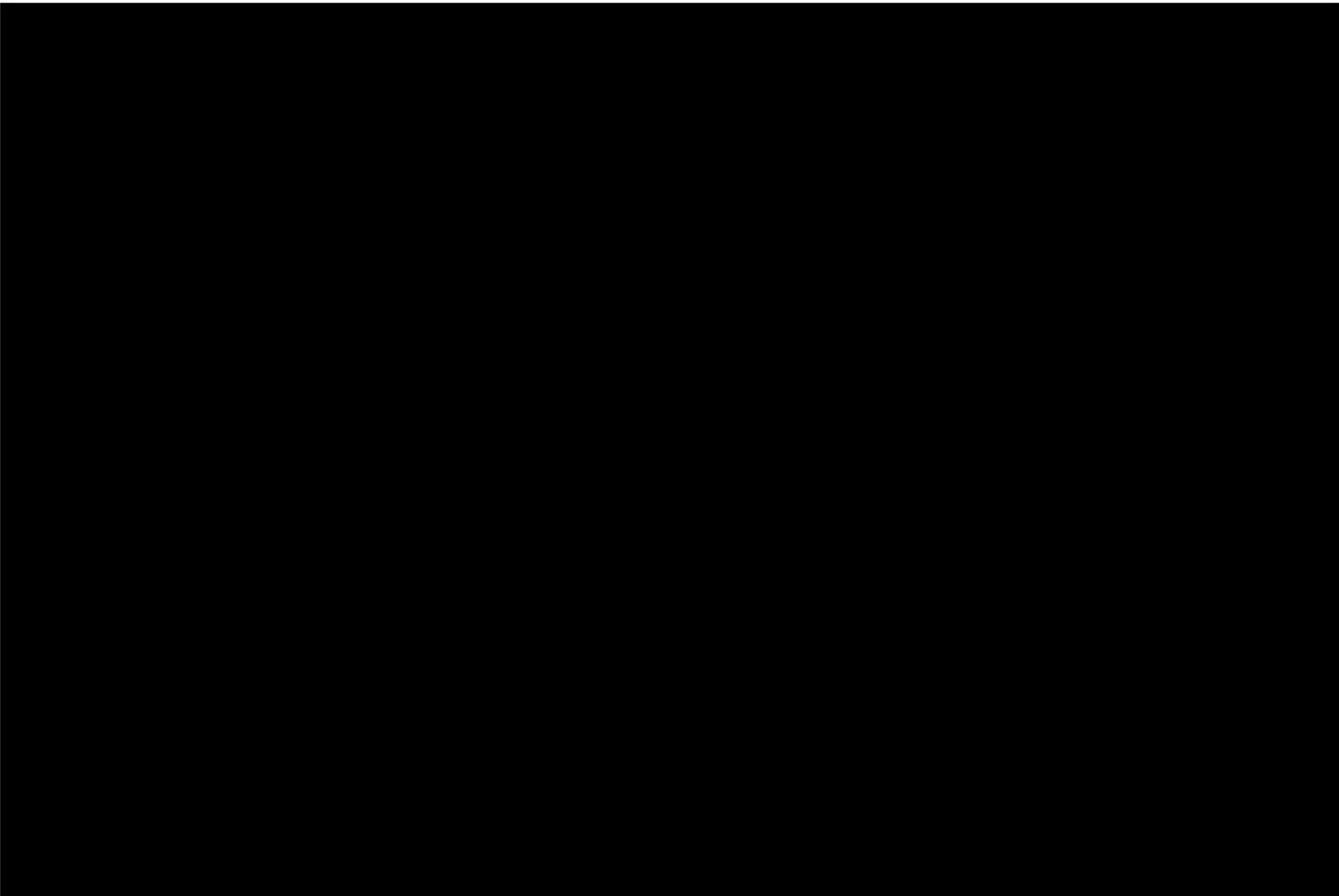
Accessibility

Any report, document or asset produced or provided as part of this service must comply with the Web Content Accessibility Guidelines (WCAG) 2.1 at AA standards. The format and product chosen for delivery must build in accessibility from the beginning to make sure it meets the required standard.

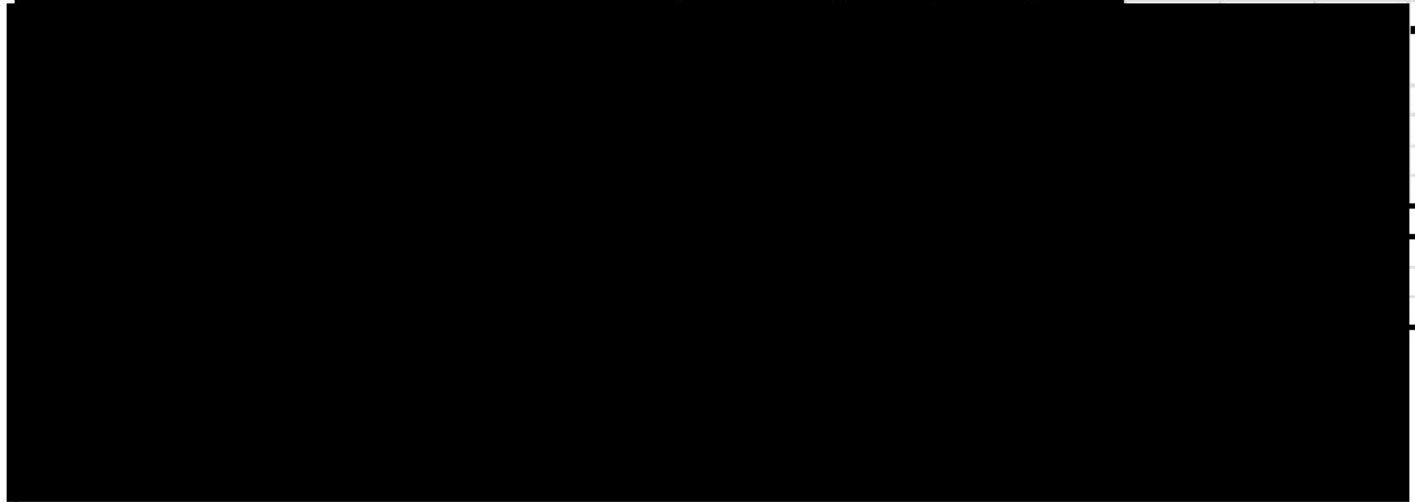
Social value

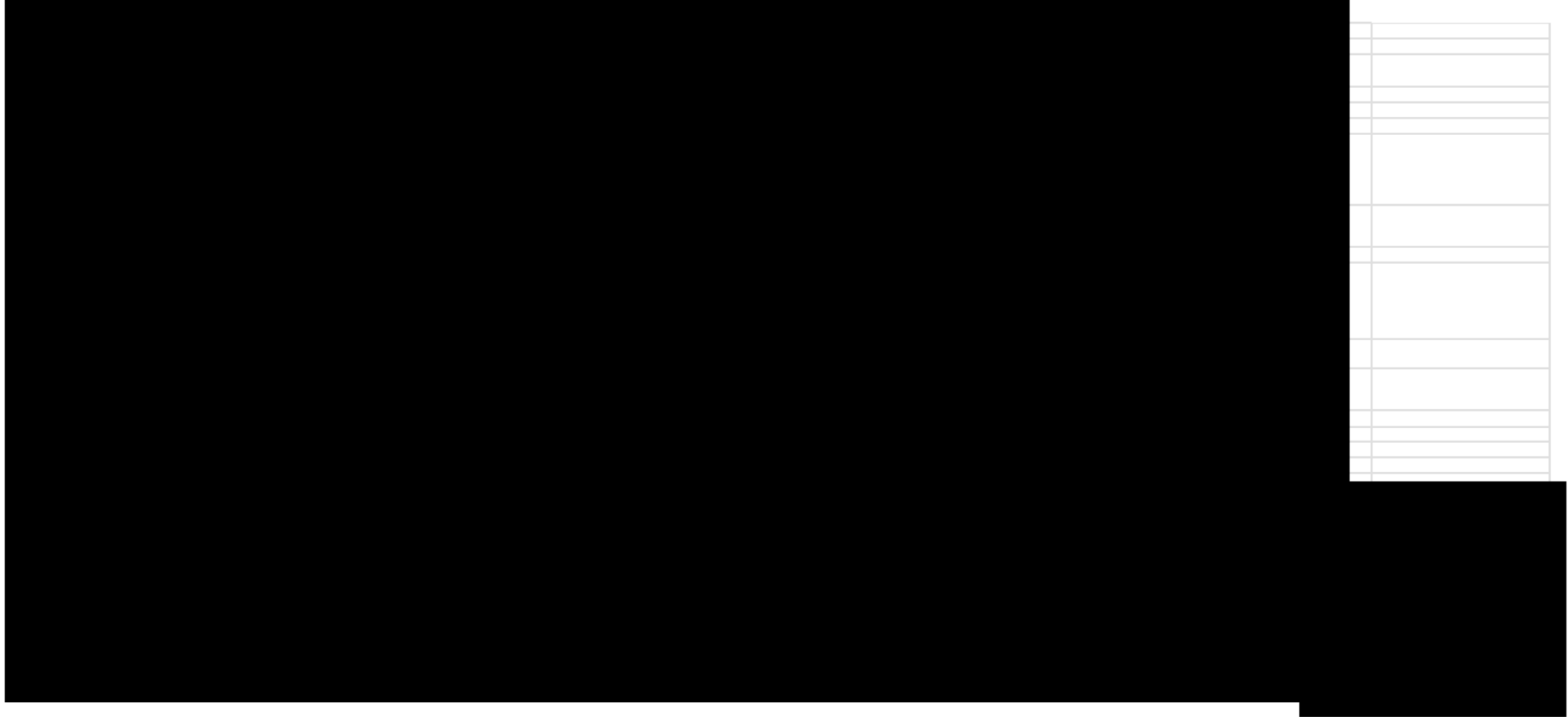
Social value has a lasting impact on individuals, communities, and the environment. The Government has an opportunity and responsibility to maximise benefits effectively and comprehensively through its commercial activity. To be effective, it is essential that the FSA considers social value at all stages of the procurement life cycle. To do this, the FSA is applying the Government Commercial Functions social value model [PPN 06/20 Procurement Policy](#) Note from 1st January 2021. The complete set of documents can be found on the [Social Value webpage](#).

The FSA is invites suppliers to advise how they will meet Theme 4 (Equal Opportunity) Tackle workforce inequality (Model Award Criteria 6.1 - Tackling inequality in the contract workforce) and Model Award Criteria 6.2 - Supporting in-work progression) over the delivery of this contract.



Total Cost for the 1 year contract (excluding VAT)	£ 70,000.00						
Total Cost for the optional 3 year contract (excluding VAT)	£ 210,000.00						







V. Annex 4 – Supplier Tender

Tender Application form for a project with the Food Standards Agency



- Applicants should complete each part of this application as fully and as clearly as possible
- Brief instructions are given in the grey boxes at the start of each section.
- Please submit the application through the Agency's electronic Public Procurement System (Bravo Solutions) by the deadline set in the invitation to tender document.
- Please limit responses to the word limits specified after each question/section.

LEAD APPLICANT'S DETAILS

Surname	Smith	First Name	Andrew	Initial		Title	Bids & Contracts Specialist
Organisation	Info-Tech Research Group	Department	Bids & Contracts				
Street Address	8 Duncannon Street						
Town/City	London	Country	UK	Postcode	WC2N 4JF		
Telephone No	0808 175 3350	E-mail Address	[REDACTED]				
Is your organisation is a small and medium enterprise . (EU recommendation 2003/361/EC refers http://www.hmrc.gov.uk/manuals/cirdmanual/cird92800.htm)			Yes		No	ü	

TENDER SUMMARY

TENDER TITLE

Research and Advisory subscription service

TENDER	C188245
PROPOSED START	4 th September 2023
PROPOSED END	3 rd September 2024

1: DELIVERY OF THE REQUIREMENTS (30%)

Please describe how your offered service will meet the FSA's requirements detailed in the specification.

Info-Tech has reviewed the required specifications and is proposing our CIO Counselor Membership. In addition, we have mapped out each specification to an Info-Tech service being offered as part of our solution in the table below our response.

Info-Tech's CIO Counselor Membership not only delivers on all FSA specifications but provides additional value-added services. The CIO Counselor Membership is our premier membership designed to help CIOs deliver results and improve their effectiveness as a leader. It includes all available content and access to services at Info-Tech. (A table of membership features is provided on page 6 of *Research and Advisory subscription service C188245 - Info-Tech Supporting Document*). We collaborate with clients through our Counselor Services to gain consensus on their priorities and develop and execute personalised plans for success. Leveraging Info-Tech's research and best practices, we provide consultative advisory services and executive coaching. Info-Tech Research Group's CIO Counselor membership provides privileged access to an executive partner ("Counselor") who has deep domain knowledge and focuses 100% of their time on ensuring client value throughout the term of the subscription. Your Counselor will schedule monthly advisory sessions

and be available on demand when you and your delegate need advice and counsel. Four one-day onsite strategy meetings are included. Typically, these full-day sessions are delivered on a quarterly basis. Info-Tech Research Group will ensure that all members of your IT team have access to research materials when required and included in the membership are five "reference" licenses. The reference license provides access to the full suite of research, access to the online academy and access to monthly webinars and training resources. With membership, Info-Tech Research Group will also support you to share and distribute all research internally within your organisation. Your representative will work with your wider team to support access to reference materials where required. There is functionality built into the online portal to enable you to share direct access to resources with your wider team, giving them the ability to download and utilise reference materials. Research is downloadable in a Microsoft format which FSA may utilise as templates, saving time and cost.

With membership your entire organisation will also be able to leverage access to the Academy. The Academy encompasses online training resources created and designed to quickly upskill IT teams, provide up to date information and be used to support personal development. The Academy is not exclusive to license holders of the membership, and Info-Tech would work with you and your learning and development team to help you leverage the maximum from over 45 courses available in the core domains of IT. (See page 8 of *Research and Advisory subscription service C188245 - Info-Tech Supporting Document* for more details of Info-Tech's proposed CIO Counselor Membership).

Info-Tech Research Group will provide unlimited access to diagnostic programmes throughout your membership. Diagnostic programmes are a simple way to collect usable data for your IT department with actionable insights. The diagnostic programmes use low-effort surveys to get data you require from your stakeholders, with experts who will prepare a detailed report for you to present back to the business. Your Counselor will support you with the presentation of the insights and furthermore support with the development and execution of deliverables.

Info-Tech Research Group provides unlimited access to analyst calls and subject matter experts with the CIO Counselor Membership, we welcome you to bring additional members of your team to the analyst calls and these will be booked for you aligning to your timelines, by your Info-Tech Research Group Representative. Membership also includes access to hundreds of software reviews. Software reviews will help you to identify champions in the area you require and rapidly shortlist your alternatives whilst also reviewing leaders in the areas of customer experience, strategy and innovation, contract negotiations, and how they deal with conflicts to find your best partner. Info-Tech Research Group software reviews are provided by members exclusively. Info-Tech Research Group has no input into the content of the reviews and therefore you can be confident that you are making an informed decision with no bias.

The CIO Counselor membership includes access to Info-Tech's IT Spend & Staffing Benchmarking. This service will enable FSA to not only map all IT Staff & Expenditure but will benchmark you against your peers in your industry and understand any subsequent impacts for IT, including helping FSA identify planning and staff optimisation initiatives. The CIO Counselor membership is an investment to save time and effort and provides direct access to additional services such as cost optimisation and expert vendor guidance saving costs on some of the largest spends in the department. This further includes reviews and recommendations of contracts with providers such as Microsoft, Workday, Adobe, etc. Info-Tech's methodology helps you maintain sustainable cost optimisation across IT by focusing on four levers: assets, vendors, project portfolio, and workforce.

Below is a table of each FSA's Specifications and how Info-Tech will address each one with one of our solutions.

FSA Specification

Info-Tech Solution

Support from dedicated expert resource for the FSA's DDaT leadership to guide strategic decision making, risk management, validation, and recommendations on best practice.	Info-Tech will provide FSA with a Dedicated Executive Counselor. FSA will receive personalised and confidential one-on-one support from a seasoned IT executive to achieve their personal/organisational goals, grow as a leader, and prepare for the next chapter of their career. The Executive Counselor will travel to the member's location throughout the year to spend the day working through the member's agenda. The Counselor will address the member's top personal and organisational challenges, presenting relevant research and conducting working sessions.
Guidance on creating a department that operates effectively despite any change in economic circumstance.	FSA's Account Manager will help FSA set up a Custom Key Initiative Plan (CKIP). The CKIP is a fully customised plan of the member's top three to five initiatives mapped to all relevant Info-Tech content and experiences to assist with execution and ensure success.
Opportunities for the DDaT leadership team to discuss specific problems and overall strategy direction with mentors who have worked at a high level in the DDaT field.	As part of the Onsite Counselor Visits, FSA leadership will have the opportunity to discuss specific problems and build an overall strategy using the different tools that are available to FSA as part of the membership.
Online access to resources and onsite access to resources where required.	Info-Tech's online research will be available to FSA 24 hours per day, 365 days per year.
Access to an expert for one to one advice for the Chief Information Officer, access to an analyst for deeper dives one to one advice and five roles to have access reference material.	This service is part of access to the Dedicated Executive Counselor. Access is available to all Info-Tech analysts.
Over the life of the contract the FSA may choose to extend access to the services provided to additional roles. Any such change would be agreed through a variation to contract.	Info-Tech has provided a supplemental document that provides a full overview of services and roles that will be made available during the term of the contract. As part of Info-Tech's dedication to FSA, we are also offering 5-complimentary Reference Membership that will give 5 more people access to Info-Tech Online Research.

<p>Provide access to benchmarking intelligence on major technology contracts (for example: Microsoft Azure, O365, Workday).</p>	<p>Info-Tech knows that ill-defined terms and weak vendor relationships lead to overspending on contracts. To avoid that, an IT organisation needs proven processes to get the right contracts for the organisation while building better vendor relationships. Info-Tech equips our clients with the expert advice and tools required to accomplish this goal by:</p> <ul style="list-style-type: none"> • Knowing the market competitive price for software that is being purchased. • Managing annual maintenance costs. • Improving organisations' contract negotiation skills. • Optimising contract language to meet specific organisational requirements. • Developing a clear understanding of contract terms and conditions. <p>Info-Tech has helped thousands of members negotiate contracts with their vendors. What we have learned along the way provides significant advantages to our clients, enabling them to:</p> <ul style="list-style-type: none"> • Pay less than other purchasers by understanding the competitive price landscape. • Realise significant savings by optimising contract terms. • Right-size contracts to purchase only what is needed, which helps avoid penalties and unforeseen costs. • Future-proof the organisation by building protections into contract terms to avoid price increases. • Maintain a competitive edge by learning how to regularly review and update contracts.
<p>Provide access to resources that will support spend optimisation, providing guidance on potential cost savings, including benchmarks. Suppliers should also provide suggested technical roadmaps with milestones.</p>	<p>Info-Tech has two services we are offering that will address this requirement.</p> <p>IT Cost Analysis & Optimisation: The IT Spend & Staffing Benchmarking report is used to further investigate potential areas of spend and staffing optimisation and form a roadmap to optimise IT spend and staffing within the organisation.</p> <p>IT Spend & Staffing Benchmarking – Online: Info-Tech experts accurately map the member's IT spend and staffing and benchmark against industry peers to build a comprehensive report detailing IT spend and staffing along four perspectives: Expense, Service, Business, and Innovation.</p>
<p>Provide a service to review current contract specifications, performance, and Service Level Agreements/KPI's and suggest improvements.</p>	<p>This is addressed with Info-Tech's Contract Review Service.</p>
<p>Provide unlimited access on demand to subject matter experts who can guide the</p>	<p>Info-Tech has a team of analysts available in house to guide members in process improvement and project management on</p>
<p>DDaT team through complex project delivery. Practical and tactical guidance required and validation of approaches in place will be requested. This needs to cover all the DDaT functions including but not limited to, data architecture, cyber security, service management, cloud optimisation and product management.</p>	<p>technical issues, in addition to strategic and management issues. These analysts are practitioners – they have been CISOs, CIOs, heads of infrastructure, etc., across their careers. Our business model uses subject matter experts who support our clients with their IT issues, primarily process improvements and project management issues. To better understand the experience and qualifications of Info-Tech's analysts available to FSA, please see the biographies listed here: Analyst Biographies.</p>

<p>Provide access to expertise on identifying user needs for software.</p>	<p>Info-Tech provides a best-in-class SoftwareReviews program where real end users provide their feedback on their software experiences. Info-Tech creates a report on solutions within a particular software category (e.g., CRM). Our process eliminates any bias toward vendors and provides real-time data to allow our clients to make informed business decisions based on peer reviews.</p> <p>Info-Tech offers vendor evaluations, SoftwareReviews, and Contract Review Services to help your IT leadership team select software and hardware vendors, maximise contract value, and ensure contract compliance.</p> <p>The vendor evaluations and research are industry specific as well. We have analysts dedicated to major industries, including Government, who publish industry-specific research and provide advice based on their previous work experience in that industry. Info-Tech has also published a Government Reference Architecture. Reference architectures are built based on years of industry expertise and honed by analysts working with real IT professionals in your industry. Leverage industry best practices so you do not waste time and money reinventing the wheel.</p>
<p>Provide access to industry trends, industry benchmarks and resources that will enable Food Standards Agency to optimise practice in alignment with sector.</p>	<p>Info-Tech's Industry Research helps our members explore deep vertical research to gain tailored insights into your industry. New Info-Tech Industry Benchmarking and Roundtables will be available to FSA per the membership levels proposed. For a deeper dive into industry strategies, trends, technologies, and benchmarking, FSA will have access to the industry-specific content offered by our government research and advisory services, as well as access to the full library of industry research, which covers fifty-six industry categories. FSA will be able to connect with industry IT leaders and peers in regular collaboration sessions to tackle pressing industry issues.</p>
<p>Provide a service to help the FSA identify appropriate technology and software options to meet user needs.</p>	<p>This service is captured in Info-Tech SoftwareReviews.</p>
<p>Provide unlimited and unrestricted access to all content including:</p> <ul style="list-style-type: none"> • project and process research • technology reviews • blueprints • tools • off the shelf, reusable templates • diagnostic programmes 	<p>Info-Tech Research Group offers a subscription-based service to provide unlimited access to research and advisory support. Members at FSA will have access to role-specific diagnostics and benchmarking programs, leadership development programs, onsite coaching and project assistance, and support from a dedicated Account Manager, Counselor, and Advisory Team to fully understand their unique goals and business context when leveraging research and support. This service has been provided to ensure your team gets the most out of the subscription and receives measurable value and results. Additional analysts and Executive Advisors will provide support to ensure specific IT expertise is available for each member of the IT executive team. We offer hundreds of do-it-yourself project and process blueprints. In addition, we offer thousands of trend reports, industry notes, reference architectures, toolkits,</p>
	<p>SoftwareReviews reports, benchmarking reports, IT policy templates, toolkits, case studies, and videos developed by our industry experts to help our members save time and money when it comes to tackling their most important IT initiatives.</p>

<p>Provide access to on-demand learning resources for the DDaT team, including but not limited to Security, Data, Risk Management, Infrastructure etc.</p>	<p>FSA's members will have full access to all programs (events, leadership development programs, and webinars) and best-practice content to not only complete projects but also develop as IT professionals. One of the main benefits of using IT research and advisory services is understanding how industry peers are addressing their initiatives and having the resources to tackle new challenges.</p> <p>Info-Tech provides an entire research focus area related to Talent Leadership & Management research specifically targeted to improve your organisation's strategies for leading your IT team effectively. We provide proven resources that will help your team become better managers.</p> <p>In addition, Info-Tech Academy enables your staff to receive training in the 45 core IT processes (based on COBIT). Nine certificates are available and can be achieved by completing the outlined solution sets for each process. We understand that IT departments struggle to develop their staff. This is a unique opportunity to increase the use and value of our IT research service. Each topic is accompanied by webinars and videos with our subject matter experts and IT members.</p>
<p>Give access to industry events and conferences that provide the DDaT team with opportunities to network, share and develop relationships.</p>	<p>Info-Tech provides local events that are organised by your account manager and UK team. Local events will give the DDaT team an opportunity to network with Info-Tech members and other leaders in the industry. FSA will also receive two tickets to the annual Info-Tech symposium (Info-Tech LIVE). Info-Tech Live is the authoritative voice for IT executives making technology decisions and influencing IT innovation. LIVE is your front-row seat to the future of IT with a focus on real, everyday challenges, ensuring that all attendees are engaged, productive, and challenged throughout each session. We have given our members access to all last year's keynotes so you can relive the excitement and revisit the content at your convenience.</p>
<p>Provide tools and content that can be used for awareness raising and communicating key messages to FSA staff.</p>	<p>Info-Tech provides hundreds of tools that make it easy to raise awareness and templates for communicating to the organisation. The majority of our blueprints provide prebuilt PowerPoint presentations that can be edited and presented to leadership or the organisation.</p>
<p>Provide access to a community of other organisations undergoing or have been through similar DDaT improvement initiatives.</p>	<p>Through Info-Tech's Industry Research, we provide Industry Roundtables where similar industries meet to discuss specific subjects that impact their specific industry. Some examples include Cloud Trend, Cloud Services Technology, IT Stakeholder Satisfaction Benchmarking, Cybersecurity Trend, Security Monitoring Technology, etc.</p>
<p>Compliance with UK GDPR regulation</p>	<p>Info-Tech requires very little Personal Identifying Information to be able to provide services. We only require publicly available information including name, role, and email. No other information is required. Info-Tech uses Amazon Web Services in the Republic of Ireland which is subject to GDPR requirements.</p>

2: ORGANISATIONAL EXPERIENCE AND EXPERTISE (10%)

Please describe your organisations experience and expertise in delivering similar services.

Info-Tech is a full-service IT research, advisory, and professional services firm founded in 1997 with over 1,400 full-time employees. Our services include technology-based business research, industry-specific reporting, best-practice methodologies, benchmarking, and market analysis research. Info-Tech offers a practical approach to complex IT and business issues. Our team, including veteran IT professionals and CIOs, works side by side with you and your team in a cooperative approach to deliver results and provide you with the tools needed for continued success. Info-Tech currently provides IT research, advisory, and consultative services to over 40,000 members across the globe.

Info-Tech's membership options provide tailored services for each role and member. Our desire is to exceed expectations in the execution of business-aligned IT strategies, governance, project management, applications, infrastructure, security, business intelligence and various other IT-related disciplines. We work with our clients as subject matter experts, developers, collaborators, and partners connecting with individuals at their pace, not ours. We understand each working environment is unique, and our solutions are therefore not one-size-fits-all.

Info-Tech has a team of analysts available in house to guide members in process improvement and project management on technical issues, in addition to strategic and management issues. These analysts are practitioners – they have been CISOs, CIOs, heads of infrastructure, etc., across their careers. Our business model uses subject matter experts who support our clients with their IT issues, primarily process improvements and project management issues. To better understand the experience and qualifications of Info-Tech's analysts available to FSA, please see the biographies listed here: [Analyst Biographies](#).

Info-Tech uses several formats to effectively present our research, including project blueprints, tools, templates, analyst calls, videos, virtual strategy sessions, webinar events, and virtual workshops. Our focus is to help your organisation navigate critical technology projects through guided implementations. We move beyond reports with innovative, action-based research to drive sustainable IT improvement. We have included several research samples to demonstrate Info-Tech's methodology and ability to meet the task requirements and provide the guidance necessary to address all top IT initiatives and projects of importance to FSA.

Info-Tech possesses one of the largest knowledge bases of advisory toolkits and implementation frameworks on the planet, and it is available to our clients at no additional cost. This includes business case templates, service costing and management frameworks, infrastructure and application reviews, the largest collection of total cost of ownership (TCO) and maturity self-assessment tools, and workshop and facilitation tools for internal IT process improvement initiatives.

Our experience ensures our research and advisory support is driven by best practices from industry peers. After each Info-Tech experience, we ask our members to quantify the real-time savings, monetary impacts, and project improvements our research helped them achieve. This feedback becomes Info-Tech's *Measured Value reports*, which drive our research agenda and ensure we are investing in providing the products and services our members need most. For first-hand accounts of how Info-Tech's services have provided ROI and enabled department improvement for our members overall, please see Info-Tech's sampling of [Measured Value testimonials](#). FSA will notice several Central Government agencies contributed to those Measured Value reports, demonstrating Info-Tech's experience in providing the level of services sought by FSA.

3: ADDED VALUE AND INNOVATION (10%)

Please detail any added value and innovation your offering will provide the FSA.

Info-Tech is providing several additional value-added services not mentioned above including Concierge Service, and 5-complimentary Reference Memberships. Below each one of these value-added services are described.

Info-Tech's Concierge Services are designed with the client's needs in mind first, and we provide valuable experiences tailored to those specific needs. Every Concierge Service is built to provide practical, custom solutions to real pain points experienced by IT leaders. Our analysts will do all the heavy lifting with minimal time commitment on your part. Our subject matter experts will lead the service and produce all final deliverables; we ensure that you will get tangible results fast. From the initial booking to the final handoff, these engagements can be completed in a matter of days. Finally, we provide highly polished deliverables that are ready to use. You will leave each Concierge Service with a set of visually stunning deliverables you will be excited to share and present across the company (See page 23 of *Research and Advisory subscription service C188245 - Info-Tech Supporting Document* for more details of Info-Tech's Concierge Service).

Info-Tech's Reference Membership includes the following:

- Individual role-based access to all research and project methodologies.
- Access to Info-Tech Academy online platform.



(See page 15 of *Research and Advisory subscription service C188245 - Info-Tech Supporting Document* for more details of Info-Tech's Reference Membership).

4. QUALITY MANAGEMENT, SECURITY, DATA PROTECTION AND ACCESSIBILITY (10%)

Please describe how you will meet the FSA's quality, security, data protection and accessibility requirements.

As part of our response, Info-Tech is providing our security package which includes Information Security and Privacy Practices document, our ISACA SOC 2® Type 2 report, our IEC/ISO 27001:2013 certification, NIST Special Publication (SP) 800-171 Revision 1 alignment, and National Cyber Security Centre (NCSC)'s Cyber Essentials Certification. In addition to our Security Package which we believe addresses FSA's quality, security, and data protection, we are providing our VPAT that describes how Info-Tech handles accessibility. In addition, we are providing copies of our Insurance Certificates. More information is provided in *Research and Advisory subscription service C188245 - Info-Tech Supporting Document- Legal Requirements* supporting document.

5. SOCIAL VALUE (10%) -Please note, responses to social value should articulate how you will perform the policy outcomes in delivering the contract, rather than detailing companies CSR policies.

Theme 4: Equal Opportunity.

MAC 6.1 - Demonstrate action to identify and tackle inequality in employment, skills and pay in the contract workforce.

Mac 6.2 - Support in-work progression to help people, including those from disadvantaged or minority groups, to move into higher paid work by developing new skills relevant to the contract.

Using a maximum of 750 words, please describe the commitment your organisation will make to ensure that opportunities under the contract deliver the Policy Outcome and Award Criteria mentioned above.

Please include:

- your 'Method Statement', stating how you will achieve this and how your commitment meets the Award Criteria, and
- a timed project plan and process, including how you will implement your commitment and by when. Also, how you will monitor, measure and report on your commitments/the impact of your proposals. You should include but not be limited to:
 - timed action plan
 - use of metrics
 - tools/processes used to gather data
 - reporting
 - feedback and improvement
 - transparency
- how you will influence staff, suppliers, customers, and communities through the delivery of the contract to support the Policy Outcome, e.g., engagement, co-design/creation, training and education, partnering/collaborating, volunteering.

To align with broader business objectives, Info-Tech is focused on creating and maintaining a collaborative, open-door, idea-forward workplace culture in which everyone's input matters.



The company supports employees from disadvantaged or minority groups in a variety of ways, including maintaining and supporting an internal DEI Committee and providing on-demand access to a Diversity, Equity & Inclusion hub available to all employees via Microsoft Teams. This hub includes a wealth of resources regarding Info-Tech's DEI strategy, as well as information and resources for the Black Professionals at Info-Tech, BIPOC, LGBTQ2IA+, and Women's Employee Resource Groups, which consult with leadership and provide education and insights to the company's various departments. These groups and committees have led to improved diversity, inclusion, and a sense of belonging and support, allowing for open and respectful dialogue in a safe learning environment.

The FY24-26 DEI strategy includes a detailed plan with initiatives and timelines to support and celebrate a diverse workforce. Included are several new programs aimed at supporting disadvantaged and/or minority groups including the RiseUp Women's mentorship program, community engagements activities, and strategic talent acquisition enhancements such as running job postings through inclusive language software.

Our learning and development programs support all employees in our commitment to continuous learning and teaching. The firm provides continuous learning opportunities to employees through its Buy-a-Book and professional development programs, as well as its \$25,000 scholarship program for employees to pursue formal education. Human resources related programs including the annual performance appraisal process, regular coaching conversations, compensation market reviews, and internal job postings promote equality, progression, and development of new skills. Training is also provided to all staff on a regular basis around Anti-Racism, Inclusive Leadership, DEI Foundations, Allyship, and Cultural Sensitivity.

Info-Tech's recruitment strategy, employee engagement, and employee retention are all positively impacted by the firm's corporate culture and organisational priorities and policies. Some of these cultural benefits that support employees include:

- Ability for many positions to work full-time from home / remotely
- Temporary remote work possibilities for international locations
- Promotions from within the company wherever possible
- Collaborative, open, innovative culture
- World class training and a leadership development training program for commercial teams

Some of Info-Tech's achievement metrics related to culture in the past 12 months include:

Being named in the #3 spot as LinkedIn's Top Companies in Canada for 2023, alongside Mastercard, TD, Scotiabank, and Amazon to round out the top five. LinkedIn's annual list is intended to be a resource for professionals at every level and stage of their careers, offering insights on in-demand skills, roles, and industry trends.

Link: <https://www.linkedin.com/pulse/top-companies-2023-25-best-workplaces-grow-your-career-canada/>

In addition, Info-Tech was recently invited to nominate the internal HR department for its Best Culture award category.

To monitor the progress of activities mentioned, regular check ins have been built into strategic plans or program framework. In addition, the company monitors engagement through new hire, monthly, and annual surveys providing employees the ability of two-way communication directly or anonymously with leadership to provide feedback on their employment experience.

ADDITIONAL SUPPORTING DOCUMENTS



Please note that any additional documents in support of the on-line application should be zipped into a single file (using WinZip). These should then be uploaded to Bravo in to the *Supporting Documents* section of the technical envelope. Each supporting document should be clearly marked with the following details:

- the tender reference number,
- the tender title,
- the name of the lead applicant submitting the proposal and
- the part number and title to which the supporting evidence appertains (e.g., Part 3 Deliverables)



VI. Not Used



VII. Short form Terms (“Conditions”)

1. Definitions used in the Contract

In this Contract, unless the context otherwise requires, the following words shall have the following meanings:

“ Affiliates ”	in relation to a body corporate, any other entity which directly or indirectly Controls (in either of the senses defined in sections 450 and 1124 of the Corporation Tax Act 2010 and “ Controlled ” shall be construed accordingly), is Controlled by, or is under direct or indirect common Control of that body corporate from time to time;
“ Audit ”	<p>the Buyer’s right to:</p> <ul style="list-style-type: none"> (a) verify the accuracy of the Charges and any other amounts payable by the Buyer under the Contract (including proposed or actual variations to them in accordance with the Contract); (b) verify the costs of the Supplier (including the costs of all Subcontractors and any third party suppliers) in connection with the provision of the Deliverables; (c) verify the Supplier’s and each Subcontractor’s compliance with the applicable Law; (d) identify or investigate actual or suspected breach of clauses 4 to 35, impropriety or accounting mistakes or any breach or threatened breach of security and in these circumstances the Buyer shall have no obligation to inform the Supplier of the purpose or objective of its investigations; (e) identify or investigate any circumstances which may impact upon the financial stability of the Supplier and/or any Subcontractors or their ability to provide the Deliverables; (f) obtain such information as is necessary to fulfil the Buyer’s obligations to supply information for parliamentary, ministerial, judicial or administrative purposes including the supply of information to the Comptroller and Auditor General; (g) review any books of account and the internal contract management accounts kept by the Supplier in connection with the Contract;



	<p>(h) carry out the Buyer's internal and statutory audits and to prepare, examine and/or certify the Buyer's annual and interim reports and accounts;</p> <p>(i) enable the National Audit Office to carry out an examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Buyer has used its resources;</p>
"Buyer"	the person named as Buyer in the Order Form. Where the Buyer is a Crown Body the Supplier shall be treated as contracting with the Crown as a whole;
"Buyer Cause"	any breach of the obligations of the Buyer or any other default, act, omission, negligence or statement of the Buyer, of its employees, servants, agents in connection with or in relation to the subject-matter of the Contract and in respect of which the Buyer is liable to the Supplier;
"Central Government Body"	<p>a body listed in one of the following sub-categories of the Central Government classification of the Public Sector Classification Guide, as published and amended from time to time by the Office for National Statistics:</p> <p>(a) Government Department;</p> <p>(b) Non-Departmental Public Body or Assembly Sponsored Public Body (advisory, executive, or tribunal);</p> <p>(c) Non-Ministerial Department; or</p> <p>(d) Executive Agency;</p>
"Charges"	the charges for the Deliverables as specified in the Order Form;
"Claim"	any claim which it appears that the Buyer is, or may become, entitled to indemnification under this Contract;
"Compliance Officer"	the person(s) appointed by the Supplier who is responsible for ensuring that the Supplier complies with its legal obligations;
"Conditions"	means these short form terms and conditions of contract;
"Confidential Information"	all information, whether written or oral (however recorded), provided by the disclosing Party to the receiving Party and which (i) is known by the receiving Party to be confidential; (ii) is marked as or stated to be confidential; or (iii) ought



	reasonably to be considered by the receiving Party to be confidential;
"Conflict of Interest"	a conflict between the financial or personal duties of the Supplier or the Supplier Staff and the duties owed to the Buyer under the Contract, in the reasonable opinion of the Buyer;
"Contract"	the contract between (i) the Buyer and (ii) the Supplier which is created by the Supplier's counter signing the Order Form and includes the cover letter (if used), Order Form, these Conditions and the Annexes;
"Controller"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Crown Body"	the government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Government and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies from time to time carrying out functions on its behalf;
"Data Loss Event"	any event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach;
"Data Protection Impact Assessment"	an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data;
"Data Protection Legislation"	(a) the UK GDPR, (b) the DPA 2018; (c) all applicable Law about the processing of personal data and privacy and guidance issued by the Information Commissioner and other regulatory authority; and (d) (to the extent that it applies) the EU GDPR (and in the event of conflict, the UK GDPR shall apply);
"Data Protection Liability Cap"	has the meaning given to it in row 13 of the Order Form;
"Data Protection Officer"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Data Subject"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;



"Data Subject Access Request"	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;
"Date of Delivery"	that date by which the Deliverables must be Delivered to the Buyer, as specified in the Order Form;
"Deliver"	hand over of the Deliverables to the Buyer at the address and on the date specified in the Order Form, which shall include unloading and any other specific arrangements agreed in accordance with clause 4.2. " Delivered " and " Delivery " shall be construed accordingly;
"Deliverables"	means the Goods and/or Services to be supplied under the Contract as set out in the Order Form;
"DPA 2018"	the Data Protection Act 2018;
"EU"	the European Union;
"EU GDPR"	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it has effect in EU law;
"Existing IPR"	any and all intellectual property rights that are owned by or licensed to either Party and which have been developed independently of the Contract (whether prior to the date of the Contract or otherwise);
"Expiry Date"	the date for expiry of the Contract as set out in the Order Form;
"FOIA"	the Freedom of Information Act 2000 together with any guidance and/or codes of practice issued by the Information Commissioner or relevant Government department in relation to such legislation;
"Force Majeure Event"	any event, circumstance, matter or cause affecting the performance by either the Buyer or the Supplier of its obligations arising from: (a) acts, events, omissions, happenings or non-happenings beyond the reasonable control of the Party seeking to claim relief in respect of a Force Majeure Event (the " Affected Party ") which prevent or materially delay the Affected Party from performing its obligations under the Contract;



	<p>(b) riots, civil commotion, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare;</p> <p>(c) acts of a Crown Body, local government or regulatory bodies;</p> <p>(d) fire, flood or any disaster; or</p> <p>(e) an industrial dispute affecting a third party for which a substitute third party is not reasonably available</p> <p>but excluding:</p> <p>(i) any industrial dispute relating to the Supplier, the Supplier Staff (including any subsets of them) or any other failure in the Supplier or the Subcontractor's supply chain;</p> <p>(ii) any event, occurrence, circumstance, matter or cause which is attributable to the wilful act, neglect or failure to take reasonable precautions against it by the Party concerned; and</p> <p>(iii) any failure of delay caused by a lack of funds,</p> <p>and which is not attributable to any wilful act, neglect or failure to take reasonable preventative action by that Party;</p>
"Goods"	the goods to be supplied by the Supplier to the Buyer under the Contract;
"Good Industry Practice"	standards, practices, methods and procedures conforming to the Law and the exercise of the degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged within the relevant industry or business sector;
"Government Data"	(a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, including any of the Buyer's confidential information, and which: (i) are supplied to the Supplier by or on behalf of the Buyer; or (ii) the Supplier is required to generate, process, store or transmit pursuant to the Contract; or (b) any Personal Data for which the Buyer is the Controller;



"Independent Controller"	a party which is Controller of the same Personal Data as the other Party and there is no element of joint control with regards to that Personal Data;
"Information"	has the meaning given under section 84 of the FOIA;
"Information Commissioner"	the UK's independent authority which deals with ensuring information relating to rights in the public interest and data privacy for individuals is met, whilst promoting openness by public bodies;
"Insolvency Event"	in respect of a person: <ul style="list-style-type: none"> (a) if that person is insolvent; (b) where that person is a company, LLP or a partnership, if an order is made or a resolution is passed for the winding up of the person (other than voluntarily for the purpose of solvent amalgamation or reconstruction); (c) if an administrator or administrative receiver is appointed in respect of the whole or any part of the person's assets or business; (d) if the person makes any composition with its creditors; or (e) takes or suffers any similar or analogous action to any of the actions detailed in this definition as a result of debt in any jurisdiction;
"IP Completion Day"	has the meaning given to it in the European Union (Withdrawal Agreement) Act 2020;
"Joint Controller Agreement"	the agreement (if any) entered into between the Buyer and the Supplier substantially in the form set out in <i>Part B – Joint Controller Agreement</i> of Annex 1 – <i>Processing Personal Data</i> ;
"Joint Controllers"	Where two or more Controllers jointly determine the purposes and means of processing;
"Key Staff"	any persons specified as such in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier;
"Law"	any law, subordinate legislation within the meaning of section 21(1) of the Interpretation Act 1978, bye-law, right within the meaning of the European Union (Withdrawal) Act



	2018 as amended by European Union (Withdrawal Agreement) Act 2020, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements of any regulatory body with which the Supplier is bound to comply;
"Month"	a calendar month and " Monthly " shall be interpreted accordingly;
"National Insurance"	contributions required by the Social Security Contributions and Benefits Act 1992 and made in accordance with the Social Security (Contributions) Regulations 2001 (SI 2001/1004);
"New IPR"	all and intellectual property rights in any materials created or developed by or on behalf of the Supplier pursuant to the Contract but shall not include the Supplier's Existing IPR;
"New IPR Items"	means a deliverable, document, product or other item within which New IPR subsists;
"Open Licence"	means any material that is published for use, with rights to access and modify, by any person for free, under a generally recognised open licence including Open Government Licence as set out at http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ and the Open Standards Principles documented at https://www.gov.uk/government/publications/open-standards-principles/open-standards-principles ;
"Order Form"	the order form signed by the Buyer and the Supplier printed above these Conditions;
"Party"	the Supplier or the Buyer (as appropriate) and " Parties " shall mean both of them;
"Personal Data"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Personal Data Breach"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires and includes any breach of Data Protection Legislation relevant to Personal Data processed pursuant to the Contract;
"Prescribed Person"	a legal adviser, an MP or an appropriate body which a whistle-blower may make a disclosure to as detailed in 'Whistleblowing: list of prescribed people and bodies', 24 November 2016, available online at: https://www.gov.uk/government/publications/blowing-the-



	whistle-list-of-prescribed-people-and-bodies--2/whistleblowing-list-of-prescribed-people-and-bodies as updated from time to time;
"Processor"	has the meaning given to it in the UK GDPR or the EU GDPR as the context requires;
"Processor Personnel"	all directors, officers, employees, agents, consultants and suppliers of the Processor and/or of any Subprocessor engaged in the performance of its obligations under the Contract;
"Protective Measures"	<p>technical and organisational measures which must take account of:</p> <ul style="list-style-type: none"> (a) the nature of the data to be protected; (b) harm that might result from Data Loss Event; (c) state of technological development; (d) the cost of implementing any measures; <p>including 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 the such measures adopted by it;</p>
"Purchase Order Number" or "PO Number"	the Buyer's unique number relating to the order for Deliverables to be supplied by the Supplier to the Buyer in accordance with the Contract;
"Rectification Plan"	<p>the Supplier's plan (or revised plan) to rectify its material default which shall include:</p> <ul style="list-style-type: none"> (a) full details of the material default that has occurred, including a root cause analysis; (b) the actual or anticipated effect of the material default; and (c) the steps which the Supplier proposes to take to rectify the material default (if applicable) and to prevent such material default from recurring, including timescales for such steps and for the rectification of the material default (where applicable);
"Regulations"	the Public Contracts Regulations 2015 and/or the Public Contracts (Scotland) Regulations 2015 (as the context



	requires) as amended from time to time;
"Request For Information"	has the meaning set out in the FOIA or the Environmental Information Regulations 2004 as relevant (where the meaning set out for the term "request" shall apply);
"Services"	the services to be supplied by the Supplier to the Buyer under the Contract;
"Specification"	the specification for the Deliverables to be supplied by the Supplier to the Buyer (including as to quantity, description and quality) as specified in the Order Form;
"Staff Vetting Procedures"	vetting procedures that accord with Good Industry Practice or, where applicable, the Buyer's procedures or policies for the vetting of personnel as specified in the Order Form or provided to the Supplier in writing following agreement to the same by the Supplier from time to time;
"Start Date"	the start date of the Contract set out in the Order Form;
"Sub-Contract"	any contract or agreement (or proposed contract or agreement), other than the Contract, pursuant to which a third party: <ul style="list-style-type: none"> (a) provides the Deliverables (or any part of them); (b) provides facilities or services necessary for the provision of the Deliverables (or any part of them); and/or (c) is responsible for the management, direction or control of the provision of the Deliverables (or any part of them);
"Subcontractor"	any person other than the Supplier, who is a party to a Sub-Contract and the servants or agents of that person;
"Subprocessor"	any third party appointed to process Personal Data on behalf of the Processor related to the Contract;
"Supplier"	the person named as Supplier in the Order Form;
"Supplier Staff"	all directors, officers, employees, agents, consultants and contractors of the Supplier and/or of any Subcontractor of the Supplier engaged in the performance of the Supplier's obligations under the Contract;
"Transparency"	In relation to Contracts with a value above the relevant



"Information"	<p>threshold set out in Part 2 of the Regulations only, the content of the Contract, including any changes to this Contract agreed from time to time, as well as any information relating to the Deliverables and performance pursuant to the Contract required to be published by the Buyer to comply with its transparency obligations, including those set out in Public Procurement Policy Note 09/21 (update to legal and policy requirements to publish procurement information on Contracts Finder) (https://www.gov.uk/government/publications/ppn-0921-requirements-to-publish-on-contracts-finder) and Public Procurement Policy Note 01/17 (update to transparency principles) where applicable (https://www.gov.uk/government/publications/procurement-policy-note-0117-update-to-transparency-principles) except for:</p> <ul style="list-style-type: none"> (a) any information which is exempt from disclosure in accordance with the provisions of the FOIA, which shall be determined by the Buyer; and (b) Confidential Information;
"Term"	the period from the Start Date to the Expiry Date as such period may be extended in accordance with clause 11.2 or terminated in accordance with the Contract;
"Third Party IPR"	intellectual property rights owned by a third party which is or will be used by the Supplier for the purpose of providing the Deliverables;
"UK GDPR"	has the meaning as set out in section 3(10) of the DPA 2018, supplemented by section 205(4);
"VAT"	value added tax in accordance with the provisions of the Value Added Tax Act 1994;
"Worker"	any one of the Supplier Staff which the Buyer, in its reasonable opinion, considers is an individual to which Procurement Policy Note 08/15 (Tax Arrangements of Public Appointees) (https://www.gov.uk/government/publications/procurement-policy-note-0815-tax-arrangements-of-appointees) applies in respect of the Deliverables; and
"Working Day"	a day (other than a Saturday or Sunday) on which banks are open for business in the City of London.



2. Understanding the Contract

In the Contract, unless the context otherwise requires:

- 2.1 references to numbered clauses are references to the relevant clause in these Conditions;
- 2.2 any obligation on any Party not to do or omit to do anything shall include an obligation not to allow that thing to be done or omitted to be done;
- 2.3 the headings in this Contract are for information only and do not affect the interpretation of the Contract;
- 2.4 references to "writing" include printing, display on a screen and electronic transmission and other modes of representing or reproducing words in a visible form;
- 2.5 the singular includes the plural and vice versa;
- 2.6 a reference to any Law includes a reference to that Law as amended, extended, consolidated or re-enacted from time to time and to any legislation or byelaw made under that Law;
- 2.7 the word "including", "for example" and similar words shall be understood as if they were immediately followed by the words "without limitation";
- 2.8 any reference which, immediately before IP Completion Day (or such later date when relevant EU law ceases to have effect pursuant to section 1A of the European Union (Withdrawal) Act 2018), is a reference to (as it has effect from time to time):
 - (a) any EU regulation, EU decision, EU tertiary legislation or provision of the EEA agreement ("**EU References**") which is to form part of domestic law by application of section 3 of the European Union (Withdrawal) Act 2018 and which shall be read on and after IP Completion Day as a reference to the EU References as they form part of domestic law by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by domestic law from time to time; and
 - (b) any EU institution or EU authority or other such EU body shall be read on and after IP Completion Day as a reference to the UK institution, authority or body to which its functions were transferred.

3. How the Contract works

- 3.1 The Order Form is an offer by the Buyer to purchase the Deliverables subject to and in accordance with the terms and conditions of the Contract.
- 3.2 The Supplier is deemed to accept the offer in the Order Form when the Buyer receives a copy of the Order Form signed by the Supplier.
- 3.3 The Supplier warrants and represents that its tender (if any) and all statements made and documents submitted as part of the procurement of Deliverables are and remain true and accurate.

4. What needs to be delivered

4.1 All Deliverables

- (a) The Supplier must provide Deliverables: (i) in accordance with the Specification, the tender in Annex 4 – Supplier Tender (where applicable) and the Contract; (ii) using reasonable skill and care; (iii) using Good Industry Practice; (iv) using its own policies, processes and internal quality control measures as long as they don't conflict with the Contract; (v) on the dates agreed; and (vi) that comply with all Law.



- (b) The Supplier must provide Deliverables with a warranty of at least 90 days (or longer where the Supplier offers a longer warranty period to its Buyers) from Delivery against all obvious defects.

4.2 **Goods clauses**

- (a) All Goods delivered must be new, or as new if recycled, unused and of recent origin.
- (b) All manufacturer warranties covering the Goods must be assignable to the Buyer on request and for free.
- (c) The Supplier transfers ownership of the Goods on completion of Delivery (including off-loading and stacking) or payment for those Goods, whichever is earlier.
- (d) Risk in the Goods transfers to the Buyer on Delivery, but remains with the Supplier if the Buyer notices damage following Delivery and lets the Supplier know within 3 Working Days of Delivery.
- (e) The Supplier warrants that it has full and unrestricted ownership of the Goods at the time of transfer of ownership.
- (f) The Supplier must Deliver the Goods on the date and to the location specified in the Order Form, during the Buyer's working hours (unless otherwise specified in the Order Form).
- (g) The Supplier must provide sufficient packaging for the Goods to reach the point of Delivery safely and undamaged.
- (h) All deliveries must have a delivery note attached that specifies the order number, type and quantity of Goods.
- (i) The Supplier must provide all tools, information and instructions the Buyer needs to make use of the Goods.
- (j) The Supplier will notify the Buyer of any request that Goods are returned to it or the manufacturer after the discovery of safety issues or defects that might endanger health or hinder performance and shall indemnify the Buyer against the costs arising as a result of any such request.
- (k) The Buyer can cancel any order or part order of Goods which has not been Delivered. If the Buyer gives less than 14 days' notice then it will pay the Supplier's reasonable and proven costs already incurred on the cancelled order as long as the Supplier takes all reasonable endeavours to minimise these costs.
- (l) The Supplier must at its own cost repair, replace, refund or substitute (at the Buyer's option and request) any Goods that the Buyer rejects because they don't conform with clause 4.2. If the Supplier doesn't do this it will pay the Buyer's costs including repair or re-supply by a third party.
- (m) The Buyer will not be liable for any actions, claims, costs and expenses incurred by the Supplier or any third party during Delivery of the Goods unless and to the extent that it is caused by negligence or other wrongful act of the Buyer or its servant or agent. If the Buyer suffers or incurs any damage or injury (whether fatal or otherwise) occurring in the course of Delivery or installation then the Supplier shall indemnify the Buyer from any losses, charges, costs or expenses which arise as a result of or in connection with such damage or injury where it is attributable to any act or omission of the Supplier or any of its Subcontractors or Supplier Staff.



4.3 **Services clauses**

- (a) Late Delivery of the Services will be a default of the Contract.
- (b) The Supplier must co-operate with the Buyer and third party suppliers on all aspects connected with the delivery of the Services and ensure that Supplier Staff comply with any reasonable instructions including the security requirements (where any such requirements have been provided).
- (c) The Buyer must provide the Supplier with reasonable access to its premises at reasonable times for the purpose of supplying the Services
- (d) The Supplier must at its own risk and expense provide all equipment required to deliver the Services. Any equipment provided by the Buyer to the Supplier for supplying the Services remains the property of the Buyer and is to be returned to the Buyer on expiry or termination of the Contract.
- (e) The Supplier must allocate sufficient resources and appropriate expertise to the Contract.
- (f) The Supplier must take all reasonable care to ensure performance does not disrupt the Buyer's operations, employees or other contractors.
- (g) On completion of the Services, the Supplier is responsible for leaving the Buyer's premises in a clean, safe and tidy condition and making good any damage that it has caused to the Buyer's premises or property, other than fair wear and tear.
- (h) The Supplier must ensure all Services, and anything used to deliver the Services, are of good quality and free from defects.
- (i) The Buyer is entitled to withhold payment for partially or undelivered Services, but doing so does not stop it from using its other rights under the Contract.

5. **Pricing and payments**

- 5.1 In exchange for the Deliverables, the Supplier must invoice the Buyer for the charges in the Order Form.
- 5.2 All Charges:
 - (a) exclude VAT, which is payable on provision of a valid VAT invoice; and
 - (b) include all costs and expenses connected with the supply of Deliverables.
- 5.3 The Buyer must pay the Supplier the charges within 30 days of receipt by the Buyer of a valid, undisputed invoice, in cleared funds to the Supplier's account stated in the invoice or in the Order Form.
- 5.4 A Supplier invoice is only valid if it:
 - (a) includes all appropriate references including the Purchase Order Number and other details reasonably requested by the Buyer; and
 - (b) includes a detailed breakdown of Deliverables which have been delivered.
- 5.5 If there is a dispute between the Parties as to the amount invoiced, the Buyer shall pay the undisputed amount. The Supplier shall not suspend the provision of the Deliverables unless the Supplier is entitled to terminate the Contract for a failure to pay undisputed sums in accordance with clause 11.6. Any disputed amounts shall be resolved through the dispute resolution procedure detailed in clause 37.



5.6 The Buyer may retain or set-off payment of any amount owed to it by the Supplier under this Contract or any other agreement between the Supplier and the Buyer if notice and reasons are provided.

5.7 The Supplier must ensure that all Subcontractors are paid, in full, within 30 days of receipt of a valid, undisputed invoice. If this doesn't happen, the Buyer can publish the details of the late payment or non-payment.

6. The Buyer's obligations to the Supplier

6.1 If Supplier fails to comply with the Contract as a result of a Buyer Cause:

- (a) the Buyer cannot terminate the Contract under clause 11;
- (b) the Supplier is entitled to reasonable and proven additional expenses and to relief from liability under this Contract;
- (c) the Supplier is entitled to additional time needed to deliver the Deliverables; and
- (d) the Supplier cannot suspend the ongoing supply of Deliverables.

6.2 Clause 6.1 only applies if the Supplier:

- (a) gives notice to the Buyer within 10 Working Days of becoming aware;
- (b) demonstrates that the failure only happened because of the Buyer Cause; and
- (c) mitigated the impact of the Buyer Cause.

7. Record keeping and reporting

7.1 The Supplier must ensure that suitably qualified representatives attend progress meetings with the Buyer and provide progress reports when specified in the Order Form.

7.2 The Supplier must keep and maintain full and accurate records and accounts on everything to do with the Contract for 7 years after the date of expiry or termination of the Contract and in accordance with the UK GDPR or the EU GDPR as the context requires.

7.3 The Supplier must allow any auditor appointed by the Buyer access to its premises to verify all contract accounts and records of everything to do with the Contract and provide copies for the Audit.

7.4 During an Audit, the Supplier must provide information to the auditor and reasonable co-operation at their request.

7.5 The Parties will bear their own costs when an Audit is undertaken unless the Audit identifies a material default by the Supplier, in which case the Supplier will repay the Buyer's reasonable costs in connection with the Audit.

7.6 If the Supplier is not providing any of the Deliverables, or is unable to provide them, it must immediately:

- (a) tell the Buyer and give reasons;
- (b) propose corrective action; and
- (c) provide a deadline for completing the corrective action.



- 7.7 If the Buyer, acting reasonably, is concerned as to the financial stability of the Supplier such that it may impact on the continued performance of the Contract then the Buyer may:
- (a) require that the Supplier provide to the Buyer (for its approval) a plan setting out how the Supplier will ensure continued performance of the Contract and the Supplier will make changes to such plan as reasonably required by the Buyer and once it is agreed then the Supplier shall act in accordance with such plan and report to the Buyer on demand; and
 - (b) if the Supplier fails to provide a plan or fails to agree any changes which are requested by the Buyer or fails to implement or provide updates on progress with the plan, terminate the Contract immediately for material breach (or on such date as the Buyer notifies).
- 7.8 If there is a material default, the Supplier must notify the Buyer within 3 Working Days of the Supplier becoming aware of the material default. The Buyer may request that the Supplier provide a Rectification Plan within 10 Working Days of the Buyer's request alongside any additional documentation that the Buyer requires. Once such Rectification Plan is agreed between the Parties (without the Buyer limiting its rights) the Supplier must immediately start work on the actions in the Rectification Plan at its own cost.
- 8. Supplier Staff**
- 8.1 The Supplier Staff involved in the performance of the Contract must:
- (a) be appropriately trained and qualified;
 - (b) be vetted in accordance with the Staff Vetting Procedures; and
 - (c) comply with all conduct requirements when on the Buyer's premises.
- 8.2 Where the Buyer decides one of the Supplier's Staff isn't suitable to work on the Contract, the Supplier must replace them with a suitably qualified alternative.
- 8.3 If requested, the Supplier must replace any person whose acts or omissions have caused the Supplier to breach clause 29.1 to 29.3 .
- 8.4 The Supplier must provide a list of Supplier Staff needing to access the Buyer's premises and say why access is required.
- 8.5 The Supplier indemnifies the Buyer against all claims brought by any person employed or engaged by the Supplier caused by an act or omission of the Supplier or any Supplier Staff.
- 8.6 The Supplier shall use those persons nominated (if any) as Key Staff in the Order Form or otherwise notified as such by the Buyer to the Supplier in writing, following agreement to the same by the Supplier to provide the Deliverables and shall not remove or replace any of them unless:
- (a) requested to do so by the Buyer or the Buyer approves such removal or replacement (not to be unreasonably withheld or delayed);
 - (b) the person concerned resigns, retires or dies or is on parental or long-term sick leave; or
 - (c) the person's employment or contractual arrangement with the Supplier or any Subcontractor is terminated for material breach of contract by the employee.



- 8.7 The Supplier shall ensure that no person who discloses that he/she has a conviction that is relevant to the nature of the Contract, relevant to the work of the Buyer, or is of a type otherwise advised by the Buyer (each such conviction a "**Relevant Conviction**"), or is found by the Supplier to have a Relevant Conviction (whether as a result of a police check, a disclosure and barring service check or otherwise) is employed or engaged in the provision of any part of the Deliverables.

9. Rights and protection

- 9.1 The Supplier warrants and represents that:
- (a) it has full capacity and authority to enter into and to perform the Contract;
 - (b) the Contract is executed by its authorised representative;
 - (c) it is a legally valid and existing organisation incorporated in the place it was formed;
 - (d) there are no known legal or regulatory actions or investigations before any court, administrative body or arbitration tribunal pending or threatened against it or its affiliates that might affect its ability to perform the Contract;
 - (e) all necessary rights, authorisations, licences and consents (including in relation to IPRs) are in place to enable the Supplier to perform its obligations under the Contract and the Buyer to receive the Deliverables;
 - (f) it doesn't have any contractual obligations which are likely to have a material adverse effect on its ability to perform the Contract; and
 - (g) it is not impacted by an Insolvency Event.
- 9.2 The warranties and representations in clause 3.3 and clause 9.1 are repeated each time the Supplier provides Deliverables under the Contract.
- 9.3 The Supplier indemnifies the Buyer against each of the following:
- (a) wilful misconduct of the Supplier, any of its Subcontractor and/or Supplier Staff that impacts the Contract; and
 - (b) non-payment by the Supplier of any tax or National Insurance.
- 9.4 If the Supplier becomes aware of a representation or warranty made in relation to the Contract that becomes untrue or misleading, it must immediately notify the Buyer.
- 9.5 All third party warranties and indemnities covering the Deliverables must be assigned for the Buyer's benefit by the Supplier.

10. Intellectual Property Rights (IPRs)

- 10.1 Each Party keeps ownership of its own Existing IPRs. The Supplier gives the Buyer a non-exclusive, perpetual, royalty-free, irrevocable, transferable worldwide licence to use, change and sub-license the Supplier's Existing IPR to enable the Buyer and its sub-licensees to both:
- (a) receive and use the Deliverables; and
 - (b) use the New IPR.



- 10.2 Any New IPR created under the Contract is owned by the Buyer. The Buyer gives the Supplier a licence to use any Existing IPRs and the New IPR which the Supplier reasonably requires for the purpose of fulfilling its obligations during the Term or using or exploiting the New IPR developed under the Contract.
- 10.3 Where a Party acquires ownership of intellectual property rights incorrectly under this Contract it must do everything reasonably necessary to complete a transfer assigning them in writing to the other Party on request and at its own cost.
- 10.4 Neither Party has the right to use the other Party's intellectual property rights, including any use of the other Party's names, logos or trademarks, except as provided in clause 10 or otherwise agreed in writing.
- 10.5 If any claim is made against the Buyer for actual or alleged infringement of a third party's intellectual property arising out of, or in connection with, the supply or use of the Deliverables (an "**IPR Claim**"), then the Supplier indemnifies the Buyer against all losses, damages, costs or expenses (including professional fees and fines) incurred as a result of the IPR Claim.
- 10.6 If an IPR Claim is made or anticipated the Supplier must at its own expense and the Buyer's sole option, either:
- (a) obtain for the Buyer the rights in clauses 10.1 and 10.2 without infringing any third party intellectual property rights; and
 - (b) replace or modify the relevant item with substitutes that don't infringe intellectual property rights without adversely affecting the functionality or performance of the Deliverables.
- 10.7 The Supplier shall not use in the Delivery of the Deliverables any Third Party IPR unless it has notified the Buyer that the owner or an authorised licensor of the relevant Third Party IPR will grant a direct licence to the Buyer for the Third Party IPR and that licence has been granted. The Buyer, in its absolute discretion, shall have 10 Working Days following the Supplier's notification to reject the grant of the licence. If the Supplier cannot obtain for the Buyer a licence in respect of any Third Party IPR, for whatever reason, the Supplier shall:
- (a) notify the Buyer in writing; and
 - (b) use the relevant Third Party IPR only if the Buyer has provided authorisation in writing, with reference to the acts authorised and the specific intellectual property rights involved.
- 10.8 In spite of any other provisions of the Contract and for the avoidance of doubt, award of this Contract by the Buyer and the ordering of any Deliverable under it does not constitute an authorisation by the Crown under Sections 55 and 56 of the Patents Act 1977, Section 12 of the Registered Designs Act 1949 or Sections 240 – 243 of the Copyright, Designs and Patents Act 1988.
- 11. Ending the contract**
- 11.1 The Contract takes effect on the Start Date and ends on the earlier of the Expiry Date or termination of the Contract, or earlier if required by Law.
- 11.2 The Buyer can extend the Contract where set out in the Order Form in accordance with the terms in the Order Form.
- 11.3 Ending the Contract without a reason**



The Buyer has the right to terminate the Contract at any time without reason or liability by giving the Supplier not less than 90 days' written notice, and if it's terminated clause 11.5(a)(ii) to 11.5(a)(viii) applies.

11.4 When the Buyer can end the Contract

- (a) If any of the following events happen, the Buyer has the right to immediately terminate its Contract by issuing a termination notice in writing to the Supplier:
 - (i) there's a Supplier Insolvency Event;
 - (ii) if the Supplier repeatedly breaches the Contract in a way to reasonably justify the opinion that its conduct is inconsistent with it having the intention or ability to give effect to the terms and conditions of the Contract;
 - (iii) the Supplier is in material breach of any obligation which is capable of remedy, and that breach is not remedied within 30 days of the Supplier receiving notice specifying the breach and requiring it to be remedied;
 - (iv) there's a change of control (within the meaning of section 450 of the Corporation Tax Act 2010) of the Supplier which isn't pre-approved by the Buyer in writing;
 - (v) the Buyer discovers that the Supplier was in one of the situations in 57 (1) or 57(2) of the Regulations at the time the Contract was awarded;
 - (vi) the Supplier or its affiliates embarrass or bring the Buyer into disrepute or diminish the public trust in them; or
 - (vii) the Supplier fails to comply with its legal obligations in the fields of environmental, social, equality or employment Law when providing the Deliverables.
- (b) The Buyer also has the right to terminate the Contract in accordance with clauses 7.7(b), 21.3, 29.4(b), 34.3 and Paragraph 8 of *Part B – Joint Controller Agreement* of Annex 1 – *Processing Personal Data* (if used).
- (c) If any of the events in 73(1) (a) or (b) of the Regulations happen, the Buyer has the right to immediately terminate the Contract and clause 11.5(a)(ii) to 11.5(a)(viii) applies.

11.5 What happens if the Contract ends (Buyer termination)

- (a) Where the Buyer terminates the Contract under clause 11.4(a), 7.7(b), 29.4(b), or Paragraph 8 of *Part B – Joint Controller Agreement* of Annex 1 – *Processing Personal Data* (if used), all of the following apply:
 - (i) the Supplier is responsible for the Buyer's reasonable costs of procuring replacement Deliverables for the rest of the term of the Contract;
 - (ii) the Buyer's payment obligations under the terminated Contract stop immediately;
 - (iii) accumulated rights of the Parties are not affected;
 - (iv) the Supplier must promptly delete or return the Government Data except where required to retain copies by Law;
 - (v) the Supplier must promptly return any of the Buyer's property provided under the Contract;



- (vi) the Supplier must, at no cost to the Buyer, give all reasonable assistance to the Buyer and any incoming supplier and co-operate fully in the handover and re-procurement;
- (vii) the Supplier must repay to the Buyer all the Charges that it has been paid in advance for Deliverables that it has not provided as at the date of termination or expiry; and
- (viii) the following clauses survive the termination of the Contract: 4.2(j), 7, 8.5, 10, 12, 14, 15, 16, 19, 20, 37 and 38 and any clauses which are expressly or by implication intended to continue.

11.6 When the Supplier can end the Contract and what happens when the contract ends (Buyer and Supplier termination)

- (a) The Supplier can issue a reminder notice if the Buyer does not pay an undisputed invoice on time. The Supplier can terminate the Contract if the Buyer fails to pay an undisputed invoiced sum due and worth over 10% of the total Contract value or £1,000, whichever is the lower, within 30 days of the date of the reminder notice.
- (b) Where the Buyer terminates the Contract in accordance with clause 11.3 or the Supplier terminates the Contract under clause 11.6(a) or 24.4:
 - (i) the Buyer must promptly pay all outstanding charges incurred by the Supplier;
 - (ii) the Buyer must pay the Supplier reasonable committed and unavoidable losses as long as the Supplier provides a fully itemised and costed schedule with evidence - the maximum value of this payment is limited to the total sum payable to the Supplier if the Contract had not been terminated; and
 - (iii) clauses 11.5(a)(ii) to 11.5(a)(viii) apply.
- (c) The Supplier also has the right to terminate the Contract in accordance with Clauses 21.3 and 24.4.

11.7 Partially ending and suspending the Contract

- (a) Where the Buyer has the right to terminate the Contract it can terminate or suspend (for any period), all or part of it. If the Buyer suspends the Contract it can provide the Deliverables itself or buy them from a third party.
- (b) The Buyer can only partially terminate or suspend the Contract if the remaining parts of it can still be used to effectively deliver the intended purpose.
- (c) The Parties must agree (in accordance with clause 26) any necessary variation required by clause 11.7, but the Supplier may not either:
 - (i) reject the variation; or
 - (ii) increase the Charges, except where the right to partial termination is under clause 11.3.
- (d) The Buyer can still use other rights available, or subsequently available to it if it acts on its rights under clause 11.7.

12. How much you can be held responsible for

- 12.1 Each Party's total aggregate liability under or in connection with the Contract (whether in tort, contract or otherwise) is no more than 125% of the Charges paid or payable to the Supplier.



12.2 No Party is liable to the other for:

- (a) any indirect losses; and/or
- (b) loss of profits, turnover, savings, business opportunities or damage to goodwill (in each case whether direct or indirect).

12.3 In spite of clause 12.1, neither Party limits or excludes any of the following:

- (a) its liability for death or personal injury caused by its negligence, or that of its employees, agents or Subcontractors;
- (b) its liability for bribery or fraud or fraudulent misrepresentation by it or its employees; or
- (c) any liability that cannot be excluded or limited by Law.

12.4 In spite of clause 12.1, the Supplier does not limit or exclude its liability for any indemnity given under clauses 8.5, 9.3(b), 10.5, or 33.2(b).

12.5 Notwithstanding clause 12.1, but subject to clauses 12.1 and 12.3, the Supplier's total aggregate liability under clause 14.7(e) shall not exceed the Data Protection Liability Cap.

12.6 Each Party must use all reasonable endeavours to mitigate any loss or damage which it suffers under or in connection with the Contract, including any indemnities.

12.7 If more than one Supplier is party to the Contract, each Supplier Party is fully responsible for both their own liabilities and the liabilities of the other Suppliers.

13. Obeying the Law

13.1 The Supplier must, in connection with provision of the Deliverables:

- (a) comply and procure that its Subcontractors comply with the Supplier Code of Conduct: (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779660/20190220-Supplier_Code_of_Conduct.pdf) as such Code of Conduct may be updated from time to time, and such other sustainability requirements as set out in the Order Form;
- (b) comply with the provisions of the Official Secrets Acts 1911 to 1989 and section 182 of the Finance Act 1989;
- (c) support the Buyer in fulfilling its Public Sector Equality duty under section 149 of the Equality Act 2010;
- (d) comply with the model contract terms contained in Example 1 of Annex C of the guidance to PPN 05/19 (Tackling Modern Slavery in Government Supply Chains) shall apply to the Contract, as such clauses may be amended or updated from time to time; and
- (e) meet the applicable Government Buying Standards applicable to Deliverables which can be found online at: <https://www.gov.uk/government/collections/sustainable-procurement-the-government-buying-standards-gbs>.

13.2 The Supplier indemnifies the Buyer against any costs resulting from any default by the Supplier relating to any applicable Law to do with the Contract.

13.3 The Supplier must appoint a Compliance Officer who must be responsible for ensuring that the Supplier complies with Law, clause 13.1 and clauses 28 to 35.



14. Data Protection

- 14.1 The Supplier must not remove any ownership or security notices in or relating to the Government Data.
- 14.2 The Supplier must make accessible back-ups data on regular basis.
- 14.3 The Supplier must ensure that any Supplier system holding any Government Data, including back-up data, is a secure system that complies with the security requirements specified in writing by the Buyer (where any such requirements have been provided).
- 14.4 If at any time the Supplier suspects or has reason to believe that the Government Data is corrupted, lost or sufficiently degraded, then the Supplier must immediately notify the Buyer and suggest remedial action.
- 14.5 If the Government Data is corrupted, lost or sufficiently degraded so as to be unusable the Buyer may either or both:
 - (a) tell the Supplier to restore or get restored Government Data as soon as practical but no later than 5 Working Days from the date that the Buyer receives notice, or the Supplier finds out about the issue, whichever is earlier; and/or
 - (b) restore the Government Data itself or using a third party.
- 14.6 The Supplier must pay each Party's reasonable costs of complying with clause 14.5 unless the Buyer is at fault.
- 14.7 The Supplier:
 - (a) must provide the Buyer with all Government Data in an agreed open format within 10 Working Days of a written request;
 - (b) must have documented processes to guarantee prompt availability of Government Data if the Supplier stops trading;
 - (c) must securely destroy all storage media that has held Government Data at the end of life of that media using Good Industry Practice;
 - (d) securely erase all Government Data and any copies it holds when asked to do so by the Buyer unless required by Law to retain it; and
 - (e) indemnifies the Buyer against any and all losses incurred if the Supplier breaches clause 14 or any Data Protection Legislation.
- 14.8 The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under the Contract dictates the status of each party under the DPA 2018. A Party may act as:
 - (a) "Controller" in respect of the other Party who is "Processor";
 - (b) "Processor" in respect of the other Party who is "Controller";
 - (c) "Joint Controller" with the other Party;
 - (d) "Independent Controller" of the Personal Data where the other Party is also "Controller",



in respect of certain Personal Data under the Contract and shall specify in Part A - *Authorised Processing Template* of Annex 1 – *Processing Personal Data* which scenario they think shall apply in each situation.

14.9 **Where one Party is Controller and the other Party its Processor**

- (a) Where a Party is a Processor, it must only process Personal Data if authorised to do so in Part A - *Authorised Processing Template* of Annex 1 – *Processing Personal Data* by the Controller. Any further written instructions relating to the processing of Personal Data are incorporated into Part A - *Authorised Processing Template* of Annex 1 – *Processing Personal Data*.
- (b) The Processor must give all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment before starting any processing, including:
 - (i) a systematic description of the expected processing and its purpose;
 - (ii) the necessity and proportionality of the processing operations;
 - (iii) the risks to the rights and freedoms of Data Subjects; and
 - (iv) the intended measures to address the risks, including safeguards, security measures and mechanisms to protect Personal Data.
- (c) The Processor must notify the Controller immediately if it thinks the Controller's instructions breach the Data Protection Legislation.
- (d) The Processor must put in place appropriate Protective Measures to protect against a Data Loss Event which must be approved by the Controller.
- (e) If lawful to notify the Controller, the Processor must promptly notify the Controller if the Processor is otherwise required to process Personal Data by Law before processing it.
- (f) The Processor must use all reasonable endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (i) are aware of and comply with the Processor's duties under this clause 14;
 - (ii) are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;
 - (iii) are informed of the confidential nature of the Personal Data and do not provide any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise allowed by the Contract; and
 - (iv) have undergone adequate training in the use, care, protection and handling of Personal Data.
- (g) Where the Personal Data is subject to UK GDPR, the Processor must not transfer Personal Data outside of the UK unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the transfer is in accordance with Article 45 of the UK GDPR (or section 73 of DPA 2018); or
 - (ii) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with UK GDPR Article 46 or section 75 of the DPA 2018) as determined by the Controller which could include relevant parties entering into the International Data Transfer Agreement (the "**IDTA**"), or International Data Transfer Agreement



Addendum to the European Commission's SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time as well as any additional measures determined by the Controller;

- (iii) the Data Subject has enforceable rights and effective legal remedies when transferred;
 - (iv) the Processor meets its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and
 - (v) the Processor complies with the Controller's reasonable prior instructions about the processing of the Personal Data.
 - (vi) Controller hereby grants consent that Supplier may process Personal Data in Ireland, Canada and the United States.
- (h) Where the Personal Data is subject to EU GDPR, the Processor must not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
- (i) the transfer is in accordance with Article 45 of the EU GDPR; or
 - (i) the Controller or Processor has provided appropriate safeguards in relation to the transfer in accordance with Article 46 of the EU GDPR as determined by the Controller which could include relevant parties entering into Standard Contractual Clauses in the European Commission's decision 2021/914/EU or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time as well as any additional measures determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the EU GDPR by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
 - (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the processing of the Personal Data.
 - (j) The Processor must notify the Controller immediately if it:
 - (i) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (ii) receives a request to rectify, block or erase any Personal Data;
 - (iii) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (iv) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Contract;
 - (v) receives a request from any third Party for disclosure of Personal Data where compliance with the request is required or claims to be required by Law; and
 - (vi) becomes aware of a Data Loss Event.



- (k) Any requirement to notify under clause (j) includes the provision of further information to the Controller in stages as details become available.
 - (i) The Processor must promptly provide the Controller with full assistance in relation to any Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause (j). This includes giving the Controller:
 - (ii) full details and copies of the complaint, communication or request;
 - (iii) reasonably requested assistance so that it can comply with a Data Subject Access Request within the relevant timescales in the Data Protection Legislation;
 - (iv) any Personal Data it holds in relation to a Data Subject on request;
 - (v) assistance that it requests following any Data Loss Event; and
 - (vi) assistance that it requests relating to a consultation with, or request from, the Information Commissioner's Office or any other regulatory authority.
- (l) The Processor must maintain full, accurate records and information to show it complies with this clause 14. This requirement does not apply where the Processor employs fewer than 250 staff, unless either the Controller determines that the processing:
 - (i) is not occasional;
 - (ii) includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or
 - (iii) is likely to result in a risk to the rights and freedoms of Data Subjects.
- (m) The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- (n) Before allowing any Subprocessor to process any Personal Data, the Processor must:
 - (i) notify the Controller in writing of the intended Subprocessor and processing;
 - (ii) obtain the written consent of the Controller;
 - (iii) enter into a written contract with the Subprocessor so that this clause 14 applies to the Subprocessor; and
 - (iv) provide the Controller with any information about the Subprocessor that the Controller reasonably requires.
- (o) The Processor remains fully liable for all acts or omissions of any Subprocessor.
- (p) Parties agree to follow requirements of DPA (attached here as Annex 5)
- (q) The Parties agree to take account of any non-mandatory guidance issued by the Information Commissioner's Office or any other regulatory authority.

14.10 Joint Controllers of Personal Data

In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in *Part B – Joint Controller Agreement of Annex 1 – Processing Personal Data*.



14.11 Independent Controllers of Personal Data

In the event that the Parties are Independent Controllers in respect of Personal Data under the Contract, the terms set out in Part C – *Independent Controllers* of Annex 1 – *Processing Personal Data* shall apply to this Contract.

15. What you must keep confidential

15.1 Each Party must:

- (a) keep all Confidential Information it receives confidential and secure;
- (b) not disclose, use or exploit the disclosing Party's Confidential Information without the disclosing Party's prior written consent, except for the purposes anticipated under the Contract; and
- (c) immediately notify the disclosing Party if it suspects unauthorised access, copying, use or disclosure of the Confidential Information.

15.2 In spite of clause 15.1, a Party may disclose Confidential Information which it receives from the disclosing Party in any of the following instances:

- (a) where disclosure is required by applicable Law, a regulatory body or a court with the relevant jurisdiction if the recipient Party notifies the disclosing Party of the full circumstances, the affected Confidential Information and extent of the disclosure;
- (b) if the recipient Party already had the information without obligation of confidentiality before it was disclosed by the disclosing Party;
- (c) if the information was given to it by a third party without obligation of confidentiality;
- (d) if the information was in the public domain at the time of the disclosure;
- (e) if the information was independently developed without access to the disclosing Party's Confidential Information;
- (f) on a confidential basis, to its auditors or for the purposes of regulatory requirements;
- (g) on a confidential basis, to its professional advisers on a need-to-know basis; and
- (h) to the Serious Fraud Office where the recipient Party has reasonable grounds to believe that the disclosing Party is involved in activity that may be a criminal offence under the Bribery Act 2010.

15.3 The Supplier may disclose Confidential Information on a confidential basis to Supplier Staff on a need-to-know basis to allow the Supplier to meet its obligations under the Contract. The Supplier shall remain responsible at all times for compliance with the confidentiality obligations set out in this Contract by the persons to whom disclosure has been made.

15.4 The Buyer may disclose Confidential Information in any of the following cases:

- (a) on a confidential basis to the employees, agents, consultants and contractors of the Buyer;
- (b) on a confidential basis to any other Central Government Body, any successor body to a Central Government Body or any company that the Buyer transfers or proposes to transfer all or any part of its business to;



- (c) if the Buyer (acting reasonably) considers disclosure necessary or appropriate to carry out its public functions;
- (d) where requested by Parliament; and
- (e) under clauses 5.7 and 16.

15.5 For the purposes of clauses 15.2 to 15.4 references to disclosure on a confidential basis means disclosure under a confidentiality agreement or arrangement including terms as strict as those required in clause 15.

15.6 Transparency Information, and Information which is exempt from disclosure by clause 16 is not Confidential Information.

15.7 The Supplier must not make any press announcement or publicise the Contract or any part of it in any way, without the prior written consent of the Buyer and must take all reasonable endeavours to ensure that Supplier Staff do not either.

16. When you can share information

16.1 The Supplier must tell the Buyer within 48 hours if it receives a Request For Information.

16.2 In accordance with a reasonable timetable and in any event within 5 Working Days of a request from the Buyer, the Supplier must give the Buyer full co-operation and information needed so the Buyer can:

- (a) comply with any FOIA request;
- (b) comply with any Environmental Information Regulations (“EIR”) request;
- (c) if the Contract has a value over the relevant threshold in Part 2 of the Regulations, comply with any of its obligations in relation to publishing Transparency Information.

16.3 To the extent that it is allowed and practical to do so, the Buyer will use reasonable endeavours to notify the Supplier of a Request For Information and may talk to the Supplier to help it decide whether to publish information under clause 16. However, the extent, content and format of the disclosure is the Buyer’s decision in its absolute discretion.

17. Insurance

The Supplier shall ensure it has adequate insurance cover for this Contract.

18. Invalid parts of the contract

If any part of the Contract is prohibited by Law or judged by a court to be unlawful, void or unenforceable, it must be read as if it was removed from the Contract as much as required and rendered ineffective as far as possible without affecting the rest of the Contract, whether it’s valid or enforceable.

19. No other terms apply

The provisions incorporated into the Contract are the entire agreement between the Parties. The Contract replaces all previous statements, or agreements whether written or oral. No other provisions apply.



20. Other people's rights in the contract

No third parties may use the Contracts (Rights of Third Parties) Act (“**CRTPA**”) to enforce any term of the Contract unless stated (referring to CRTPA) in the Contract. This does not affect third party rights and remedies that exist independently from CRTPA.

21. Circumstances beyond your control

- 21.1 Any Party affected by a Force Majeure Event is excused from performing its obligations under the Contract while the inability to perform continues, if it both:
- (a) provides written notice to the other Party; and
 - (b) uses all reasonable measures practical to reduce the impact of the Force Majeure Event.
- 21.2 Any failure or delay by the Supplier to perform its obligations under the Contract that is due to a failure or delay by an agent, Subcontractor and/or Supplier Staff will only be considered a Force Majeure Event if that third party is itself prevented from complying with an obligation to the Supplier due to a Force Majeure Event.
- 21.3 Either Party can partially or fully terminate the Contract if the provision of the Deliverables is materially affected by a Force Majeure Event which lasts for 90 days continuously.
- 21.4 Where a Party terminates under clause 21.3:
- (a) each Party must cover its own losses; and
 - (b) clause 11.5(a)(ii) to 11.5(a)(viii) applies.

22. Relationships created by the contract

The Contract does not create a partnership, joint venture or employment relationship. The Supplier must represent themselves accordingly and ensure others do so.

23. Giving up contract rights

A partial or full waiver or relaxation of the terms of the Contract is only valid if it is stated to be a waiver in writing to the other Party.

24. Transferring responsibilities

- 24.1 The Supplier cannot assign, novate or in any other way dispose of the Contract or any part of it without the Buyer's written consent.
- 24.2 The Buyer can assign, novate or transfer its Contract or any part of it to any Crown Body, public or private sector body which performs the functions of the Buyer.
- 24.3 When the Buyer uses its rights under clause 24.2 the Supplier must enter into a novation agreement in the form that the Buyer specifies.
- 24.4 The Supplier can terminate the Contract novated under clause 24.2 to a private sector body that is experiencing an Insolvency Event.
- 24.5 The Supplier remains responsible for all acts and omissions of the Supplier Staff as if they were its own.



25. Supply Chain

- 25.1 The Supplier cannot sub-contract the Contract or any part of it without the Buyer's prior written consent. The Supplier shall provide the Buyer with the name of any Subcontractor the Supplier proposes to engage for the purposes of the Contract. The decision of the Buyer to consent or not will not be unreasonably withheld or delayed. If the Buyer does not communicate a decision to the Supplier within 10 Working Days of the request for consent then its consent will be deemed to have been given. The Buyer may reasonably withhold its consent to the appointment of a Subcontractor if it considers that:
- (a) the appointment of a proposed Subcontractor may prejudice the provision of the Deliverables or may be contrary to its interests;
 - (b) the proposed Subcontractor is unreliable and/or has not provided reliable goods and or reasonable services to its other customers; and/or
 - (c) the proposed Subcontractor employs unfit persons.
- 25.2 If the Buyer asks the Supplier for details about Subcontractors, the Supplier must provide details of all such Subcontractors at all levels of the supply chain including:
- (a) their name;
 - (b) the scope of their appointment; and
 - (c) the duration of their appointment.
- 25.3 The Supplier must exercise due skill and care when it selects and appoints Subcontractors.
- 25.4 The Supplier will ensure that all Sub-Contracts in the Supplier's supply chain entered into after the Start Date wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Contract contain provisions that:
- (a) allow the Supplier to terminate the Sub-Contract if the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law;
 - (b) require the Supplier to pay all Subcontractors in full, within 30 days of receiving a valid, undisputed invoice; and
 - (c) allow the Buyer to publish the details of the late payment or non-payment if this 30-day limit is exceeded.
- 25.5 The Supplier will take reasonable endeavours to ensure that all Sub-Contracts in the Supplier's supply chain entered into before the Start Date but made wholly or substantially for the purpose of performing or contributing to the performance of the whole or any part of this Contract contain provisions that:
- (a) allow the Supplier to terminate the Sub-Contract if the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law;
 - (b) require the Supplier to pay all Subcontractors in full, within 30 days of receiving a valid, undisputed invoice; and
 - (c) allow the Buyer to publish the details of the late payment or non-payment if this 30-day limit is exceeded.



- 25.6 At the Buyer's request, the Supplier must terminate any Sub-Contracts in any of the following events:
- (a) there is a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 of a Subcontractor which isn't pre-approved by the Buyer in writing;
 - (b) the acts or omissions of the Subcontractor have caused or materially contributed to a right of termination under Clause 11.4;
 - (c) a Subcontractor or its Affiliates embarrasses or brings into disrepute or diminishes the public trust in the Buyer;
 - (d) the Subcontractor fails to comply with its obligations in respect of environmental, social, equality or employment Law; and/or
 - (e) the Buyer has found grounds to exclude the Subcontractor in accordance with Regulation 57 of the Regulations.
- 25.7 The Supplier is responsible for all acts and omissions of its Subcontractors and those employed or engaged by them as if they were its own.
- 26. Changing the contract**
- Either Party can request a variation to the Contract which is only effective if agreed in writing and signed by both Parties. The Buyer is not required to accept a variation request made by the Supplier.
- 27. How to communicate about the contract**
- 27.1 All notices under the Contract must be in writing and are considered effective on the Working Day of Delivery as long as they're delivered before 5:00pm on a Working Day. Otherwise the notice is effective on the next Working Day. An email is effective at 9am on the first Working Day after sending unless an error message is received.
- 27.2 Notices to the Buyer or Supplier must be sent to their address or email address in the Order Form.
- 27.3 This clause does not apply to the service of legal proceedings or any documents in any legal action, arbitration or dispute resolution.
- 28. Dealing with claims**
- 28.1 If the Buyer becomes aware of any Claim, the Buyer must:
- (a) notify the Supplier as soon as reasonably practical becoming aware of a Claim;
 - (b) at the Supplier's cost, allow the Supplier to conduct all negotiations and proceedings to do with a Claim;
 - (c) at the Supplier's cost, give the Supplier reasonable assistance with the Claim if requested; and
 - (d) not make admissions about the Claim without the prior written consent of the Supplier which cannot be unreasonably withheld or delayed.
- 28.2 The Supplier must:
- (a) consider and defend the Claim diligently and in a way that does not damage the Buyer's reputation; and



- (b) not settle or compromise any Claim without the Buyer's prior written consent which it must not unreasonably withhold or delay.

29. Preventing fraud, bribery and corruption

29.1 The Supplier shall not:

- (a) commit any criminal offence referred to in 57(1) and 57(2) of the Regulations; or
- (b) offer, give, or agree to give anything, to any person (whether working for or engaged by the Buyer or any other public body) an inducement or reward for doing, refraining from doing, or for having done or refrained from doing, any act in relation to the obtaining or execution of the Contract or any other public function or for showing or refraining from showing favour or disfavour to any person in relation to the Contract or any other public function.

29.2 The Supplier shall take all reasonable endeavours (including creating, maintaining and enforcing adequate policies, procedures and records), in accordance with Good Industry Practice, to prevent any matters referred to in clause 29.1 and any fraud by the Supplier Staff and the Supplier (including its shareholders, members and directors) in connection with the Contract and shall notify the Buyer immediately if it has reason to suspect that any such matters have occurred or is occurring or is likely to occur.

29.3 If the Supplier notifies the Buyer as required by clause 29.2, the Supplier must respond promptly to their further enquiries, co-operate with any investigation and allow the Audit of any books, records and relevant documentation.

29.4 If the Supplier or the Supplier Staff engages in conduct prohibited by clause 29.1 or commits fraud in relation to the Contract or any other contract with the Crown (including the Buyer) the Buyer may:

- (a) require the Supplier to remove any Supplier Staff from providing the Deliverables if their acts or omissions have caused the default; and
- (b) immediately terminate the Contract.

30. Equality, diversity and human rights

30.1 The Supplier must follow all applicable employment and equality Law when they perform their obligations under the Contract, including:

- (a) protections against discrimination on the grounds of race, sex, gender reassignment, religion or belief, disability, sexual orientation, pregnancy, maternity, age or otherwise; and
- (b) any other requirements and instructions which the Buyer reasonably imposes related to equality Law.

30.2 The Supplier must use all reasonable endeavours, and inform the Buyer of the steps taken, to prevent anything that is considered to be unlawful discrimination by any court or tribunal, or the Equality and Human Rights Commission (or any successor organisation) when working on the Contract.

31. Health and safety

31.1 The Supplier must perform its obligations meeting the requirements of:

- (a) all applicable Law regarding health and safety; and
- (b) the Buyer's current health and safety policy while at the Buyer's premises, as provided to the Supplier.



31.2 The Supplier and the Buyer must as soon as possible notify the other of any health and safety incidents or material hazards they're aware of at the Buyer premises that relate to the performance of the Contract.

32. Environment and sustainability

32.1 In performing its obligations under the Contract, the Supplier shall, to the reasonable satisfaction of the Buyer:

- (a) meet, in all material respects, the requirements of all applicable Laws regarding the environment; and
- (b) comply with its obligations under the Buyer's current environmental policy, which the Buyer must provide.

32.2 The Supplier must ensure that Supplier Staff are aware of the Buyer's environmental policy.

33. Tax

33.1 The Supplier must not breach any tax or social security obligations and must enter into a binding agreement to pay any late contributions due, including where applicable, any interest or any fines. The Buyer cannot terminate the Contract where the Supplier has not paid a minor tax or social security contribution.

33.2 Where the Supplier or any Supplier Staff are liable to be taxed or to pay National Insurance contributions in the UK relating to payment received under the Contract, the Supplier must both:

- (a) comply with the Income Tax (Earnings and Pensions) Act 2003 and all other statutes and regulations relating to income tax, the Social Security Contributions and Benefits Act 1992 (including IR35) and National Insurance contributions; and
- (b) indemnify the Buyer against any Income Tax, National Insurance and social security contributions and any other liability, deduction, contribution, assessment or claim arising from or made during or after the Term in connection with the provision of the Deliverables by the Supplier or any of the Supplier Staff.

33.3 If any of the Supplier Staff are Workers who receive payment relating to the Deliverables, then the Supplier must ensure that its contract with the Worker contains requirements that:

- (a) the Buyer may, at any time during the term of the Contract, request that the Worker provides information which demonstrates they comply with clause 33.2, or why those requirements do not apply, the Buyer can specify the information the Worker must provide and the deadline for responding;
- (b) the Worker's contract may be terminated at the Buyer's request if the Worker fails to provide the information requested by the Buyer within the time specified by the Buyer;
- (c) the Worker's contract may be terminated at the Buyer's request if the Worker provides information which the Buyer considers isn't good enough to demonstrate how it complies with clause 33.2 or confirms that the Worker is not complying with those requirements; and
- (d) the Buyer may supply any information they receive from the Worker to HMRC for revenue collection and management.



34. Conflict of interest

- 34.1 The Supplier must take action to ensure that neither the Supplier nor the Supplier Staff are placed in the position of an actual, potential or perceived Conflict of Interest.
- 34.2 The Supplier must promptly notify and provide details to the Buyer if an actual, potential or perceived Conflict of Interest happens or is expected to happen.
- 34.3 The Buyer will consider whether there are any appropriate measures that can be put in place to remedy an actual, perceived or potential Conflict of Interest. If, in the reasonable opinion of the Buyer, such measures do not or will not resolve an actual or potential conflict of interest, the Buyer may terminate the Contract immediately by giving notice in writing to the Supplier where there is or may be an actual or potential Conflict of Interest and clauses 11.5(a)(ii) to 11.5(a)(viii) shall apply.

35. Reporting a breach of the contract

- 35.1 As soon as it is aware of it the Supplier and Supplier Staff must report to the Buyer any actual or suspected breach of Law, clause 13.1, or clauses 28 to 34.
- 35.2 The Supplier must not retaliate against any of the Supplier Staff who in good faith reports a breach listed in clause 35.1 to the Buyer or a Prescribed Person.

36. Further Assurances

Each Party will, at the request and cost of the other Party, do all things which may be reasonably necessary to give effect to the meaning of this Contract.

37. Resolving disputes

- 37.1 If there is a dispute between the Parties, their senior representatives who have authority to settle the dispute will, within 28 days of a written request from the other Party, meet in good faith to resolve the dispute by commercial negotiation.
- 37.2 If the dispute is not resolved at that meeting, the Parties can attempt to settle it by mediation using the Centre for Effective Dispute Resolution ("CEDR") Model Mediation Procedure current at the time of the dispute. If the Parties cannot agree on a mediator, the mediator will be nominated by CEDR. If either Party does not wish to use, or continue to use mediation, or mediation does not resolve the dispute, the dispute must be resolved using clauses 37.3 to 37.5.
- 37.3 Unless the Buyer refers the dispute to arbitration using clause 37.4, the Parties irrevocably agree that the courts of England and Wales have the exclusive jurisdiction to:
 - (a) determine the dispute;
 - (b) grant interim remedies; and
 - (c) grant any other provisional or protective relief.
- 37.4 The Supplier agrees that the Buyer has the exclusive right to refer any dispute to be finally resolved by arbitration under the London Court of International Arbitration Rules current at the time of the dispute. There will be only one arbitrator. The seat or legal place of the arbitration will be London and the proceedings will be in English.



37.5 The Buyer has the right to refer a dispute to arbitration even if the Supplier has started or has attempted to start court proceedings under clause 37.3, unless the Buyer has agreed to the court proceedings or participated in them. Even if court proceedings have started, the Parties must do everything necessary to ensure that the court proceedings are stayed in favour of any arbitration proceedings if they are started under clause 37.4.

37.6 The Supplier cannot suspend the performance of the Contract during any dispute.

38. Which law applies

This Contract and any issues or disputes arising out of, or connected to it, are governed by English law.



Annex 5 – DPA

DATA PROCESSING ADDENDUM

This Data Processing Addendum (this “**DPA**”) is effective as of the date of the last signature below (the “**Effective Date**”) and is between the Info-Tech legal entity identified in Article 14 (“Info-Tech Signatory”) including McLean & Company as a division thereof (“**Info-Tech**”) and the client legal entity identified in the signature page below (the “**Client**”) (each a “**Party**” or together the “**Parties**”). This DPA governs the Processing of Personal Data by Info-Tech in providing services to the Client (the “**Services**”) pursuant to the definitive services agreement between Info-Tech and the Client, including any quotation documents, order forms, statements of work, or similar documents thereunder (the “**Agreement**”). This DPA forms an integral part of and is hereby incorporated into the Agreement. To the extent of any conflict between this DPA and the Agreement, this DPA has precedence.

1. Definitions

1.1 Any capitalized terms not otherwise defined in this DPA have the following meanings:

- (a) “**Audit Report**” means a certificate or report of an external auditor not older than eighteen (18) months that the security controls of Info-Tech are in accordance with SOC 2 Type II, ISO/IEC 27001:2013, or similar industry standard.
- (b) “**Authentication Credentials**” means membership account credentials including usernames and passwords.
- (c) “**CCPA**” means the California Consumer Privacy Act of 2018 (California Civil Code, Title 1.81.5 §§ 1798.100 – 1798.199).
- (d) “**Controller**” means the party that determines the purposes and means of Processing of Personal Data and is inclusive of the term “Controller” as defined in the GDPR and the term “Business” as defined in the CCPA.
- (e) “**Data Protection Laws**” means all laws, regulations, and other legally enforceable requirements of a governmental or supervisory authority directly applicable to the Processing of Personal Data.
- (f) “**Data Subject**” means an identified or identifiable natural person and is inclusive of the term “Data Subject” as defined in the GDPR and the term “Consumer” as defined in the CCPA.
- (g) “**Data Subject Requests**” means a request by a Data Subject to exercise his or her rights under Data Protection Laws.
- (h) “**European Personal Data**” means Personal Data that originates from a Data Subject in the European Economic Area, Switzerland, or the United Kingdom.
- (i) “**GDPR**” means the General Data Protection Regulation (Regulation (EU) 2016/679) of the European Parliament and of the Council of 27 April 2016.
- (j) “**Info-Tech Group**” means (i) Info-Tech Research Group Inc, a Canada corporation the principal office and place of business of which is 345 Ridout Street North, London, Ontario, Canada N6A 2N8 (ii) Info-Tech Research Group Inc, a Delaware corporation the principal office and place of business of which is 3960 Howard Hughes Parkway, Suite 500, Las Vegas, Nevada, United States of America 89169; (iii) Info-Tech Research Group Ltd, a United Kingdom corporation the principal office and place of business of which is Golden Cross House, 8 Duncannon Street, London, United Kingdom WC2N 4JF; and (iv) Info-Tech Research Group Pty Ltd, an Australia company the principal office and place of business of which is Level 3, 100 Harris Street, Sydney, New South Wales, Australia 2009.



- (k) **“Personal Data”** means any information relating to a Data Subject Processed by Info-Tech on behalf of Client in providing the Services and is inclusive of the term “Personal Information” as defined in each PIPEDA and the CCPA and the term “Personal Data” as defined in the GDPR.
- (l) **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, non-public Personal Data transmitted, stored or otherwise processed in the provision of the Services and that creates a real risk of significant harm to a Data Subject, except to the extent such breach is caused by the Client or Client users.
- (m) **“PIPEDA”** means the Personal Information Protection and Electronic Documents Act (Canada) SC 2000, c 5.
- (n) **“Privacy Contact Person”** means the individual assigned as such by a Party under Article 7 (“Privacy Contact Person”) of this DPA.
- (o) **“Processing”** means any operation or set of operations which is performed upon Personal Data or sets of Personal Data and is inclusive of “Processing” as defined in each the GDPR and CCPA; and “Process”, “Processes”, and “Processed” have corresponding meanings.
- (p) **“Processor”** means the party that processes Personal Data on behalf of the Controller and is inclusive of “Processor” as defined in the GDPR and the term “Service Provider” as defined in the CCPA.
- (q) **“Standard Contractual Clauses”** means (i) the standard contractual clauses adopted by European Commission or equivalent European Union supervisory authority for transfers of personal data to third countries, as amended or replaced from time to time; and (ii) as applicable, the UK Addendum.
- (r) **“Sub-processor”** means any Info-Tech service provider or subcontractor that sub-Processes Personal Data in supporting the provision or delivery of the Services.
- (s) **“UK Addendum”** means the International Transfer Addendum to the Standard Contractual Clauses issued by the United Kingdom Information Commissioner under the UK DPA 2018 and UK GDPR.
- (t) **“UK DPA 2018”** means the United Kingdom Data Protection Act 2018 (c 12).
- (u) **“UK GDPR”** means the retained EU law version of the GDPR, within the laws of England and Wales, Scotland, and Northern Ireland.

2. Processing of Personal Data

- 2.1 With respect to the Processing of Personal Data the Client is the Controller and Info-Tech is the Processor.
- 2.2 The Client shall comply with any requirements under Data Protection Laws to provide notice to and obtain consents of Data Subjects to use Info-Tech as a Processor. The Client shall be solely responsible for the means by which the Client collects Personal Data and for the accuracy, quality, and legality of such Personal Data.
- 2.3 Info-Tech shall Process Personal Data in accordance with (a) Data Protection Laws; and (b) the instructions of the Client as set out in this DPA or the Agreement. The Client hereby instructs Info-Tech to Process Personal Data for purposes of providing the Services and in accordance with this DPA. Any purported instructions of the Client that do not comply with Data Protection Laws (or that if followed would cause Info-Tech to not comply with Data Protection Laws) shall be void and of no effect. Info-Tech shall not take any action that would reasonably be considered a “Sale” of Personal Data within the meaning of the CCPA.



- 2.4** Set out on Annex A is an initial record of Processing activities including categories of Data Subjects and Personal Data, and the purposes of the Processing.
- 2.5** Set out on Annex B are technical and organizational measures that Info-Tech presently maintains. Info-Tech may adapt or improve such technical and organizational measures from time to time in response to developments in technology, industry standards, applicable law, and otherwise; provided, that the technical and organizational measures shall, in accordance with the GDPR, at all times present an appropriate level of security having regard to the costs of implementation in relation to the risks and nature of the Personal Data.
- 2.6** Info-Tech maintains SOC 2 Type II, ISO/IEC 27001:2013, and NCSC Cyber Essentials certifications, made available to clients in accordance with the terms and conditions of Article 9 (“Compliance Assistance and Audits”). Info-Tech is NIST SP 800-171 r1 aligned.
- 2.7** Info-Tech shall not disclose Personal Data to any third party outside the Info-Tech Group, except (a) as the Client instructs; (b) as provided in the Agreement; (c) to authorized Sub-processors in accordance with this DPA; or (d) as required by applicable law or other mandatory governmental process.
- 2.8** Info-Tech shall only disclose Personal Data to those employees and personnel within the Info-Tech Group who are subject to contractual or professional obligations to maintain the security and confidentiality of Personal Data appropriate to the risks and nature of the Personal Data.
- 3. Data Subject Requests**
- 3.1** The Client as Controller shall comply with any requirements under Data Protection Laws to provide notice to Data Subjects of rights in relation to Data Subject Requests.
- 3.2** If a Data Subject Request is made to Info-Tech directly, Info-Tech shall, unless otherwise required by Data Protection Laws, direct such Data Subject to the Client, and the Client shall inform the Data Subject that he may exercise his rights solely through the Client. The Client shall respond to and facilitate Data Subject Requests in accordance with Data Protection Laws.
- 3.3** If Info-Tech notifies the Client of any Data Subject Request or Personal Data Breach in accordance with this DPA, the Client shall further notify any other relevant Controller; provided that Info-Tech shall reserve the right to direct any such notifications to such other relevant Controller directly, if required by Data Protection Laws.
- 4. Deletion of Personal Data**
- 4.1** Subsequent to the termination of the Agreement or upon the earlier written request of the Client, Info-Tech shall, unless otherwise required by applicable law, delete or anonymize Personal Data on its systems; provided, that Info-Tech may retain (a) backup copies of Personal Data made pursuant to its regular archival practices so long as such copies are not readily accessible to Info-Tech employees or personnel; and (b) documents containing Personal Data as are held by its internal legal department or external counsel for legal retention purposes; and (c) any Personal Data as it may be required to retain under applicable law. The Client acknowledges that a request to delete or anonymize Personal Data before the termination of the Agreement may interfere with the provision of the Services, and that Info-Tech shall have no responsibility for the same.
- 5. Location of Processing**
- 5.1** Info-Tech may Process Personal Data in any country in which Info-Tech, any member of the Info-Tech Group or any authorized Sub-processor maintains systems used in connection with the performance of the Services. Any transfer of Personal Data by Info-



Tech from one territorial jurisdiction to another (the EU constituting a single jurisdiction for purposes of this Article) will, in any case, only be undertaken in compliance with Data Protection Laws. If a transfer of European Personal Data is made from the EU or UK to a country outside the EU or UK not subject to an adequacy decision under the GDPR or applicable UK Data Protection Laws, the Client (as data exporter) and Info-Tech (as data importer) will be deemed to have entered into the Standard Contractual Clauses (including, for the avoidance of doubt, the UK Addendum as applicable); provided that if the Client's Personal Data includes European Personal Data, the Client will have given Info-Tech prior written notice thereof. To the extent of any conflict between this DPA and such Standard Contractual Clauses, the Standard Contractual Clauses have precedence. The Standard Contractual Clauses will be deemed to contain the information set out on Annex C, as applicable.

6. Sub-Processing

- 6.1** The Client authorizes Info-Tech to engage third party Sub-processors to support the provision of the Services, provided that (a) any transfer of Personal Data to any such Sub-processor is performed in accordance with this Article, any Standard Contractual Clauses between the Client and Info-Tech, and Data Protection Laws; and (b) Info-Tech will have entered into a written agreement any such Sub-processor imposing data protection obligations appropriate to the risks and nature of the relevant Personal Data. Notwithstanding the engagement of any Sub-processor, Info-Tech will remain primarily responsible to the Client for its obligations under this DPA.
- 6.2** If required by Data Protection Laws, Info-Tech shall, upon the written request of the Client, make available to the Client a list of third party Sub-processors. The Client acknowledges that such list may be made available through a hyperlink to a dedicated page on the Info-Tech website, and that any change to the list from time to time concerning the addition or replacement of a Sub-processor shall be deemed to constitute notice thereof. If the Client reasonably objects to Processing of Personal Data by an additional Sub-processor, the Client shall notify Info-Tech in writing within fourteen (14) calendar days after the date on which notice of such additional Sub-processor is given in accordance with the foregoing sentence. Info-Tech shall use commercially reasonable efforts to change the affected Services to avoid the Processing by the additional Sub-processor. If Info-Tech is unable to implement such change within fourteen (14) calendar days, the Client may, upon further fourteen (14) calendar days' written notice, terminate the Agreement only with respect to those Services that cannot be provided by Info-Tech without the use of the additional Sub-processor, and such termination shall be the sole and exclusive remedy of the Client with respect to use of the additional Sub-processor. For the avoidance of doubt, to the extent of any conflict between this Article and any Standard Contractual Clauses between the Parties, the Standard Contractual Clauses shall have precedence.

7. Privacy Contact Person

- 7.1** The Parties shall each appoint a Privacy Contact Person responsible for privacy matters under this DPA, including, where required by Data Protection Laws, a data protection officer.

For Info-Tech:
 Chief Privacy Officer
legal@infotech.com
 345 Ridout Street North, London, ON Canada N6A 2N8

- 7.2** Upon the Effective Date, the Client may designate in writing a Privacy Contact Person by notice to Info-Tech's Privacy Contact Person (identified above). In the event the Client does not designate a Privacy Contact Person in accordance with this Article, Info-Tech may use other contact information on file (for example, the email address of a Client representative with whom Info-Tech customarily communicates) to issue notification or other communications and such notifications or communications shall be deemed to have been made to the Client's Privacy Contact Person.



- 7.3** Subject to the foregoing, any notification required by or made pursuant to this DPA, including a Personal Data Breach notification, may be delivered to the Client's Privacy Contact Persons by email. The Client shall be responsible for timely notifying Info-Tech of any changes to the contact information of its Privacy Contact Person.

8. Personal Data Breach

- 8.1** Info-Tech shall notify Client within forty-eight (48) hours after becoming aware of any actual or reasonably suspected Personal Data Breach.
- 8.2** Info-Tech shall (i) investigate any Personal Data Breach without delay; (ii) make reasonable efforts to keep the Client informed of the progress of the investigation; and (iii) take commercially reasonable measures to minimize the effects of the Personal Data Breach. Info-Tech shall provide reasonable assistance to the Client with respect to any notifications required under Data Protection Laws, including, as the case may be, assistance in preparing notifications to the relevant supervisory or regulatory authority (for example, by providing the Client a description of the Personal Data Breach). In the event the Client determines that the relevant supervisory or regulatory authority is required to be notified of the Personal Data Breach under Data Protection Laws then, if and to the extent the notification the Client proposes to refer to Info-Tech in a notification, Info-Tech shall have the right to review and approve the notification, provided that such approval shall not be unreasonably withheld, conditioned, or delayed.
- 8.3** Any notice or investigation of a Personal Data Breach by Info-Tech shall not be deemed an acknowledgement of any fault or liability with respect to the Personal Data Breach.
- 8.4** The Client shall notify Info-Tech without undue delay of any actual or reasonably suspected unauthorized access to its user accounts or Authentication Credentials.

9. Compliance Assistance and Audits

- 9.1** Info-Tech shall provide such commercially reasonable assistance to the Client as the Client may request with respect to records of processing and data impact assessments as may be required under the GDPR.
- 9.2** To the extent legally permitted, Info-Tech shall promptly notify the Client if Info-Tech receives any request for inspection or audit or any inquiry or legal process from a competent supervisory or regulatory authority relating to the Processing. Info-Tech shall provide such commercially reasonable assistance as the Client may request with respect to such request, inquiry, or process.
- 9.3** The Client may from time to time request an Audit Report (which Info-Tech will provide through secure file sharing means). The Audit Report shall be deemed the Confidential Information of Info-Tech in accordance with the confidentiality provisions of the Agreement (or, if the Agreement contains no such provisions or such provisions are not applicable to the information of Info-Tech or the Audit Report in particular, the right of the Client to receive the Audit Report pursuant to this paragraph shall be deemed conditional upon the Parties entering into an appropriate confidentiality and non-disclosure agreement with respect to the Audit Report in form and substance satisfactory to Info-Tech acting reasonably) and the Audit Report shall not be used by the Client for any purpose except assessment of Info-Tech's compliance with Data Protection Laws.
- 9.4** To the extent the Client has a right to do so under Data Protection Laws, the Client may at its sole expense audit, or instruct reputable audit professionals who are not competitors of Info-Tech (and who are bound by written obligations of confidentiality in form and substance satisfactory to Info-Tech acting reasonably) to audit, Info-Tech's compliance with Data Protection Laws; provided, that the Parties, acting in good faith, shall have agreed upon the scope, timing, and duration of the audit. Info-Tech reserves the right to invoice the Client on a time and materials basis at its reasonable, then-current professional rates for any work required in connection with the audit. The Client shall promptly notify Info-Tech of any non-compliance discovered during the audit. All findings made during the audit shall be deemed Confidential Information of Info-Tech in accordance with the Agreement (or, if the Agreement contains no such provisions or such provisions are not applicable to the information of Info-Tech



or the audit findings in particular, the right of the Client to audit Info-Tech shall be deemed conditional upon the Parties entering into an appropriate confidentiality and non-disclosure agreement with respect to the audit in form and substance satisfactory to Info-Tech acting reasonably) and shall not be used by the Client for any purpose except assessment of Info-Tech's compliance with Data Protection Laws. Info-Tech shall cooperate in good faith with the Client in the course of the audit but shall not be required to take disclose or make available information or materials containing, and the Client shall not be entitled to access, any data or confidential information of other clients of Info-Tech or its affiliates, any internal accounting or financial information of Info-Tech or its affiliates, or any other information or materials requested other than for good faith purposes of the exercise of the Client's audit right under Data Protection Laws.

10. Liability

10.1 The liability of each Party under this DPA shall be subject to the limitation of liability set out in the Agreement.

11. Termination

11.1 This DPA terminates automatically upon termination of the Agreement; provided, that the obligations of each party survive such termination until Personal Data is deleted or anonymized in accordance with this DPA.

12. Governing Law

12.1 Except as required by any Standard Contractual Clauses between Info-Tech and the Client, the interpretation of this DPA shall be governed by the laws of the jurisdiction in which the Info-Tech signatory to this DPA subsists, as described further in Article 14 ("Info-Tech Signatory").

13. Interpretation

13.1 This Agreement shall not be construed against any one Party only by reason that such Party has proffered this Agreement.

14. Info-Tech Signatory

Jurisdiction of Client Legal Entity	Info-Tech Signatory	Governing Law
Canada or jurisdiction other than United States, the United Kingdom, Australia, or New Zealand	Info-Tech Research Group Inc. a Canada corporation	The laws of the Province of Ontario and the laws of Canada applicable in the Province of Ontario
United States	Info-Tech Research Group Inc. a Delaware corporation	The laws of the State of Delaware
United Kingdom	Info-Tech Research Group Ltd a UK corporation	The laws of England and Wales
Australia or New Zealand	Info-Tech Research Group Pty. Ltd. an Australia company	The laws of the State of New South Wales

Annexes



- A. Initial Record of Processing
- B. Technical and Organizational Measures
- C. Standard Contractual Clauses

Signature Page Follows



The Parties have executed this Data Processing Addendum as of the dates below.

Info-Tech		Client: <div></div>	
By:		By:	
Name:		Name:	
Title:		Title:	
Date:		Date:	