Crown Commercial Service

RM6100 Technology Services 3 Agreement
Framework Schedule 4 - Annex 1
Lots 2, 3 and 5 Order Form

Order Form

This Order Form is issued in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100 dated **16th June 2021** between the Supplier (as defined below) and the Minister for the Cabinet Office (the "**Framework Agreement**") and should be used by Buyers after making a direct award or conducting a further competition under the Framework Agreement.

The Contract, referred to throughout this Order Form, means the contract between the Supplier and the Buyer (as defined below) (entered into pursuant to the terms of the Framework Agreement) consisting of this Order Form and the Call Off Terms. The Call-Off Terms are substantially the terms set out in Annex 2 to Schedule 4 to the Framework Agreement and copies of which are available from the Crown Commercial Service website RM6100 Technology Services 3. The agreed Call-Off Terms for the Contract being set out as the Annex 1 to this Order Form.

The Supplier shall provide the Services and/or Goods specified in this Order Form (including any attachments to this Order Form) to the Buyer on and subject to the terms of the Contract for the duration of the Contract Period.

In this Order Form, capitalised expressions shall have the meanings set out in Schedule 1 (Definitions) of the Call-Off Terms

This Order Form shall comprise:

1. This document headed “Order Form”;
2. Attachment 1 – Services Specification;
3. Attachment 2 – Charges and Invoicing;
4. Attachment 3 – Implementation Plan;
5. Attachment 4 – Service Levels and Service Credits:
6. Attachment 5 – Key Supplier Personnel and Key Sub-Contractors;
7. Attachment 6 – Software; (Not Applicable)
8. Attachment 7 – Financial Distress; (Not Applicable)
9. Attachment 8 - Governance
10. Attachment 9 – Schedule of Processing, Personal Data and Data Subjects;
11. Attachment 10 – Transparency Reports; and
12. Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses.

The Order of Precedence shall be as set out in Clause 2.2 of the Call-Off Terms being:

1.1.1 the Framework, except Framework Schedule 18 (Tender);

Crown Commercial Service

1.1.2 the Order Form;

1.1.3 the Call Off Terms; and

1.1.4 Framework Schedule 18 (Tender).

Section A
General information

Contract Details	
Contract Reference:	C341360
Contract Title:	Support and Continuous Improvement for External Digital Services II
Contract Description:	The provision of Support for Continuous Improvement and External Digital Services II as described in the specification.
Contract Anticipated Potential Value: this should set out the total potential value of the Contract	[redacted]

Total Cost for the Onboarding + Initial Contract Period (excluding VAT)	**£ 90,720.00**

Crown Commercial Service

Total Cost for the 2 x optional contract extension (excluding VAT)	**£**	**151,200.00**

Estimated Year 1 Charges: [redacted]

Commencement Date: this should be the date of the last signature on Section E of this Order Form 1st April 2025

Buyer details

Buyer organisation name
Food Standards Agency

Billing address
Your organisation's billing address - please ensure you include a postcode
Clive House, 70 Petty France, Westminster, SW1H 9EX

Buyer representative name
The name of your point of contact for this Order

[redacted]

Buyer representative contact details
Email and telephone contact details for the Buyer's representative. This must include an email for the purpose of Clause 50.6 of the Contract.

[redacted]

Crown Commercial Service

Buyer Project Reference
Please provide the customer project reference number.
C311618.

Supplier details

Supplier name
The supplier organisation name, as it appears in the Framework Agreement

TPXimpact Limited
Company Registration No: 06472420

Supplier address
Supplier's registered address

2 Whitechapel Road
2nd Floor, The Hickman
London
E1 1EW
United Kingdom.

Supplier representative name
The name of the Supplier point of contact for this Order

[redacted]

Supplier representative contact details
Email and telephone contact details of the supplier's representative. This must include an email for the purpose of Clause 50.6 of the Contract.

[redacted]

Order reference number or the Supplier's Catalogue Service Offer Reference Number
A unique number provided by the supplier at the time of the Further Competition Procedure. Please provide the order reference number, this will be used in management information provided by suppliers to assist CCS with framework management. If a Direct Award, please refer to the Supplier's Catalogue Service Offer Reference Number.

Not Applicable.

Guarantor details

Guidance Note: Where the additional clause in respect of the guarantee has been selected to apply to this Contract under Part C of this Order Form, include details of the Guarantor immediately below.

Crown
Commercial
Service

Guarantor Company Name
The guarantor organisation name

Not Applicable.

Guarantor Company Number
Guarantor's registered company number

Not Applicable.

Guarantor Registered Address
Guarantor's registered address

Not Applicable.

Crown Commercial Service

Section B
Part A – Framework Lot

Framework Lot under which this Order is being placed
Tick one box below as applicable (unless a cross-Lot Further Competition or Direct Award, which case, tick Lot 1 also where the buyer is procuring technology strategy & Services Design in addition to Lots 2, 3 and/or 5. Where Lot 1 is also selected then this Order Form and corresponding Call-Off Terms shall apply and the Buyer is not required to complete the Lot 1 Order Form.

1.	TECHNOLOGY STRATEGY & SERVICES DESIGN	☐
2.	TRANSITION & TRANSFORMATION	☐
3.	OPERATIONAL SERVICES	
	a: End User Services	☐
	b: Operational Management	☐
	c: Technical Management	☐
	d: Application and Data Management	**Yes**
5.	SERVICE INTEGRATION AND MANAGEMENT	☐

Part B – The Services Requirement

Commencement Date
See above in Section A

Contract Period
Guidance Note – this should be a period which does not exceed the maximum durations specified per Lot below:

Lot	Maximum Term (including Initial Term and Extension Period) – Months (Years)
2	36 (3)
3	60 (5)
5	60 (5)

Initial Term Months
18 Months

Extension Period (Optional) Months
Two (2) x Six (6) month extension

Minimum Notice Period for exercise of Termination Without Cause 90 (Calendar days) *Insert right (see Clause 35.1.9 of the Call-Off Terms)*

Sites for the provision of the Services

Services will be delivered remotely to the entire Food Standards Agency.

Crown Commercial Service

Buyer Assets
Guidance Note: see definition of Buyer Assets in Schedule 1 of the Call-Off Terms
ServiceNow Licenses

Additional Standards
Guidance *Note: see Clause 13 (Standards) and the definition of Standards in Schedule 1 of the Contract. Schedule 1 (Definitions). Specify any particular standards that should apply to the Contract over and above the Standards.*

Not Applicable.

Buyer Security Policy
Guidance Note: where the Supplier is required to comply with the Buyer's Security Policy then append to this Order Form below.

Please refer to:

FSA Patching Policy Sept 2019 1.1 for new

FSA High Level Security Policy July 2C

Buyer ICT Policy
Guidance Note: where the Supplier is required to comply with the Buyer's ICT Policy then append to this Order Form below.

Please refer to:

Supporting Document 2 - Data Pr

Insurance
Guidance Note: if the Call Off Contract requires a higher level of insurance cover than the £1m default in Framework Agreement or the Buyer requires any additional insurances please specify the details below.

Third Party Public Liability Insurance (£) - £1,000,000

Professional Indemnity Insurance (£) - £1,000.000

Buyer Responsibilities
Guidance Note: list any applicable Buyer Responsibilities below.

The Buyer will be responsible for providing TPXimpact Limited access to all relevant sites, providing ServiceNow licenses for supplier to use, and sharing all information required for the service in a timely manner.

Please refer to the specification for additional information.

Goods

Guidance Note: list any Goods and their prices.

Not Applicable.

Governance – Option Part A or Part B
Guidance Note: the Call-Off Terms has two options in respect of governance. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is limited project governance required during the Contract Period.

Governance Schedule	Tick as applicable
Part A – Short Form Governance Schedule	Yes
Part B – Long Form Governance Schedule	No

The Part selected above shall apply this Contract.

Change Control Procedure – Option Part A or Part B
Guidance Note: the Call-Off Terms has two options in respect of change control. Part A is the short form option and Part B is the long form option. The short form option should only be used where there is no requirement to include a complex change control procedure where operational and fast track changes will not be required.

Change Control Schedule	Tick as applicable
Part A – Short Form Change Control Schedule	No
Part B – Long Form Change Control Schedule	Yes

The Part selected above shall apply this Contract.

Section C

Part A - Additional and Alternative Buyer Terms

Additional Schedules and Clauses *(see Annex 3 of Framework Schedule 4)*
This Annex can be found on the RM6100 CCS webpage. The document is titled RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5.

Part A – Additional Schedules
Guidance Note: Tick any applicable boxes below

Additional Schedules	Tick as applicable
S1: Implementation Plan	☐
S2: Testing Procedures	☐
S3: Security Requirements (either Part A or Part B)	Part A ☐ or Part B Yes
S4: Staff Transfer	☐
S5: Benchmarking	☐
S6: Business Continuity and Disaster Recovery	Yes
S7: Continuous Improvement	Yes
S8: Guarantee	☐
S9: MOD Terms	☐

Part B – Additional Clauses
Guidance Note: Tick any applicable boxes below

Additional Clauses	Tick as applicable
C1: Relevant Convictions	Yes
C2: Security Measures	Yes
C3: Collaboration Agreement	☐

Where selected above the Additional Schedules and/or Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part C - Alternative Clauses
Guidance Note: Tick any applicable boxes below

The following Alternative Clauses will apply:

Alternative Clauses	Tick as applicable
Scots Law	No
Northern Ireland Law	No
Joint Controller Clauses	No

Where selected above the Alternative Clauses set out in document RM6100 Additional and Alternative Terms and Conditions Lots 2, 3 and 5 shall be incorporated into this Contract.

Part B - Additional Information Required for Additional Schedules/Clauses Selected in Part A

Additional Schedule S3 (Security Requirements)
Guidance Note: where Schedule S3 (Security Requirements) has been selected in Part A of Section C above, then for the purpose of the definition of "Security Management Plan" insert the Supplier's draft security management plan below.

TPXimpact Limited will complete a Security Management plan and deliver this to the FSA for approval within 20 days of contract start date.

Additional Schedule S4 (Staff Transfer)
Guidance Note: where Schedule S4 (Staff Transfer) has been selected in Part A of Section C above, then for the purpose of the definition of "Fund" in Annex D2 (LGPS) of Part D (Pension) insert details of the applicable fund below.

Not Applicable.

Additional Clause C1 (Relevant Convictions)
Guidance Note: where Clause C1 (Relevant Convictions) has been selected in Part A of Section C above, then for the purpose of the definition of "Relevant Convictions" insert any relevant convictions which shall apply to this contract below.

Crown Commercial Service

TPXimpact Limited will work with FSA as part of onboarding and on any Work Packages over the life of the contract, to determine if any roles that require additional vetting and a specific national security vetting clearance. Roles which are likely to require additional vetting include system administrators whose role would provide those individuals with privileged access to IT systems.

Additional Clause C3 (Collaboration Agreement)
Guidance Note: where Clause C3 (Collaboration Agreement) has been selected in Part A of Section C above, include details of organisation(s) required to collaborate immediately below.

Not Applicable.

An executed Collaboration Agreement shall be delivered from the Supplier to the Buyer within the stated number of Working Days from the Commencement Date:

Not Applicable.

An executed Collaboration Agreement from the Supplier has been provided to the Buyer.

Not Applicable.

Crown
Commercial
Service

Section D
Supplier Response

Commercially Sensitive information
Any confidential information that the Supplier considers sensitive for the duration of an awarded Contract should be included here. Please refer to definition of Commercially Sensitive Information in the Contract – *use specific references to sections rather than copying the relevant information here.*

TPXimpact Limited Price and the breakdown of the pricing but excluding the Total Contract Value.

Crown
Commercial
Service

Section E
Contract Award

This Call Off Contract is awarded in accordance with the provisions of the Technology Services 3 Framework Agreement RM6100.

SIGNATURES

[redacted]

Attachment 1 – Services Specification

Food Standards Agency
food.gov.uk

APPENDIX B – SPECIFICATION

1. PURPOSE

1.1 FSA is seeking a supplier to provide support services in relation to its external digital applications.

1.2 The Supplier will provide ongoing 'Business as Usual' (BAU) support within the budget and timescales agreed, including but not limited to security and software updates and bug fixing. Support activities are outlined in this document.

2 BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The Food Standards Agency (FSA) is a non-ministerial government department of over 1500 people, with a big vision – FSA work across England, Wales and Northern Ireland ensure that food system delivers Food You Can trust (food that is safe, that is what it says is and that is healthy and sustainable).

2.2 The context in which we operate has transformed following the UK leaving the EU and continues to change at an unprecedented rate. Working Digitally from Anywhere is the key to achieving our ambitions and transforming the way we do business, and the FSA 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.

2.3 The FSA has a Cloud First strategy and have successfully completed our migration from on-premise data centres to service-based hosting.

2.4 Background to requirement

2.5 Food Standard Agency's external, digital applications, based on Drupal 10 provide the service to consumers, food businesses, industry, and academia to help the FSA deliver its mission to ensure that food is safe and what it says it is. The websites provide access to key content, including latest regulation and policy and enable

18

businesses to use online tool for risk assessment (MyHACCP). They are also pivotal in keeping consumers informed about any food or allergy incidents through alert service and enabling the public to find their local food safety team.

2.6 As FSA's flagship services, reflective of the Agency's brand are key tools for effective communication. A such, these applications need to be secure and robust. Serving a wide range of users, the websites need to meet government standards and accessibility regulations. Continuous improvement is necessary to ensure they also meet evolving user needs and are aligned to FSA's priorities.

3 SCOPE OF REQUIREMENT

3.1 The scope of this requirement is for support of the external digital services:

- food.gov.uk,
- Science Advisory Committees sites,
- MyHACCP,
- FSA LINK and
- FSA pattern library

Please refer to the links provided in Section 3.3.

3.2 SUPPORT

3.2.1 The Supplier will support and work with the Agency and its partners to handle incidents, changes, fixes and updates as needed. We expect the supplier to work to the Service Level Agreements - SLAs set out below in Section 3.11, work in conjunction with us to understand what is needed.

3.2.2 All changes will need to be robustly tested by the Supplier before launching, with the test report provided prior to a release for the User Acceptance Testing (UAT). The Agency will also manage the utilisation of this support against a fixed monthly budget of hours, this will be managed through the weekly prioritisation and review meetings.

(a) Support requirements are outlined in Section 3.5 below.
(b) Support activities will be funded through a fixed monthly budget of hours.
(c) The FSA would look to collaboratively review this every 6 months of the contract with the supplier, to ensure the contracted resources remain aligned to the FSAs evolving support needs.
(d) Any agreed changes to the fixed fee, whether increasing or decreasing these, will be managed through a variation to call-off contract.

Food Standards Agency
food.gov.uk

3.2.3 To ensure that there is scope within the service for response to business change the Supplier will be required to provide support and maintenance for the FSA's external web applications. This can cover regular minor version updates of Drupal, PHP version updates, front-end and back-end functionality updates and fixes, as well as improvements to site stability and resilience.

3.2.4 Examples of tasks include:

(a) Updating Drupal 10 to latest minor version, updating PHP version and databases versions as needed, to ensure all systems and components are at version n, with tolerance of n-1
(b) Applying security patches as soon as they become available and monitor the channels for any emergent security threats that the application is vulnerable to (e.g. compromised Drupal modules / libraries)
(c) Bug fixes for external users or editors (Please note that FSA does not expect to be charged for fixing bugs introduced by the supplier.)
(d) Updates to content type templates
(e) Minor changes to the functionality, features or presentation as required to meet business needs
(f) Applying accessibility improvements through the pattern library
(g) Updates to the application flow

3.2.5 The supplier will need to have the capacity to manage support requests and be able to scale up the team to deliver our requirements.

3.2.6 A monthly report will need producing showing the number of days used each month by activity, the balance of any days remaining and rolled over, the total number of days available for use.

3.2.7 The costs for any unused support days are to be refunded to the FSA at the end of the contract term.

3.2.8 We would expect estimations for support work to be accurate to 95% compared to actual for completion of work.

3.2.9 FSA are to approve any support activity prior to work starting. The supplier needs to provide estimates against each support activity.

21

Food Standards Agency
food.gov.uk

3.3 SITES COVERED FOR SUPPORT AND CONTIMUOIS IMPROVEMENT

3.3.1 Below is a list of sites for the immediate inclusion in the support contract. Over the lifetime of the contract there may be additional sites that the FSA will incorporate into this contract. Sites requiring support within the contract may not be Drupal sites. The FSA reserves the right to decouple services, introduce new functionality which may be decoupled from the main sites or choose to utilise different technologies, to respond to the evolving user needs and technological landscape.

Food.gov.uk (including Development, Staging, Production environments) (Drupal10)	https://www.food.gov.uk/
MyHACCP (Development, Staging, Production) MyHACCP (Drupal 10)	https://myhaccp.food.gov.uk/
Science Committees (including Development, Production environments) (Drupal10)	https://acaf.food.gov.uk https://cot.food.gov.uk https://science-council.food.gov.uk https://acmsf.food.gov.uk https://acnfp.food.gov.uk https://acss.food.gov.uk https://sac.food.gov.uk
FSA LINK (Drupal 10)	https://fsalink.food.gov.uk/
Pattern library (Storybook)	https://github.com/FoodStandardsAgency/fsa-pattern-library https://github.com/FoodStandardsAgency/fsa-pattern-library-assets https://github.com/FoodStandardsAgency/fsa-pattern-library-source

22

Food Standards Agency
food.gov.uk

3.4 SPECIFICATION FOR SUPPORT FOR EXTERNAL DIGITAL SERVICES

SUPPLIER'S ROLE:

3.4.1 The Supplier will provide ongoing BAU support within the budget and timescales agreed, including but not limited to security and software updates and bug fixing. Support activities are outlined in the table below:

a	**Support and Maintenance**	Monitor the performance, capacity and availability of the applications and proactively identify opportunities for application changes to improve these.
		Monitor and report on security vulnerabilities – including those identified by NCSC – and work with FSA and other suppliers to provide timely remediation.
		Ensure that all supported components, including application and database servers and environments are patched to a target of N with a tolerance of N-1. For Drupal - minor version updates i.e. 10.4 -> 10.5 to be covered under support. Major version changes to be discussed, as needed.
		Although backup and restore is the responsibility of the Cloud Infrastructure Management supplier, the Supplier will be responsible for providing them with a backup schedule which must also include areas and data to be backed up and recovery points. The Supplier will also contribute to and take part in scheduled restore and Business Continuity/ Disaster recovery tests.
		Adhere to the industry standards in the support, development and

23

Food Standards Agency
food.gov.uk

		maintenance of digital services (please see Sections 3.8 & 3.9)
b	**Cloud hosting**	Configure, operate and maintain the applications, application servers and containers within the hosting environments. Currently this is Acquia Cloud Platform. However the FSA may also use different platforms over the life of the contract.
c	**Dev Ops**	Provide a service that follows an Agile approach and principles to delivery utilising Scrum framework and DevOps practices such as continuous integration and delivery
d	**Technical and Code Skills**	The Supplier must be able to support and develop code using the following tools and languages: - Drupal 9/10 CMS - PHP8 + - SQL databases (MySQL, MSSQL, Postgres) - Modern JavaScript - NodeJS - JavaScript frameworks (e.g.React, NextJS) - Sass and CSS - HTML - Elasticsearch (including Elastic Serverless)
e	**Application and Database Management**	Maintain and annotate supported application source code within FSA's GitHub
		Support and manage the application databases to ensure that requirements for availability, capacity and performance are met
		Maintain all technical, service and system documentation for the FSA, other suppliers and for other developers using public API.

24

Food Standards Agency
food.gov.uk

f	**Environments**	Maintain Production, Test and Development environments, including application databases, ensuring that the Test environment is maintained as an up-to-date mirror of Production
g	**Test, Change and Release** (See further details on Testing in Section 3.6 below)	Be responsible for change support, release management and system testing for all new patch versions and releases.
		Ensure web application updates are thoroughly tested before deployment so that no aspects of the service are affected.
		Carry out and document system, regression and compatibility tests for upgrades and new releases.
		Support User Acceptance Testing by providing test scripts and guidance for users.
		Fix application defects and raising incidents, problems and changes when required in line with FSA processes. Please note that FSA does not expect to be charged for defect corrections and bug fixes identified prior to acceptance into service.
h	**Design and Improvement**	The Supplier must provide high- and low-level design documents for all services and solutions. These must be reviewed and updated on at least an annual basis and following the successful implementation of changes.

3.4.2 Major incidents will be managed through the FSA IT Service Desk and logged on ServiceNow or equivalent systems. The supplier will need to provide contacts, escalation paths and agree communications channels with the FSA IT Service Desk during onboarding to ensure critical issues are managed effectively.

25

Food Standards Agency
food.gov.uk

3.4.3 The Supplier will provide support service within the budget and timescales agreed of up to 6 days per month. If this time is not used, unused hours should be rolled over to the next monthly period. This may cover for all site functionality, UX, Drupal CMS 10, databases and templates.

3.4.4 All data must be stored in FSA systems and not on Suppliers systems or platforms.

3.4.5 The Supplier will log, estimate, manage and prioritise support using collaborative tools on FSA systems. FSA GitHub Projects is the current tool for this purpose.

3.4.6 The Supplier will work with the FSA on the backlog, prioritising and helping deliver new features. This will ensure FSA services continue to evolve inline with the organisations ambitions.

3.4.7 The Supplier will ensure clear project management and governance is in place at all times so the FSA can clearly understand what changes have been made and the reasons why.

3.4.8 The Supplier will work in partnership with internal teams and the FSA's other service delivery partners when required.

3.4.9 It is the Suppliers responsibility to identify and supply key personnel across the service offering (including projects) to maintain service levels and availability of escalation points.

3.4.10 The Supplier should be able to work and communicate fully remotely.

26

Food Standards Agency
food.gov.uk

3.5 CURRENT SERVICE AND ONBOARDING

3.5.1 Introduction

The Drupal platform underpins four public-facing services: the main FSA website, MyHACCP service, a multisite installation for Science Committees, and the FSA LINK service used to communicate with Local Authorities. The key stakeholders include the Product Team in the Openness, Data and Digital directorate, the Communication team, the Science and Research Division team, and the Regulatory Compliance Teams, who are business users of the Drupal products.

3.5.2 Service Overview

The services provide functionalities to publish content using various bespoke templates, such as multipage guides and bespoke integration with the Alerts API to publish allergy and food alerts. They are also customised to manage subscribers for the alerts service and integrate with the gov.uk Notify service to deliver high-priority text and email messages.

The MyHACCP service is a highly customised webform that assists businesses in completing their assessments and generating PDF reports at the end of the process. This service also includes user account management.

The FSA LINK service is used to communicate with Local Authorities, including issuing sensitive, high-priority messages in case of incidents. The entire service is behind a user login, with multiple user roles having access to various areas of the service, including Official Sensitive information for the FSA and LA users.

Recently, the focus has been on the support and maintenance of the service. The last substantial project included an upgrade to Drupal 10. The update of the accessibility guidelines to WCAG 2.2 AA may require tweaks to the components. All front-end changes need to be implemented through the pattern library.

3.5.3 Technical Infrastructure

The current codebase is maintained by the incumbent supplier in their instance of BitBucket. There is a copy available in the FSA

Food Standards Agency
food.gov.uk

GitHub, but it is not the latest version. The incoming supplier needs to take ownership of the codebase and develop the deployment pipelines/process.

There are no automated tests for the services available (unit/functional/regression) – any deployment process requires manual testing. The FSA expects this to be completed by the Supplier before passing any release candidates to the FSA for User Acceptance Testing. The service is hosted on the Acquia platform.

3.5.4 **Onboarding**

The FSA can provide a high-level overview of the services to demonstrate the features and functionalities as used by external users and internal teams.

The FSA can also arrange access to key systems, such as Acquia, FSA GitHub, and Drupal services. We expect to grant higher-level access to a delivery manager or similar role on the incoming supplier team to enable the supplier to manage access for their technical team going forward.

There is limited-service documentation available. The incoming supplier is required to thoroughly review the existing codebase and service functionality and set up their environments to enable them to develop, test, and deploy all Drupal services and the pattern library service. The current deployment process and deployment pipelines are maintained by the incumbent supplier on their infrastructure and will not be handed over.

This includes a small number of bespoke Drupal modules, which the incoming supplier will need to identify, propose suitable replacements for and replace as part of the onboarding process. The incoming supplier will need to develop their own deployment pipelines and process to enable them to move any changes from local development environments to Acquia Dev, Stage and Production.

The FSA operates gated deployment model, so the pipelines need to operate as continuous delivery, rather than continuous deployment. In case of specific technical questions, the FSA could schedule meetings or facilitate message exchanges to get clarification from the incumbent supplier.

28

Food Standards Agency
food.gov.uk

The questions or areas for discussion would need to be shared ahead of any meetings being arranged. The incoming supplier would need to facilitate the meetings to ensure they are getting all the information they require to successfully onboard the service. The FSA can intervene if the information is not being shared in a timely manner, falling back to the contract SLA for requests (3 working days).

The Agency expects to receive an indicative onboarding plan by the end of week 2. Following a review the Agency may sign off or seek clarification on how the service will be onboarded. The plan needs to cover onboarding of all services covered under this contract and schedule meetings to demonstrate the ability by the incoming supplier to amend the service and deploy the code to Acquia staging environment.

If, during onboarding, any issues are identified with the service (apart from the repository ownership, lack of deployment pipelines and the use of proprietary Drupal modules mentioned above), the Agency expects to receive a proposal with options and recommendations for any remedial actions needed.

3.6 TESTING

3.6.1 To ensure the application continues to perform and there are no regression errors, we require appropriate testing of the affected websites prior to the handover for User Acceptance Testing (UAT) and release to ensure no negative impact.

3.6.2 We require the Supplier to carry out an internal Quality Assurance process before releasing to FSA for acceptance testing.

3.6.3 We require the Supplier to prepare and agree with the FSA a complete plan detailing the tests that they will complete prior to UAT handover. The FSA also requires the report, at the UAT handover point, with a list of tests carried out together with the dates and outcome recorded to ensure testing covers requirements.

Food Standards Agency
food.gov.uk

3.6.4 We expect the testing to cover:

(a) functional testing for front-end users and editors (websites front-end and Drupal admin area)

(b) integration tests that make sure different modules used in tandem work well together.

(c) end-to-end checks to verify there are no broken user journeys or workflow issues

(d) regression testing to ensure previously fixed bugs do not reappear.

(e) accessibility testing to WCAG 2.2 AA standards (appropriate manual tests and assistive technology testing for any new work, to pass WCAG 2.2 AA, including passing automated tests, e.g. aXe browser plug-in, SiteImprove or SilkTide)

(f) adherence to quality and coding standards (see Sections 3.8 & 3.9)

3.6.5 The required acceptance testing process is outlined below:

(a) Once the testing is completed by the supplier, the Supplier will inform the FSA that it is ready for acceptance testing and provide testing report.

(b) FSA will perform user acceptance testing to verify if the application satisfies business requirements. FSA will raise any queries or problems with the Supplier

(c) FSA informs the Supplier once the agreed acceptance testing is satisfactorily completed.

(d) Both parties shall keep the completed work under review for one month and issues found resolved without further cost.

(e) Any work found to not meet WCAG 2.2 AA or other standards listed above during testing or external audit must be fixed without further cost.

(f) Supporting document 1 "Food.gov – high-level testing plan" outlines the key functionality of food.gov.uk site.

30

Food Standards Agency
food.gov.uk

3.7 CHANGE CONTROL PROCESSES

3.7.1 The supplier will need to follow FSA approval processes:

- For changes: Pre-release the supplier will need to request approval from the FSA Change Approval Board (CAB) and provide the following information: justification for the change, implementation plan, risk and impact analysis, test plan, back-out plan, link to documentation.
- ensure design components are incorporated into the FSA pattern library.
- follow best practice for safe and secure deployments with rollback plan.

3.8 QUALITY STANDARDS

3.8.1 The services must meet the following quality standards:

- All work and processes must be aligned with Government standards and principles within the Service manual and service standard.
  Service Manual - GOV.UK (www.gov.uk)
  Service standard: https://www.gov.uk/service-manual/service-standard
  Technology: https://www.gov.uk/service-manual/technology
- Meet WCAG 2.2 'AA' accessibility standards in line with the Public Sector Bodies (Website and Mobile Applications)(No.2) Regulations 2018. Regular external accessibility audits will be arranged by the FSA. Once WCAG 2.2 is released (expected Q3 2023) we will need to meet WCAG 2.2 'AA' of the new Guidelines Making your service accessible: an introduction - Service Manual - GOV.UK (www.gov.uk)
- The services should be tested and work across browsers, devices and platforms listed in the GDS browser matrix and assistive technologies
  https://www.gov.uk/service-manual/technology/designing-for-different-browsers-and-devices
  https://www.gov.uk/service-manual/technology/testing-with-assistive-technologies

31

- Ensure progressive enhancement / graceful degradation as per GDS standards.https://www.gov.uk/service-manual/technology/using-progressive-enhancement
- Supplier must maintain and annotate supported application source code and clear and up-to-date technical documentation of all work completed for transferable site management in the wiki on FSA's GitHub.
- ITIL Principles - ITIL principles must be followed.

3.9 CODING STANDARDS

3.9.1 For Drupal-based projects, the supplier needs to adhere to Drupal Coding Standards: https://www.drupal.org/docs/develop/standards. For projects not using Drupal, a standard must be agreed before commencing work.

3.9.2 All work needs to adhere to the following standards:

- HTML/CSS (https://html.spec.whatwg.org/ and https://www.w3.org/TR/css-2023/)
- Accessibility (https://www.w3.org/TR/WCAG22/)
- Security (https://owasp.org/www-project-top-ten/, ISO 27001)

3.9.3 Ensure JavaScript version in use is supported by all major browsers.

3.9.4 Any new front-end code should have valid markup. This can be validated here, however suppliers are welcome to use alternative tools: https://validator.w3.org/#validate_by_uri+with_options

3.9.5 Any back-end code should be error-free and secure. An example of a free checker can be found here, however suppliers are welcome to use alternative tools: https://snyk.io/code-checker/php/

Food Standards Agency
food.gov.uk

3.10 REPORTING REQUIREMENTS

Type of Information	Required regularity
Weekly stand up meeting to include: Call via Microsoft Teams only with Product Owner Review to include: - Progress of tickets including Open and Closed - Risks and issues identified - Work allocation	Weekly
Monthly Review to include: Written report which will be shared with FSA Stakeholders at least 3 working days before the scheduled service review call. (Head of Product, Product Owner) which will include but not be limited to: - Overall months progress on all support and continuous improvement tickets to include performance against SLAs and the required standards and processes outlined in this contract - Progress on any major enhancements - Successes and Areas for improvement. - Appropriateness of solutions - Accuracy of work time/budget estimations. - Upcoming work based on FSAs Backlog and Continuous improvements - Team capacity - Risk log - Log of dates for known future critical releases - Social Value commitments and progress specifically based on the FSA Contract Call to be hosted by the Supplier using Microsoft Teams Only	Monthly
Breakdown and tracker of hours (to be included as part of the monthly review): Written report which will be shared with FSA Stakeholders at least 3 working days before the scheduled service review call. (Head of Product and Product owner) which will include: - Current support and continuous improvement	Monthly

33

Food Standards Agency
food.gov.uk

hours used in month and carried over if applicable - Hours estimated and used against each tasks/tickets. - Current balance of Hours - Major enhancement budget tracker - Tracking against estimations Call to be hosted by the Supplier using Microsoft Teams Only	
Annual review to include: Written report which will be shared with FSA Stakeholders (Head of Product, Product Owner) which will include: - Overall progress for the year to include a full breakdown of performance for the year. Focusing on tickets raised, completion, SLAs performance, new features implemented, hours used, hours rolled forward - Upcoming work for the year ahead - Lessons learned throughout the year - Social Value commitments and progress specifically based on the FSA Contract - Report to be shared with FSA by the 10th Working day of Month following the anniversary of the contract. Call to be done by the 20th of the month following the anniversary of the contract. Call to be hosted by the Supplier using Microsoft Teams Only	Yearly

3.10.1 Governance Arrangements

The Supplier will report into the Product Owner and the Head of Product who oversee the activity.

The Supplier will be required to feed into existing reporting and governance structures where appropriate. See 'Reporting requirements' Section 3.10, and 'Deployment processes' Section 3.8'.

34

Food Standards Agency
food.gov.uk

3.11 HOURS AND DEPLOYMENT TIME

3.12 See table below for standard SLAs for incidents and requests, including response times and resolution times within contracted working hours.

3.13 In the event of a P1 or P2 Incident major incident processes will be invoked, Supplier shall conduct a formal Problem Management review, which shall include undertaking a Root Cause Analysis ("RCA") to determine the underlying cause of the Incident and providing guidance to support any activity required to amend the underlying cause.

Incident

Priority	Description	Response Time*	Resolution Time
P1	Severe business disruption: business unit or sub-unit unable to operate, critical components failed. Failure to meet technological minimums.	15 minutes	4 Hours
P2	Major business disruption: critical user(s) or user group unable to operate, or business unit experiencing significant reduction in system performance.	30 minutes	8 Hours
P3	Minor business disruption: single user unable to operate with no circumvention available	0.5 Working day	3 Working Days
P4	Minor disruption: single user or user group experiencing problems, but with circumvention available	1 Working Day	3 Working Days

* The Resolution Time starts when the incident is raised and ends when the Incident is Resolved

35

Food Standards Agency
food.gov.uk

Adherence to incident management responsibilities will also be assessed via reviews of completed incidents.

Request

Standard Request Management Responsibilities for all suppliers include:

- Carrying out request tasks within the allocated timescales
- Providing regular and comprehensive updates

Description	Resolution Time	Monthly Service Target
Request tasks	3 working days	<=1

- Most deployments can be completed within standard working hours - Monday to Friday 9am to 6pm. However, Friday deployments should be avoided if not critical.
- Deployments should be agreed with FSA and may need to be scheduled for out of hours or agreed at 'quiet' traffic times to avoid potential disruption to the service.
- Out of hours support may be required for specific events by arrangement.

3.14 GDPR AND SECURITY

3.14.1 The supplier will:

- adhere to government security standards, up to date and support any health checks that are carried out when needed/required.
- adhere to the FSA's Data Protection Policy and Procedure (found in supporting document 2 "Data Protection Policy) and understand the importance of safeguarding privacy of FSA staff data at all times
- The FSA will be using Part B of S3: Security Requirements additional Schedule for this contract.

36

Food Standards Agency
food.gov.uk

4 KEY MILESTONES AND DELIVERABLES

The onboarding process for the support contract is structured to ensure a smooth transition and effective collaboration between the client and the support provider. The key milestones are designed to establish a strong foundation for the project, facilitate access to necessary resources, and maintain open communication throughout the onboarding phase. Below are the critical milestones and their respective timeframes.

4.1 The following Contract milestones/deliverables shall apply:

Milestone/ Deliverable	Description	Timeframe or Delivery Date
1 Contract Signing and Initial Setup	Once the contract is signed, the first step is to set up an introductory meeting to align on expectations, timelines, and deliverables. This meeting should include key stakeholders from both the client and the support provider	Within week 1 of Contract Award
2 Access Provisioning	Once the team is assembled and confirmed, access to all necessary systems can be arranged, including GitHub repositories, Acquia environments, and any other relevant platforms. This step is crucial for the team to start working on the project.	Within week 1 of Contract Award
3 Current state review	Review all relevant documentation, including specifications, testing plans, and summaries	Within week 2 of Contract Award

37

Food Standards Agency
food.gov.uk

	of support tickets.	
4 Implementation plan	Supplier to prepare and share indicative onboarding plan, for Agency's review and approval. This needs to capture specific milestones required to successfully onboard all services.	Within week 2 of Contract Award
5 Regular check-ins	Schedule regular check-in meetings to monitor progress, address any issues, and ensure that the onboarding process is on track. These meetings help maintain open communication and ensure that any potential roadblocks are addressed promptly	Within week 3 (set-up), then ongoing during onboarding;
6 Transition to support	Once onboarding is concluded, set-up regular meetings as per specification; set up ticket tracking tools and share report templates for Agency's review and approval.	Final week of onboarding;

5 CONTINUOUS IMPROVEMENT

5.1 The Supplier will be expected to continually improve the way in which the required Services are to be delivered throughout the Contract duration.

5.2 Changes to the way in which the Services are to be delivered must be brought to the Buyer's attention and agreed prior to any changes being implemented.

38

6 PRICE

6.1 All quotations are to be sourced from Lot 3d under the CCS Technology Services 3 framework agreement (RM6100).

6.2 Prices are to be submitted via the e-Sourcing Suite Attachment 4 – Price Schedule excluding VAT and including all other expenses relating to Contract delivery.

6.3 For Statements of Work called off under the contract, the FSA will define how suppliers should price these up when issuing the requirements to the Supplier. Statement of Works are not guaranteed.

6.4 The expectation is most of the Statements of Work will be either fixed price or Capped Time and Materials.

7 STAFF AND CUSTOMER SERVICE

7.1 The Supplier shall provide a sufficient level of resource throughout the duration of the Contract in order to consistently deliver a quality service.

7.2 The Supplier's staff assigned to the Contract shall have the relevant qualifications and experience to deliver the Contract to the required standard.

7.3 The Supplier shall ensure that staff understand the Buyer's vision and objectives and will provide excellent customer service to the Buyer throughout the duration of the Contract.

8 SECURITY AND CONFIDENTIALITY REQUIREMENTS

8.1 All supplier team members will need clearance to Baseline Personnel Security Standard (https://www.gov.uk/government/publications/government-baseline-personnel-security-standard), and the Supplier lead must sign a non-disclosure agreement (NDA) on behalf of the successful organisation.

39

Food Standards Agency
food.gov.uk

8.2 Evidence of certification/alignment to recognised information security standards (e.g. ISO27001, Cyber Essentials, NCSC guidance/principles, etc.), how you ensured compliance with GDPR (including ICO registration number).

8.3 The successful Supplier will be required to commit to maintaining their certifications (Cyber Essentials or ISO27001) over the life of the awarded contract.

9 PAYMENT AND INVOICING

9.1 The invoice schedule will be agreed for each individual Statement of Work.

9.2 Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

9.3 Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs.

9.4 Invoices should be submitted to: [redacted]

9.5 All invoices must contain a Valid Purchase Order number, the Contract reference number and the Statement of Work reference number.

10 CONTRACT MANAGEMENT

10.1 The Supplier is expected to participate in weekly review meetings with key stakeholders from the FSA. These will be held virtually using Microsoft Teams.

10.2 A verbal update should be shared with FSA stakeholders at the weekly review containing details of:

10.3 Progress of all live Statements of Work.

10.4 The supplier is expected to attend monthly contract reviews. A written report should be shared with FSA stakeholders ahead of the monthly review containing details of:

- Progress of all live statements of work, including progress against timelines and budget, risks and opportunities.
- Delivery against social value and cultural requirements.
- Potential opportunities to help support or enable the FSA.

10.5 The Supplier should present any proposed new ways of working to the Authority during monthly Contract review meetings.

10.6 Attendance at Contract Review meetings shall be at the Supplier's own expense.

10.7 Suppliers will be expected to participate in regular meetings for this call-off contract and/or for each individual Statement of Work called off under this contract. These will be defined in each individual Statement of Work.

10.8 Statements of Work will be called-off through the FSA's e-Sourcing system, with the FSA submitting draft Statements of Work containing the requirements to suppliers.

10.9 The Supplier will review and respond to the Statements of Work within 10 working days. If a Statement of Work is considered urgent by the FSA then this response time frame may be reduced. The FSA will then review the response and costs before making a decision whether to proceed with the Statement of Work or not.

10.10 Until Statements of Work are formally approved and signed by both parties and a Purchase Order has been raised there will be no commitment to undertake them and any work carried out will be entirely at the Suppliers own risk.

10.11 Only the FSA Commercial Team have the authority to sign off and commission Statements of Work and contract/SoW changes.

10.12 Proposed changes to the way in which the Services and Statements of Work are to be delivered must be brought to the Authority's attention, agreed and signed off by the FSA Commercial Team prior to any changes being implemented.

10.13 The FSA reserves the right to issue Statements of Work to both or only one of the successful suppliers to provide a response too.

Food Standards Agency
food.gov.uk

11 LOCATION

11.1 The FSA is a home working enabled organisation and therefore you will not have regular access to an FSA office.

11.2 The supplier will primarily work remotely from within the UK, with occasional face to face, but are expected to work openly and collaboratively on digital channels (using client provided services, principally Microsoft 365 e.g. MS Teams).

11.3 On rear occasion any requests for staff to work on projects from outside the UK will need approval from FSA.

12 Out of Scope

12.1 Please note the following is out of scope of this contract:

12.1.1 Hosting of the services & hosting support (i.e. we want the supplier to use Acquia, but we own relationship with Acquia).
12.1.2 Maintenance of Drupal community modules that our application may rely on (i.e. it is open-source, and there are some community supported modules)
12.1.3 Content creation - this is focused on technical support and development SEO and Marketing
12.1.4 Training - staff training in how to use Drupal is out of scope, as we focus on technical support.

13 Commercial Approach

13.1 This contract will be tendered under Lot 2 of the Crown Commercial Service RM6100 Technology Service 3 Framework.

13.2 FSA are looking to award a contract term for **18 Months years with 2 x 6 months optional extension (i.e., 18+6+6)**, subject to satisfactory performance. The maximum contract duration is **2 years and 8 months**.

13.3 The Start date for this contract will be **February 2025** with the successful supplier expected to have completed onboarding ahead of this.

C311618 Support for Continuous Improven

Crown Commercial Service

Project Name: Support for Continuous Improvements for External Digital Service II
Project Reference No:
C311618

Clarifications				
No.	**Date**	**Clarification**	**Answer**	**Date Issued**

1	06-Dec-2024	Social Value: What is FSA's Social Value Strategy, and what specific impact metrics is FSA working towards, relating to tackling inequality? Understanding this will help maximise alignment towards achieving your goals. Alongside measures to ensure equality and inclusion across this contract, are there any particular groups or dimensions of inequality that FSA would like our Social Value efforts to focus on? Does FSA prefer Social Value activities that are delivered through the contract, additional activities, or a combination? What is FSA's minimum expectation of investment in social value on this contract? Does FSA expect social value delivery to involve only the contract	What is FSA's Social Value Strategy, and what specific impact metrics is FSA working towards, relating to tackling inequality? Understanding this will help maximise alignment towards achieving your goals. Response: We are seeking a response from the supplier on how they will provide the service to address the SV strategy in their delivery of the service. Alongside measures to ensure equality and inclusion across this contract, are there any particular groups or dimensions of inequality that FSA would like our Social Value efforts to focus on? Response: FSA isn't focusing on any particular group. Does FSA prefer Social Value activities that are delivered through the contract, additional activities, or a combination? Response: FSA would prefer SV activities delivered via the proposed contract.		10/12/2024

		workforce, or does FSA value the opportunity for its employees to participate in social value activities?	What is FSA's minimum expectation of investment in social value on this contract? Response: Please refer to the scoring for Social Value question. Does FSA expect social value delivery to involve only the contract workforce, or does FSA value the opportunity for its employees to participate in social value activities? Response: Please refer to the scoring for Social Value question. As part of their contract proposal, we require the supplier to detail their Social Value delivery plan.	
2	06-Dec-2024	Please provide the nature and mix of the type of CMS applications: a) Static websites b) Transactional Websites / Portal c) E-Commerce web sites	Services in scope are listed in section 3.1 of the specification, with further detail on their purpose and functionality given in sections 3.5.1 and 3.5.2 of the specification. The pattern library is the only non-drupal site, created using Storybook, and it	10/12/2024

			contains the components for the FSA front-ends for food.gov and MyHACCP.	
3	06-Dec-2024	How many Drupal websites should we consider in scope?	All sites in scope of the tender are listed in section 3.1 of the specification, with further detail, including development and staging environments and URLs given in section 3.3.1 in the specification.	10/12/2024
4	06-Dec-2024	Can we get the past ticket dump of last year or 6 months for analysis of service requests and Incidents (L2 and L3 ticket dumps)? Please provide the support ticket split by priority and detailed summary of tickets	The tickets are a mixture of updates - for example, applying security patches, minor version Drupal upgrades, module updates, PHP version updates, etc... and minor support tasks, such as fixing order in the drop-down fields, correcting visual presentation of the website or tweaking any hardcoded text or translations. We usually include about 5 tickets per release.	10/12/2024
5	06-Dec-2024	For cost effectiveness, can we propose few key roles and onshore and non key roles at offshore?	For security reasons, all staff must be UK based.	10/12/2024
6	06-Dec-2024	Which tool do you use to track and report on support incidents and resolutions?	P1 / P2 - FSA instance of SreviceNow; BAU support - Github Project.	10/12/2024

Crown Commercial Service

7	06-Dec-2024	What is your escalation process for critical issues (P1)?	P1 incident are raised through FSA ServiceNow. The supplier providing IT HelpDesk support is responsible for organising bridge call with key stakeholders, including Drupal support supplier. The progress is tracked in ServiceNow.	10/12/2024
8	06-Dec-2024	Do you maintain a knowledge base or documentation portal for self-service support?	This is not currently available.	10/12/2024
9	06-Dec-2024	What is the support coverage required viz 24x7 or 16x5	Monday - Friday, 9am to 6pm, as detailed in section 3.11 of the specification.	10/12/2024
10	06-Dec-2024	Are there any business requirement document, Design Documents, Architecture diagrams, Release Documents, Support Documents and process documents that can be shared for the existing website and backend applications	The details about website in scope, including technical detail is provided in the specification document. The codebase and any further documentation are commercially sensitive at this point. Available documents will be shared with successful bidder in this tender exercise. The review and follow up questioning should be factored in the onboarding plan.	10/12/2024
11	06-Dec-2024	As we will be supporting L2 & L3 support, but can you share if L1 support is also in scope ?	Initial queries and requests related to Drupal services are handled by Product Team and IT ServiceDesk.	10/12/2024

12	06-Dec-2024	Will there be any house keeping activities required viz creating any kind of reports for business, version upgrade, building CI-CD pipeline etc.	Reporting - please see section 3.10 of the specification; Upgrade, piplines set up activities anticipated as part of onboarding are detailed in sections 3.5.3 and 3.5.4 of the specification.	10/12/2024
13	06-Dec-2024	What is the current technology stack being used along with Drupal? Is there any headless application with React/Angular at the frontend? Currently, does any of the website has decoupled approach?	The site is hosted on Acquia, there is a React app providing search front-end interface, with ElasticSearch powering it.	10/12/2024
14	06-Dec-2024	How many resources are currently supporting Drupal? How are they being distributed between onsite and offshore locations?	All staff working on Drupal support are UK-based. The in-house team consist of 3 staff members. The size and composition of the supplier team is commercially sensitive.	10/12/2024
15	06-Dec-2024	What are the approximate number of pages and components used for the Drupal website and mobile application?	For number of components, please refer to the Pattern library (https://foodstandardsagency.github.io/fsa-pattern-library/main/). There are approx. 10k pages across Drupal sites.	10/12/2024
16	06-Dec-2024	How files (media files, videos, photos and documents XLS, word, PDFs) are associated with content?	Standard Drupal method, Drupal core file handling.	10/12/2024
17	06-Dec-2024	CICD implementation will be in-scope or out of scope?	In-scope, as per section 3.5.4 of the specification.	10/12/2024

18	06-Dec-2024	is incumbent supplier using any coding standard tool or php sniffer or anything which highlights the vulnerabilities?	Warden module - highlights when security are required; Coding standards follow PHP-CS.	10/12/2024
19	06-Dec-2024	Any public or third party API's are getting utilized in current application? Please list all	MapItAPI, FSA Ratings API, FSA Alerts API, ElasticSearchAPI, gov.uk Notify API	10/12/2024
20	06-Dec-2024	What tools are getting utilized for the Accessibility testing? & provide us the major A11y issue details	SiteImprove, perioding auditing by Digital Accessibility Centre. For current list on known accessibility issues please refer to accessibility statement: https://www.food.gov.uk/other/accessibility-statement-for-foodgovuk	10/12/2024
21	06-Dec-2024	Are there two separate teams currently working to handle the support tickets? like a separate team to handle the work coming from service now tickets (reported by external users) & another team would be to support regular issues (created by stakeholders) on production sites.	Requests are initially reviewed by Product team, regardless of origin.	10/12/2024
22	06-Dec-2024	Any pattern library drupal module is getting utilized?	Integration uses contributed components module in Drupal.	10/12/2024
23	06-Dec-2024	Any tool is getting utilized to monitor the performance? like new relic or any other tools	We have access to standard tools available in Acqua Cloud.	10/12/2024
24	06-Dec-2024	Could you please elaborate on the NCSC role on identifying vulnerabilities from the systems?	NCSC sends alerts if a vulnerability is identified. It is then for the product	10/12/2024

			team and supplier to access severity and apply a fix.	
25	06-Dec-2024	Disaster recovery comes under the contract? anything implemented in current system	Yes. There is a backup schedule. If the service went down restoring service would come under support.	10/12/2024
26	06-Dec-2024	what kind of support activities involved in Elastic search?	Ensuring the search is performing as required. ES hosting / upgrades are out of scope.	10/12/2024
27	06-Dec-2024	Are emails getting send out using any acquia platform?	System emails (e.g. password reset emails) are emailed from Drupal, Alerts notification use gov.uk Notify.	10/12/2024
28	06-Dec-2024	Any drupal contrib module contribution to the drupal.org community from either FSA or incumbent supplier? Any bespoke modules which will not be handed over to new supplier from the incumbent supplier? please provide details about it	FSA does not support any 'community modules', however the site relies on several such modules. There are also bespoke modules which will not be handed over and can either be removed or replaced (i.e. non-critical). There is further detail in section 3.5.4.	10/12/2024
29	06-Dec-2024	Any html twig writing methodology is implemented in current twig templates? like BEM	Yes. Using BEM.	10/12/2024
30	06-Dec-2024	Are there any special data security requirements for the application	Data security requirements are provided in Attachment 9 – Schedule of Processing, Personal Data and Data Subjects in the Order Form. Please refer APPENDIX A C311618 Support for Continuous Improvements - RM6100 Order Form	10/12/2024

			Draft **v2** COMPLETED AT CONTRACT AWARD.	
31	06-Dec-2024	What is the average number of releases done in a month?	Two. We aim for fortnightly releases.	10/12/2024
32	06-Dec-2024	What is the usual release window? Are any releases planned during weekends?	Releases usually take place on Thursdays.	10/12/2024
33	06-Dec-2024	Has DevOps or any form of automation been implemented?	This is not currently implemented.	10/12/2024
34	06-Dec-2024	What testing practices and frameworks have been used during development?	The site is manually tested before release.	10/12/2024
35	06-Dec-2024	Are the test cases and test scenarios available for functional and integration testing?	There is a manual available for food.gov.uk	10/12/2024

Crown Commercial Service

Attachment 4 – Service Levels and Service Credits

INTRODUCTION

Suppliers will be required to provide the Incident Management element of this agreement using the following parameters:

• Core or 'working' hours 7am to 8pm Monday to Friday

• Non-core 8pm to 7am Monday to Friday plus weekends and bank holidays

There will be no Service Credit/Debit regime associated with this call-off.

Instead the target achievement levels detailed in Table A will attract failure points where resolution targets are not met. Performance against SLAs must be monitored and reported on by the Supplier. The Supplier must also identify why they have not been achieved and what plans are being instigated to ensure that this does not continue.

1.1 See table below for standard SLAs for incidents and requests, including response times and resolution times within contracted working hours.

1.2 In the event of a P1 or P2 Incident major incident processes will be invoked, Supplier shall conduct a formal Problem Management review, which shall include undertaking a Root Cause Analysis ("RCA") to determine the underlying cause of the Incident and providing guidance to support any activity required to amend the underlying cause.

Table A:

Incident

Priority	Description	Response Time*	Resolution Time
P1	Severe business disruption: business unit or sub-unit unable to operate, critical components failed. Failure to meet technological minimums.	15 minutes	4 Hours

P2	Major business disruption: critical user(s) or user group unable to operate, or business unit experiencing significant reduction in system performance.	30 minutes	8 Hours
P3	Minor business disruption: single user unable to operate with no circumvention available	0.5 Working day	3 Working Days
P4	Minor disruption: single user or user group experiencing problems, but with circumvention available	1 Working Day	3 Working Days

* The Resolution Time starts when the incident is raised and ends when the Incident is Resolved

Adherence to incident management responsibilities will also be assessed via reviews of completed incidents.

Request

Standard Request Management Responsibilities for all suppliers include:

- Carrying out request tasks within the allocated timescales
- Providing regular and comprehensive updates

Description	**Resolution Time**	**Monthly Service Target**
Request tasks	3 working days	<=1

- Most deployments can be completed within standard working hours - Monday to Friday 9am to 6pm. However, Friday deployments should be avoided if not critical.
- Deployments should be agreed with FSA and may need to be scheduled for out of hours or agreed at 'quiet' traffic times to avoid potential disruption to the service.
- Out of hours support may be required for specific events by arrangement.

No Service credits applicable.

Crown Commercial Service

Attachment 5 – Key Supplier Personnel and Key Sub-Contractors

1.1.5 The Parties agree that they will update this Attachment 5 periodically to record any changes to Key Supplier Personnel and/or any Key Sub-Contractors appointed by the Supplier after the Commencement Date for the purposes of the delivery of the Services.

Part A – Key Supplier Personnel

Key Supplier Personnel	Key Role(s)	Duration
Resource name will vary from time to time,	Drupal Certified Developer Front-End Developer Senior Account Manager Client Strategy Partner Quality Assurance Senior Technical Principal Lead Strategist Designer Creative Director	The full contract term.

Part B – Key Sub-Contractors

Contractors will only be used who meet the same security clearance as all TPX impact staff and when a freelancer is onboard they are UK based and are agreed prior to project start date by FSA

Crown Commercial Service

Attachment 6 – Software

1.1.1 The Software below is licensed to the Buyer in accordance with Clauses 20 (*Intellectual Property Rights*) and 21 (*Licences Granted by the Supplier*).

1.1.2 The Parties agree that they will update this Attachment 6 periodically to record any Supplier Software or Third Party Software subsequently licensed by the Supplier or third parties for the purposes of the delivery of the Services.

Part A – Supplier Software

The Supplier Software includes the following items:

Not Applicable - All software used to deliver the contract deliverables are Open Sourced.

Part B – Third Party Software

The Third Party Software shall include the following items:

Not Applicable - All software used to deliver the contract deliverables are Open Sourced.

Attachment 7 – Financial Distress

For the purpose of Schedule 7 (Financial Distress) of the Call-Off Terms, the following shall apply:

Not Applicable.

PART A – CREDIT RATING THRESHOLD

Entity	**Credit Rating (long term)** *(insert credit rating issued for the entity at the Commencement Date)*	**Credit Rating Threshold** *(insert the actual rating (e.g. AA-) or the Credit Rating Level (e.g. Credit Rating Level 3)*
Supplier	[Rating Agency 1] – [insert rating for Rating Agency 1]	[Rating Agency 1] – [insert threshold for Rating Agency 1]
	[Rating Agency 2] – [insert rating for Rating Agency 2]	[Rating Agency 2] – [insert threshold for Rating Agency 2]
	[etc.]	[etc.]
[Guarantor]	[Rating Agency 1] – [insert rating for Rating Agency 1]	[Rating Agency 1] – [insert threshold for Rating Agency 1]
	[Rating Agency 2] – [insert rating for Rating Agency 2]	[Rating Agency 2] – [insert threshold for Rating Agency 2]
	[etc.]	[etc.]
[Key Sub-contractor 1]	[etc.]	[etc.]
[Key Sub-contractor 2]	[etc.]	[etc.]

PART B – RATING AGENCIES

- [Rating Agency 1 (e.g Standard and Poors)]
  - Credit Rating Level 1 = [AAA]
  - Credit Rating Level 2 = [AA+]
  - Credit Rating Level 3 = [AA]
  - Credit Rating Level 4 = [AA-]

- Credit Rating Level 5 = [A+]
- Credit Rating Level 6 = [A]
- Credit Rating Level 7 = [A-]
- Credit Rating Level 8 = [BBB+]
- Credit Rating Level 9 = [BBB]
- Credit Rating Level 10 = [BBB-]
- Etc.

- [Rating Agency 2 (e.g Moodys)]
  - Credit Rating Level 1 = [Aaa]
  - Credit Rating Level 2 = [Aa1]
  - Credit Rating Level 3 = [Aa2]
  - Credit Rating Level 4 = [Aa3]
  - Credit Rating Level 5 = [A1]
  - Credit Rating Level 6 = [A2]
  - Credit Rating Level 7 = [A3]
  - Credit Rating Level 8 = [Baa1]
  - Credit Rating Level 9 = [Baa2]
  - Credit Rating Level 10 = [Baa3]
  - Etc.

- [Rating Agency 3 (etc.)]
  - Credit Rating Level 1 = [XXX]
  - Etc.

Attachment 8 – Governance

PART A – SHORT FORM GOVERNANCE

For the purpose of Part A of Schedule 7 (Short Form Governance) of the Call-Off Terms, the following board shall apply:

Project Operational Board	
Buyer Members for the Operational Board	Anna Nikiel Lead Product Development - ODD Danielle Tucker Head of Product - ODD
Supplier Members for the Operational Board	 Client Services Project Management Principle Tech Strategy lead
Frequency of the Operational Board	Weekly Project Status Meeting Monthly Account / Contract Management Meeting
Location of the Operational Board	Virtual Meeting and Face to Face from time to time.

PART B – LONG FORM GOVERNANCE

For the purpose of Part B of Schedule 7 (Long Form Governance) of the Call-Off Terms, the following boards shall apply:

Not Applicable.

Attachment 9 – Schedule of Processing, Personal Data and Data Subjects

This Attachment 9 shall be completed by the Controller, who may take account of the view of the Processors, however the final decision as to the content of this Schedule shall be with the Buyer at its absolute discretion.

1.1.1.1 The contact details of the Buyer's Data Protection Officer are:
Information.Management@food.gov.uk

1.1.1.2 The contact details of the Supplier's Data Protection Officer are:

iinfogov@tpximpact.com

1.1.1.3 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.1.1.4 Any such further instructions shall be incorporated into this Attachment 9.

Description	Details
Identity of Controller for each Category of Personal Data	**The Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Clause 34.2 to 34.15 and for the purposes of the Data Protection Legislation, the Buyer is the Controller and the Supplier is the Processor of the following Personal Data: • Any personal data contained within documents or data records by the Supplier in the Relevant Authority's IT Infrastructure. **The Supplier is Controller and the Authority is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Buyer is the Processor in accordance with Clause 34.2 to 34.15 of the following Personal Data: • **Not Applicable.** **The Parties are Joint Controllers** The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of: • **Not Applicable** For the purpose of Clause 1.2 of the joint controller clauses the Supplier shall be the Party referenced and responsible for those matters set out in Clause 1.2(a)-(e). ***Insert for the purpose of Paragraph 1.2 of the joint controller clauses which Party (either Supplier or Buyer) shall be responsible for***

	those matters listed in Clause 1.2(a) – (e), including whose privacy policy should apply i.e. **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of*:* ● *Business contact details of Supplier Personnel,* ● *Business contact details of any directors, officers, employees, agents, consultants and contractors of the Buyer (excluding the Supplier Personnel) engaged in the performance of the Buyer's duties under this Contract.*
Duration of the processing	Initial Contract Term of 18 months, up to the maximum of additional 12 months. The Full Contract duration.
Nature and purposes of the processing	Viewing of the data where required for software administration or troubleshooting purposes over a remote desktop connection from the supplier's offices.
Type of Personal Data	*Any data contained within documents that have been indexed in the platform. This will ordinarily be low risk information such as contact details, names and addresses. This may in exceptional circumstances include special category and sensitive financial information.*
Categories of Data Subject	*Employees, Local Authority Contacts, Food Business Owners or Employees or Customers*
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The full contract duration.

Attachment 10 – Transparency Reports

Title	Content	Format	Frequency
Budget Reporting	Finance Project Management	Excel and Word	Monthly Bespoke and aligned to project timeline
Impact Reporting	Account Management	Excel, Word and presentation	Quarterly
Technical	Health check and stability	Excel, Word and presentation	Quarterly
Technical	Incident report	Word	only if incident triggered

Annex 1 – Call Off Terms and Additional/Alternative Schedules and Clauses

FRAMEWORK SCHEDULE 4 – ANNEX 3

ALTERNATIVE AND ADDITIONAL CLAUSES AND SCHEDULES FOR LOTS 3

ADDITIONAL CLAUSES AND SCHEDULES

SCHEDULES

S1	Implementation Plan
	S3 Security Requirements (Part B)
	S6: Business Continuity and Disaster Recovery

CLAUSES

C1	Relevant Convictions
C2	Security Measures

Unless there is a clear adjustment to an existing provision of the Contract, additional Clauses incorporated into the Contract via the Order Form will have the effect of being inserted sequentially immediately after Clause 55. New definitions for Schedule 1 (Definitions) will have the effect of being inserted alphabetically into the table therein and associated schedules will have the effect of being inserted sequentially immediately after Schedule 10.

ADDITIONAL CLAUSES AND SCHEDULES - SCHEDULES

S1 IMPLEMENTATION PLAN

1. INTRODUCTION

1.1 This Schedule S1 (Implementation Plan):

1.1.1 defines the process for the preparation and implementation of the Outline Implementation Plan and Detailed Implementation Plan; and

1.1.2 identifies the Milestones (and associated Deliverables) including the Milestones which trigger payment to the Supplier of the applicable Milestone Payments following the issue of the applicable Milestone Achievement Certificate.

2. OUTLINE IMPLEMENTATION PLAN

2.1 The Outline Implementation Plan is set out in Attachment 3 (outline Implementation Plan) the Order Form.

2.2 All changes to the Outline Implementation Plan shall be subject to the Change Control Procedure provided that the Supplier shall not attempt to postpone any of the Milestones using the Change Control Procedure or otherwise (except in accordance with Clause 32 (Supplier Relief Due to Buyer Cause)).

3. APPROVAL OF THE DETAILED IMPLEMENTATION PLAN

3.1 The Supplier shall submit a draft of the Detailed Implementation Plan to the Buyer for approval within twenty (20) Working Days of the Commencement Date.

3.2 The Supplier shall ensure that the draft Detailed Implementation Plan:

3.2.1 incorporates all of the Milestones and Milestone Dates set out in the Outline Implementation Plan;

3.2.2 includes (as a minimum) the Supplier's proposed timescales in respect of the following for each of the Milestones:

(a) the completion of each design document;

(b) the completion of the build phase;

(c) the completion of any Testing to be undertaken in accordance with Schedule S2 (Testing Procedures); and

(d) training and roll-out activities;

3.2.3 clearly outlines all the steps required to implement the Milestones to be achieved in the next 15 months (or such other period agreed between the Parties), together with a high level plan for the rest of the programme;

3.2.4 clearly outlines the required roles and responsibilities of both Parties, including staffing requirements; and

3.2.5 is produced using a software tool as specified, or agreed by the Buyer.

3.3 Prior to the submission of the draft Detailed Implementation Plan to the Buyer in accordance with Paragraph 3.1, the Buyer shall have the right:

3.3.1 to review any documentation produced by the Supplier in relation to the development of the Detailed Implementation Plan, including:

(a) details of the Supplier's intended approach to the Detailed Implementation Plan and its development;

(b) copies of any drafts of the Detailed Implementation Plan produced by the Supplier; and

(c) any other work in progress in relation to the Detailed Implementation Plan; and

3.3.2 to require the Supplier to include any reasonable changes or provisions in the Detailed Implementation Plan.

3.4 Following receipt of the draft Detailed Implementation Plan from the Supplier, the Buyer shall:

3.4.1 review and comment on the draft Detailed Implementation Plan as soon as reasonably practicable; and

3.4.2 notify the Supplier in writing that it approves or rejects the draft Detailed Implementation Plan no later than twenty (20) Working Days after the date on which the draft Detailed Implementation Plan is first delivered to the Buyer.

3.5 If the Buyer rejects the draft Detailed Implementation Plan:

3.5.1 the Buyer shall inform the Supplier in writing of its reasons for its rejection; and

3.5.2 the Supplier shall then revise the draft Detailed Implementation Plan (taking reasonable account of the Buyer's comments) and shall re-submit a revised draft Detailed Implementation Plan to the Buyer for the Buyer's approval within twenty (20) Working Days of the date of the Buyer's notice of rejection. The provisions of Paragraph 3.4 and this Paragraph 3.5 shall apply again to any resubmitted draft Detailed Implementation Plan, provided that either Party may refer any disputed matters for resolution by the Dispute Resolution Procedure at any time.

3.6 If the Buyer approves the draft Detailed Implementation Plan, it shall replace the Outline Implementation Plan from the date of the Buyer’s notice of approval.

4. UPDATES TO AND MAINTENANCE OF THE DETAILED IMPLEMENTATION PLAN

4.1 Following the approval of the Detailed Implementation Plan by the Buyer:

4.1.1 the Supplier shall submit a revised Detailed Implementation Plan to the Buyer every three (3) months starting three (3) months from the Commencement Date;

4.1.2 without prejudice to Paragraph 4.1.1, the Buyer shall be entitled to request a revised Detailed Implementation Plan at any time by giving written notice to the Supplier and the Supplier shall submit a draft revised Detailed Implementation Plan to the Buyer within twenty (20) Working Days of receiving such a request from the Buyer (or such longer period as the Parties may agree provided that any failure to agree such longer period shall be referred to the Dispute Resolution Procedure);

4.1.3 any revised Detailed Implementation Plan shall (subject to Paragraph 4.2) be submitted by the Supplier for approval in accordance with the procedure set out in Paragraph 3; and

4.1.4 the Supplier's performance against the Implementation Plan shall be monitored at meetings of the Service Management Board (as defined in Part B of Schedule 7 (Governance) where used) or any such service management board established under Part A of Schedule 7 (Governance) where used. In preparation for such meetings, the current Detailed Implementation Plan shall be provided by the Supplier to the Buyer not less than five (5) Working Days in advance of such meeting.

4.2 Save for any amendments which are of a type identified and notified by the Buyer (at the Buyer's discretion) to the Supplier in writing as not requiring approval, any material amendments to the Detailed Implementation Plan shall be subject to the Change Control Procedure provided that:

4.2.1 any amendments to elements of the Detailed Implementation Plan which are based on the contents of the Outline Implementation Plan shall be deemed to be material amendments; and

4.2.2 in no circumstances shall the Supplier be entitled to alter or request an alteration to any Milestone Date except in accordance with Clause 32 (Supplier Relief Due to Buyer Cause).

4.3 Any proposed amendments to the Detailed Implementation Plan shall not come into force until they have been approved in writing by the Buyer.

5. GOVERNMENT REVIEWS

1.1.3 The Supplier acknowledges that the Services may be subject to Government review at key stages of the project. The Supplier shall cooperate with any bodies undertaking such review and shall allow for such reasonable assistance as may be required for this purpose within the Charges.

S3 SECURITY REQUIREMENTS
PART A – SHORT FORM SECURITY REQUIREMENTS

1. DEFINITIONS

1.1 In this Part A of Schedule S3 (Security Requirements), the following definitions shall apply:

"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Schedule, a draft of which has been provided by the Supplier to the Buyer and is set out in the Order Form and as updated from time to time.

2. COMPLIANCE WITH SECURITY REQUIREMENTS AND UPDATES

2.1 The Supplier shall comply with the Security Policy and the requirements of this Schedule S3 (Security Requirements) including the Security Management Plan (if any) and shall ensure that the Security Management Plan produced by the Supplier fully complies with the Security Policy.

2.2 Where the Security Policy applies, the Buyer shall notify the Supplier of any changes or proposed changes to the Security Policy.

2.3 If the Supplier believes that a change or proposed change to the Security Policy will have a material and unavoidable cost implication to the provision of the Services it may propose a Change to the Buyer. In doing so, the Supplier must support its request by providing evidence of the cause of any increased costs and the steps that it has taken to mitigate those costs. Any change to the Charges shall then be subject to the Change Control Procedure.

2.4 Until and/or unless a change to the Charges is agreed by the Buyer pursuant to the Change Control Procedure the Supplier shall continue to provide the Services in accordance with its existing obligations.

3. SECURITY STANDARDS

3.1 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Services, confidentiality, integrity and availability of information and consequently on security.

3.2 The Supplier shall be responsible for the effective performance of its security obligations and shall at all times provide a level of security which:

3.2.1 is in accordance with the Law and this Contract;

3.2.2 as a minimum demonstrates Good Industry Practice;

3.2.3 meets any specific security threats of immediate relevance to the Services and/or the Buyer Data; and

3.2.4 where specified by the Buyer in accordance with Paragraph 2.1 complies with the Security Policy and the ICT Policy.

1.1.4

3.3 The references to standards, guidance and policies contained or set out in this Schedule shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.4 In the event of any inconsistency in the provisions of the above standards, guidance and policies, the Supplier should notify the Buyer Representative of such inconsistency immediately upon becoming aware of the same, and the Buyer Representative shall, as soon as practicable, advise the Supplier which provision the Supplier shall be required to comply with.

4. SECURITY MANAGEMENT PLAN

Introduction

4.1 The Supplier shall develop and maintain a Security Management Plan in accordance with this Part A of Schedule S3 (Security Requirements). The Supplier shall thereafter comply with its obligations set out in the Security Management Plan.

Content of Security Management Plan

4.2 The Security Management Plan shall:

4.2.1 comply with the principles of security set out in Paragraph 3 and any other provisions of this Contract relevant to security;

4.2.2 identify the necessary delegated organisational roles for those responsible for ensuring it is complied with by the Supplier;

4.2.3 detail the process for managing any security risks from Sub-Contractors and third parties authorised by the Buyer with access to the Services, processes associated with the provision of the Services, the Buyer Premises, the Sites and any IT, information and data (including the Buyer's Confidential Information and the Buyer Data) and any system that could directly or indirectly have an impact on that Information, data and/or the Services;

4.2.4 be developed to protect all aspects of the Services and all processes associated with the provision of the Deliverables, including the Buyer Premises, the Sites, and any IT, information and data (including the Buyer's Confidential Information and the Buyer Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

4.2.5 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the provision of the Goods and/or Services and shall at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Contract;

4.2.6 set out the plans for transitioning all security arrangements and responsibilities for the Supplier to meet the full obligations of the security requirements set out in this Contract and, where necessary in accordance with Paragraph 2.1 the Security Policy; and

4.2.7 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the provision of the Services and shall only

reference documents which are in the possession of the Parties or whose location is otherwise specified in this Part A Schedule S3 (Security Requirements).

Development of the Security Management Plan

4.3 Within twenty (20) Working Days after the Commencement Date and in accordance with Paragraph 4, the Supplier shall prepare and deliver to the Buyer for approval a fully complete and up to date Security Management Plan which will be based on the draft Security Management Plan set out in the Order Form.

4.4 If the Security Management Plan submitted to the Buyer in accordance with Paragraph 4.3, or any subsequent revision to it in accordance with Paragraph 4, is approved it will be adopted immediately and will replace the previous version of the Security Management Plan and thereafter operated and maintained in accordance with this Part A Schedule S3 (Security Requirements). If the Security Management Plan is not approved, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit to the Buyer for approval. The Parties will use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of its first submission to the Buyer. If the Buyer does not approve the Security Management Plan following its resubmission, the matter will be resolved in accordance with the Dispute Resolution Procedure.

4.5 The Buyer shall not unreasonably withhold or delay its decision to approve or not the Security Management Plan pursuant to Paragraph 4.4. However a refusal by the Buyer to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.6 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.4 or of any change to the Security Management Plan in accordance with Paragraph 4 shall not relieve the Supplier of its obligations under this Part A Schedule S3 (Security Requirements).

Amendment of the Security Management Plan

4.7 The Security Management Plan shall be fully reviewed and updated by the Supplier at least annually to reflect:

4.7.1 emerging changes in Good Industry Practice;

4.7.2 any change or proposed change to the Services and/or associated processes;

4.7.3 where necessary in accordance with Paragraph 2.1, any change to the Security Policy;

4.7.4 any new perceived or changed security threats; and

4.7.5 any reasonable change in requirements requested by the Buyer.

4.8 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amendment of the Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

4.8.1 suggested improvements to the effectiveness of the Security Management Plan;

4.8.2 updates to the risk assessments; and

4.8.3 suggested improvements in measuring the effectiveness of controls.

4.9 Subject to Paragraph 4.10, any change or amendment which the Supplier proposes to make to the Security Management Plan (as a result of a review carried out in accordance with Paragraph 4.7, a request by the Buyer or otherwise) shall be subject to the Change Control Procedure.

4.10 The Buyer may, acting reasonably, approve and require changes or amendments to the Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment.

5. SECURITY BREACH

5.1 Either Party shall notify the other in accordance with the agreed security incident management process (as detailed in the Security Management Plan) upon becoming aware of any Breach of Security or any potential or attempted Breach of Security.

5.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 5.1, the Supplier shall:

5.3 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

5.3.1 minimise the extent of actual or potential harm caused by any Breach of Security;

5.3.2 remedy such Breach of Security to the extent possible and protect the integrity of the Buyer and the provision of the Goods and/or Services to the extent within its control against any such Breach of Security or attempted Breach of Security;

5.3.3 prevent an equivalent breach in the future exploiting the same cause failure; and

5.3.4 as soon as reasonably practicable provide to the Buyer, where the Buyer so requests, full details (using the reporting mechanism defined by the Security Management Plan) of the Breach of Security or attempted Breach of Security, including a cause analysis where required by the Buyer.

5.4 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the Security Management Plan with the Security Policy (where relevant in accordance with Paragraph 2.1) or the requirements of this Part A Schedule S3 (Security Requirements), then any required change to the Security Management Plan shall be at no cost to the Buyer.

S6: Business Continuity and Disaster Recovery

DOCUMENT CONTROL

Reference	TPX-BCDR-PN01
Title	TPXimpact Business Continuity & Disaster Recovery Plan
Type	Plan
Owner	[redacted]
Executive sponsor	[redacted]
Approved by	Operational Board
Published date	03/04/2023
Next review date	01/11/2024

Version	Issued by	Description of change	Date issued
0.1	Sean Beverton-Tubbs	Draft taken to Operations Board for approval before release.	17/03/2023
1.0	Mike Bobroff	First Operations Board approved version published.	03/04/2023
1.1	Sean Beverton-Tubbs	Updated scenarios following external audit April 2023.	24/04/2023
1.2	Sean Beverton-Tubbs	Updated scenarios following comments from a client.	20/09/2023
2.0	Sean Beverton-Tubbs	Updated scenarios following introduction of Occupational Health & Safety ISO 45001.	01/05/2024

TPXimpact Holdings PLC
7 Savoy Court, London, England, England, WC2R 0EX
Company Number 10533096, Registered in England and Wales

SCOPE

This plan applies to all **employees** (in a permanent, temporary or voluntary capacity) of **TPXimpact Holdings PLC** and its **subsidiaries** (hereby referred to as **TPXimpact**), and **suppliers** operating on behalf of TPXimpact (hereby collectively referred to as **users**) who deliver our services. Users must follow this plan to ensure business continuity and/or recovery in the event of a disaster.

This plan forms an integral part of our **Business Management System** (BMS) which outlines our compliance to the ISO 9001, ISO 14001, ISO 27001 and ISO 45001 standards and the UK's National Cyber Security Center's (NCSC) Cyber Essentials standard. It also ensures that we meet our responsibilities and obligations under all relevant and applicable legislation as defined in our *Register of Regulations* (RoR). This plan is endorsed and mandated by our Executive Directors, with **fully delegated authority given to the Operational Board**.

OVERVIEW

As we continue to grow by winning and delivering bigger, more impactful work, we must ensure our operation can **continue to deliver our business critical services in the event of a material interruption or disaster** (including another global pandemic). Timely and effective recovery of our service, processes, environments, systems and data are key in ensuring our revenue and reputation is suitably protected. This robust Business Continuity & Disaster Recovery (BCDR) plan safeguards the continuity of client-facing service delivery and seeks to minimise any disruption to our contractual Key Performance Indicators (KPIs).

TPXimpact operates a **remote-first business model** where users are able to flexibly work from either remote, client site or any of our designated hubs (offices) across the UK. This means we have a fully mobile workforce which can function normally irrespective of location.

TPXimpact operates a **cloud-first approach** to providing applications to our users by utilising enterprise-grade, public cloud 'as-a-service' solutions which are accessed by public internet. This means that our data is primarily held in the cloud (or where this is not the case, synchronised backups are maintained in the cloud, enabling full recovery in the event of the loss of a device) and we do not maintain a traditional network or 'on-premise' infrastructure. Network and physical server security is provided by our cloud providers and enforced as part of our contractual arrangements and with them.

This model and approach enables our operation to be **highly resilient in terms of business continuity and disaster recovery by design**. The focus of our preventative planning ensures minimal risk of data loss, seeks to minimise the impact on customer delivery across its active projects, and aims to preserve essential services for our employees and subcontractors.

Our philosophy is that **no business-critical data is held outside of either a trusted, highly-resilient cloud provider** (e.g. Amazon Web Services, Google, Microsoft, etc.) or locally in a storage medium that is automatically **synchronised to a highly-resilient cloud backup service** (E.g. Google Drive). Devices used routinely by staff in the course of their duties are utilitarian and can be quickly substituted or replaced if necessary, with key data remaining secure (and accessible) via cloud services.

The absence of connectivity to cloud services (e.g. failure of Wi-Fi or internet connectivity) is anticipated to cause only short-term business continuity issues. Given the localised nature of connectivity issues and the essentially mobile nature of all our staff, **re-connectivity is a simple matter of moving to a new location** (e.g. a different client site, a shared office space or a public space/coffee-bar etc.).

TPXimpact Holdings PLC
7 Savoy Court, London, England, England, WC2R 0EX
Company Number 10533096, Registered in England and Wales

Where service delivery is dependent on a client's infrastructure, we must rely on their own BCDR plans as they will have them in place for their own purposes. Key dependencies on our service deliverables must be noted in relevant commercial arrangements to ensure they are effectively and openly managed. Typically our delivery teams are entirely self-sufficient as TPXimpact provides all relevant tooling and infrastructure for the successful delivery of our services.

TPXimpact Holdings PLC
7 Savoy Court, London, England, England, WC2R 0EX
Company Number 10533096, Registered in England and Wales

ROLES & RESPONSIBILITIES

The following named individuals are responsible for coordination and enactment of the business continuity and disaster recovery plan. Each business area has a primary and secondary responsible role with a generic email address to ensure full coverage. In the event of the email system being affected by the incident, users should contact via an alternative channel such as Slack or phone.

Business area	Primary	Secondary	Contact details
[redacted]			

In the event that a BCDR plan had to be activated to ensure continuity of service to a client, the relevant TPXimpact BCDR Coordinator would work through the designated TPXimpact Engagement Lead(s) of any impacted client(s) who would in turn notify their designated Client Engagement Lead with the relevant details pertaining to the BCDR event.

TESTING

Our business continuity & disaster recovery plan must be tested annually to ensure its effectiveness in the event of a live event. Each scenario outlined below must be tested either as a paper-based exercise or in a suitable test environment to ensure confidence in the mitigation or recovery strategy.

SCENARIOS

To illustrate our business continuity planning, the following scenarios and mitigations have been taken into consideration:

Scenario	Mitigation or recovery strategy
Loss of internet access at any location	Relocate to an alternative hub or suitable remote location to resume normal business operations. Alternatively, use a secure MiFi device to regain internet access.
Loss of access to a hub	Relocate to an alternative hub or suitable remote location to resume normal business operations.
Loss of one or more business-dependent third-party, cloud-based services	Protection is via the Service Level Agreement (SLA) with the third party service provider. We only select vendors who can guarantee a reasonable time-to-recover for both service and data, in the event of loss-of-service. Measures beyond this are not deemed proportionate or cost-effective (e.g. a backup service provider or alternative data store) and the mitigation strategy would represent an additional risk in its own right.
Loss of team's core collaboration tool - Slack	In addition to SLA protection, the business can easily switch to other viable alternatives: email, other messaging services. No business-critical data is stored in Slack.
Loss of team's core productivity suite - Google Workspace (Incl. email, calendar, productivity & document repository)	Data retention policy for all deleted items is set to 12 months, allowing for recovery of data inadvertently deleted. Service levels are such that no service outage will significantly affect business-as-usual operations. In the

	extremely unlikely event there is a material outage, operations would be switched to Microsoft 365 to enable operations to continue.
Loss of Customer Relationship Management (CRM) - Pipedrive	In addition to SLA protection, business development data (contacts, pipeline, sales data) exists in alternative formats typically updated on a minimum monthly cycle (e.g. Excel spreadsheet reports). Revenue pipelines, client contact information, opportunity lifecycle data can be reconstructed from alternative data sources (e.g. monthly reporting packs, email contact lists, opportunity tracking spreadsheets).
Loss of the project accounting tool - Harvest	Protection is via the Service Level Agreement with the third party service provider. The business can revert to manual tracking of time and billing of clients using back-up spreadsheet based processes to ensure timely invoices are sent to clients.
Loss of the HR management system - HiBob	Protection is via the Service Level Agreement with the third party service provider. The business can revert to manual tracking of HR related activities (on and offboarding etc.) using spreadsheet based processes whilst the core system is restored.
Loss of the finance management system - Oracle Netsuite	Protection is via the Service Level Agreement with the third party service provider. The business can revert to manual tracking processing and accounting practices using a temporary alternative supplier (E.g. Xero) and/or spreadsheet based processes to ensure financial processes continue whilst the core system is restored.
Loss of video conferencing - Google Meets	Users can switch to an alternative service (e.g. Zoom, Teams, Appear.in, GoToMeeting, etc.).
Loss/theft/failure of key items of equipment (I.e. devices – since TPXimpact has no network or server infrastructure)	Purchase temporary/permanent replacement devices, configure with user access permissions, recover data from cloud services and continue.

Sudden removal or unavailability of key staff engaged in delivery (or provision of critical internal services to TPXimpact)	If there is sufficient warning, arrange a handover. Delivery teams work in a highly collaborative fashion, working in the open and sharing work-in-progress. This promotes knowledge sharing which will help other team members pick up the additional responsibilities.
Churn of key staff with business critical knowledge	Staff in key roles must document their processes clearly to ensure other members of staff can cover in the event they are not available and/or they leave the business. Recruitment underneath key roles must be ongoing to ensure succession plans are in place. Staff in more senior key roles must have longer notice periods (I.e. 3/6 months), preferably with specific handover criteria that must be met in the event their employment comes to an end.
Loss of a subcontractor during service delivery	TPXimpact ensures that robust contractual arrangements with suitable termination clauses and notices etc. are in place to allow for a subcontractor to be carefully off-boarded and a replacement sub-contractor brought in. TPXimpact work with a number of subcontractors on a wide range of engagements across our client-base. We nurture these relationships carefully to ensure we can rely on them to deliver our overarching service. In the event that a sub-contractor was to be off-boarded, this would be transparently communicated to any affected client(s) to ensure it is managed openly and the quality of our service does not drop during the transition period.

PART B – LONG FORM SECURITY REQUIREMENTS

1. DEFINITIONS

1.1 In this Part B of Schedule S3 (Security Requirements), the following definitions shall apply:

"Baseline Security Requirements"	the baseline security requirements set out in Annex 1 of this Part B Schedule S3 (Security Requirements);
"ISMS"	the information security management system and process developed by the Supplier in accordance with Paragraph 3 (ISMS) as updated from time to time in accordance with this Part B Schedule S3 (Security Requirements);
"Security Management Plan"	the Supplier's security management plan prepared pursuant to this Part B Schedule S3 (Security Requirements), a draft of which has been provided by the Supplier to the Buyer and is set out in the Order Form and as updated from time to time; and
"Security Tests"	tests to validate the ISMS and security of all relevant processes, systems, incident response plans, patches to vulnerabilities and mitigations to Breaches of Security.

1.2

2. SECURITY REQUIREMENTS

2.1 The Parties acknowledge that the purpose of the ISMS and Security Management Plan are to ensure a good organisational approach to security under which the specific requirements of this Contract will be met.

2.2 The Parties shall each appoint a security representative to be responsible for security.

2.3 The Buyer shall clearly articulate its high level security requirements so that the Supplier can ensure that the ISMS, security related activities and any mitigations are driven by these fundamental needs.

2.4 Both Parties shall provide a reasonable level of access to any members of their staff for the purposes of designing, implementing and managing security.

2.5 The Supplier shall use as a minimum Good Industry Practice in the day to day operation of any system holding, transferring or processing Buyer Data and any system that could directly or indirectly have an impact on that information, and shall ensure that Buyer Data remains under the effective control of the Supplier at all times.

2.6 The Supplier shall ensure the up-to-date maintenance of a security policy relating to the operation of its own organisation and systems and on request shall supply this document as soon as practicable to the Buyer.

2.7 The Buyer and the Supplier acknowledge that information security risks are shared between the Parties and that a compromise of either the Supplier or the Buyer's security provisions represents an unacceptable risk to the Buyer requiring immediate communication and co-operation between the Parties.

3. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

3.1 The Supplier shall develop and submit to the Buyer, within twenty (20) Working Days after the Commencement Date, an information security management system for the purposes of this Contract and shall comply with the requirements of Paragraphs 3.4 to 3.7.

3.2 The Supplier acknowledges that the Buyer places great emphasis on the reliability of the performance of the Services, confidentiality, integrity and availability of information and consequently on the security provided by the ISMS and that the Supplier shall be responsible for the effective performance of the ISMS.

3.3 The Buyer acknowledges that:

3.3.1 if the Buyer has not stipulated that it requires a bespoke ISMS, the ISMS provided by the Supplier may be an extant ISMS covering the Services and their implementation across the Supplier's estate; and

3.3.2 where the Buyer has stipulated that it requires a bespoke ISMS then the Supplier shall be required to present the ISMS for the Buyer's approval.

3.4 The ISMS shall:

3.4.1 if the Buyer has stipulated that it requires a bespoke ISMS, be developed to protect all aspects of the Services and all processes associated with the provision of the associated with the delivery of the Services, including the Buyer Premises, the Sites,

the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, information and data (including the Buyer's Confidential Information and the Buyer Data) to the extent used by the Buyer or the Supplier in connection with this Contract;

3.4.2 meet the relevant standards in ISO/IEC 27001 and ISO/IEC27002 in accordance with Paragraph 1.7;

3.5 at all times provide a level of security which:

3.5.1 is in accordance with the Law and this Contract;

3.5.2 complies with the Baseline Security Requirements;

3.5.3 as a minimum demonstrates Good Industry Practice;

3.5.4 complies with the Security Policy and the ICT Policy;

3.5.5 complies with at least the minimum set of security measures and standards as determined by the Security Policy Framework (Tiers 1-4) (https://www.gov.uk/government/publications/security-policy-framework/hmg-security-policy-framework);

3.5.6 takes account of guidance issued by the Centre for Protection of National Infrastructure (https://www.cpni.gov.uk);

3.5.7 complies with HMG Information Assurance Maturity Model and Assurance Framework (https://www.ncsc.gov.uk/articles/hmg-ia-maturity-model-iamm);

3.5.8 meets any specific security threats of immediate relevance to the ISMS, the Deliverables and/or Government Data;

3.5.9 addresses issues of incompatibility with the Supplier's own organisational security policies; and

3.5.10 complies with ISO/IEC27001 and ISO/IEC27002 in accordance with Paragraph 3.12;

3.5.11 document the security incident management processes and incident response plans;

3.5.12 document the vulnerability management policy including processes for identification of system vulnerabilities and assessment of the potential impact on the Services of any new threat, vulnerability or exploitation technique of which the Supplier becomes aware, prioritisation of security patches, testing of security patches, application of security patches, a process for Buyer approvals of exceptions, and the reporting and audit mechanism detailing the efficacy of the patching policy; and

3.5.13 be certified by (or by a person with the direct delegated authority of) a Supplier's main board representative, being the "Chief Security Officer", "Chief Information Officer", "Chief Technical Officer" or "Chief Financial Officer" (or equivalent as agreed in writing by the Buyer in advance of issue of the relevant Security Management Plan).

3.6 Subject to Paragraph 2, the references to Standards, guidance and policies contained or set out in Paragraph 3.4 shall be deemed to be references to such items as developed and updated and to any successor to or replacement for such standards, guidance and policies, as notified to the Supplier from time to time.

3.7 In the event that the Supplier becomes aware of any inconsistency in the provisions of the standards, guidance and policies set out in Paragraph 3.4, the Supplier shall immediately notify the Buyer Representative of such inconsistency and the Buyer Representative shall, as soon as practicable, notify the Supplier as to which provision the Supplier shall comply with.

3.8 If the bespoke ISMS submitted to the Buyer pursuant to Paragraph 3.3.1 is approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Part B Schedule S3 (Security Requirements). If the ISMS is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission of the ISMS to the Buyer. If the Buyer does not approve the ISMS following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Buyer pursuant to this Paragraph 3 may be unreasonably withheld or delayed. However any failure to approve the ISMS on the grounds that it does not comply with any of the requirements set out in Paragraphs 3.4 to 3.7 shall be deemed to be reasonable.

3.9 Approval by the Buyer of the ISMS pursuant to Paragraph 1.3.7 or of any change to the ISMS shall not relieve the Supplier of its obligations under this Part B Schedule S3 (Security Requirements).

4. SECURITY MANAGEMENT PLAN

4.1 Within twenty (20) Working Days after the Commencement Date, the Supplier shall prepare and submit to the Buyer for approval in accordance with Paragraph 4 fully developed, complete and up-to-date Security Management Plan which shall comply with the requirements of Paragraph 4.2.

4.2 The Security Management Plan shall:

4.2.1 be based on the initial Security Management Plan set out in the Order Form;

4.2.2 comply with the Baseline Security Requirements and, where specified by the Buyer in accordance with Paragraph 3.5.4, the Security Policy;

4.2.3 identify the necessary delegated organisational roles defined for those responsible for ensuring this Part B Schedule S3 (Security Requirements) is complied with by the Supplier;

4.2.4 detail the process for managing any security risks from Sub-Contractors and third parties authorised by the Buyer with access to the Goods and/or Services, processes associated with the delivery of the Goods and/or Services, the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, Information and data (including the Buyer's Confidential Information and the Buyer Data) and any system that could directly or indirectly have an impact on that information, data and/or the Services;

4.2.5 unless otherwise specified by the Buyer in writing, be developed to protect all aspects of the Services and all processes associated with the delivery of the Services, including the Buyer Premises, the Sites, the Supplier System, the Buyer System (to the extent that it is under the control of the Supplier) and any IT, Information and

data (including the Buyer's Confidential Information and the Buyer Data) to the extent used by the Buyer or the Supplier in connection with this Contract or in connection with any system that could directly or indirectly have an impact on that Information, data and/or the Services;

4.2.6 set out the security measures to be implemented and maintained by the Supplier in relation to all aspects of the Services and all processes associated with the delivery of the Services and at all times comply with and specify security measures and procedures which are sufficient to ensure that the Services comply with the provisions of this Part B Schedule S3 (Security Requirements) (including the requirements set out in Paragraph 3.4);

4.2.7 demonstrate that the Supplier's approach to delivery of the Services has minimised the Buyer and Supplier effort required to comply with this Part B Schedule S3 (Security Requirements) through consideration of available, appropriate and practicable pan-government accredited services (for example, 'platform as a service' offering from the G-Cloud catalogue);

4.2.8 set out the plans for transitioning all security arrangements and responsibilities from those in place at the Commencement Date to those incorporated in the ISMS within the timeframe agreed between the Parties;

4.2.9 set out the scope of the Buyer System that is under the control of the Supplier;

4.2.10 be structured in accordance with ISO/IEC27001 and ISO/IEC27002, cross-referencing if necessary to other Schedules of this Contract which cover specific areas included within those standards; and

4.2.11 be written in plain English in language which is readily comprehensible to the staff of the Supplier and the Buyer engaged in the Services and shall reference only documents which are in the possession of the Parties or whose location is otherwise specified in this Part B Schedule S3 (Security Requirements).

4.3 If the Security Management Plan submitted to the Buyer pursuant to Paragraph 4.1 is approved by the Buyer, it shall be adopted by the Supplier immediately and thereafter operated and maintained in accordance with this Part B Schedule S3 (Security Requirements). If the Security Management Plan is not approved by the Buyer, the Supplier shall amend it within ten (10) Working Days of a notice of non-approval from the Buyer and re-submit it to the Buyer for approval. The Parties shall use all reasonable endeavours to ensure that the approval process takes as little time as possible and in any event no longer than fifteen (15) Working Days from the date of the first submission to the Buyer of the Security Management Plan. If the Buyer does not approve the Security Management Plan following its resubmission, the matter shall be resolved in accordance with the Dispute Resolution Procedure. No approval to be given by the Buyer pursuant to this Paragraph may be unreasonably withheld or delayed. However any failure to approve the Security Management Plan on the grounds that it does not comply with the requirements set out in Paragraph 4.2 shall be deemed to be reasonable.

4.4 Approval by the Buyer of the Security Management Plan pursuant to Paragraph 4.3 or of any change or amendment to the Security Management Plan shall not relieve the Supplier of its obligations under this Part B Schedule S3 (Security Requirements).

5. AMENDMENT OF THE ISMS AND SECURITY MANAGEMENT PLAN

5.1 The ISMS and Security Management Plan shall be fully reviewed and updated by the Supplier and at least annually to reflect:

5.1.1 emerging changes in Good Industry Practice;

5.1.2 any change or proposed change to the Supplier System, the Services and/or associated processes;

5.1.3 any new perceived or changed security threats;

5.1.4 where required in accordance with Paragraph 3.5.4, any changes to the Security Policy;

5.1.5 any new perceived or changed security threats; and

5.1.6 any reasonable change in requirement requested by the Buyer.

5.2 The Supplier shall provide the Buyer with the results of such reviews as soon as reasonably practicable after their completion and amend the ISMS and Security Management Plan at no additional cost to the Buyer. The results of the review shall include, without limitation:

5.2.1 suggested improvements to the effectiveness of the ISMS;

5.2.2 updates to the risk assessments;

5.2.3 proposed modifications to the procedures and controls that affect information security to respond to events that may impact on the ISMS; and

5.2.4 suggested improvements in measuring the effectiveness of controls.

5.3 Subject to Paragraph 5.4, any change which the Supplier proposes to make to the ISMS or Security Management Plan (as a result of a review carried out pursuant to Paragraph 5.1, a Buyer request, a change to the Baseline Security Requirements or otherwise) shall be subject to the Change Control Procedure and shall not be implemented until approved in writing by the Buyer.

5.4 The Buyer may, acting reasonably, approve and require changes or amendments to the ISMS or Security Management Plan to be implemented on timescales faster than set out in the Change Control Procedure but, without prejudice to their effectiveness, all such changes and amendments shall thereafter be subject to the Change Control Procedure for the purposes of formalising and documenting the relevant change or amendment.

6. SECURITY TESTING

6.1 The Supplier shall conduct Security Tests from time to time (and at least annually across the scope of the ISMS) and additionally after any change or amendment to the ISMS (including security incident management processes and incident response plans) or the Security Management Plan. Security Tests shall be designed and implemented by the Supplier so as to minimise the impact on the delivery of the Services and the date, timing, content and conduct of such Security Tests shall be agreed in advance with the Buyer. Subject to compliance by the Supplier with the foregoing requirements, if any Security Tests adversely affect the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Security Tests.

6.2 The Buyer shall be entitled to send a representative to witness the conduct of the Security Tests. The Supplier shall provide the Buyer with the results of such Security Tests (in a form approved by the Buyer in advance) as soon as practicable after completion of each Security Test.

6.3 Without prejudice to any other right of audit or access granted to the Buyer pursuant to this Contract, the Buyer and/or its authorised representatives shall be entitled, at any time upon giving reasonable notice to the Supplier, to carry out such tests (including penetration tests) as it may deem necessary in relation to the ISMS and the Supplier's compliance with the ISMS and the Security Management Plan. The Buyer may notify the Supplier of the results of such tests after completion of each such test. If any such Buyer's test adversely affects the Supplier's ability to deliver the Services so as to meet the Service Levels, the Supplier shall be granted relief against any resultant under-performance for the period of the Buyer's test.

6.4 Where any Security Test carried out pursuant to Paragraphs 6.2 or 6.3 reveals any actual or potential Breach of Security or weaknesses (including un-patched vulnerabilities, poor configuration and/or incorrect system management), the Supplier shall promptly notify the Buyer of any changes to the ISMS and to the Security Management Plan (and the implementation thereof) which the Supplier proposes to make in order to correct such failure or weakness. Subject to the Buyer's prior written approval, the Supplier shall implement such changes to the ISMS and the Security Management Plan and repeat the relevant Security Tests in accordance with the timetable agreed with the Buyer or, otherwise, as soon as reasonably possible. For the avoidance of doubt, where the change to the ISMS or Security Management Plan is to address a non-compliance with the Security Policy or Baseline Security Requirements or the requirements of this Part B Schedule S3 (Security Requirements), the change to the ISMS or Security Management Plan shall be at no cost to the Buyer.

6.5 If any repeat Security Test carried out pursuant to Paragraph 6.4 reveals an actual or potential Breach of Security exploiting the same root cause failure, such circumstance shall constitute a material Default of this Contract.

7. COMPLYING WITH THE ISMS

7.1 The Buyer shall be entitled to carry out such security audits as it may reasonably deem necessary in order to ensure that the ISMS maintains compliance with the principles and practices of ISO 27001 and/or the Security Policy where such compliance is required in accordance with Paragraph [ ].

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

7.3 If, as a result of any such independent audit as described in Paragraph 7.1, the Supplier is found to be non-compliant with the principles and practices of ISO/IEC 27001 and/or, where relevant, the Security Policy then the Supplier shall, at its own expense, undertake those actions required in order to achieve the necessary compliance and shall reimburse in full the costs incurred by the Buyer in obtaining such audit.

8. SECURITY BREACH

8.1 Either Party shall notify the other in accordance with the agreed security incident management process as defined by the ISMS upon becoming aware of any breach of security or any potential or attempted Breach of Security.

8.2 Without prejudice to the security incident management process, upon becoming aware of any of the circumstances referred to in Paragraph 8.1, the Supplier shall:

8.2.1 immediately take all reasonable steps (which shall include any action or changes reasonably required by the Buyer) necessary to:

8.2.2 minimise the extent of actual or potential harm caused by any Breach of Security;

8.2.3 remedy such Breach of Security or any potential or attempted Breach of Security in order to protect the integrity of the Buyer Assets and/or ISMS to the extent that this is within the Supplier's control;

8.2.4 apply a tested mitigation against any such Breach of Security or attempted Breach of Security and provided that reasonable testing has been undertaken by the Supplier, if the mitigation adversely affects the Supplier's ability to provide the Services so as to meet the relevant Service Levels, the Supplier shall be granted relief against any resultant under-performance for such period as the Buyer, acting reasonably, may specify by written notice to the Supplier;

8.2.5 prevent a further Breach of Security or any potential or attempted Breach of Security in the future exploiting the same root cause failure; and

8.2.6 supply any requested data to the Buyer (or the Computer Emergency Response Team for UK Government ("GovCertUK")) on the Buyer's request within two (2) Working Days and without charge (where such requests are reasonably related to a possible incident or compromise); and

8.2.7 as soon as reasonably practicable provide to the Buyer full details (using the reporting mechanism defined by the ISMS) of the Breach of Security or attempted Breach of Security, including a root cause analysis where required by the Buyer.

8.3 In the event that any action is taken in response to a Breach of Security or potential or attempted Breach of Security that demonstrates non-compliance of the ISMS with the Security Policy (where relevant) or the requirements of this Part B Schedule S3 (Security Requirements), then any required change to the ISMS shall be at no cost to the Buyer.

9. VULNERABILITIES AND FIXING THEM

9.1 The Buyer and the Supplier acknowledge that from time to time vulnerabilities in the IT Environment will be discovered which unless mitigated will present an unacceptable risk to the Buyer's information.

9.2 The severity of threat vulnerabilities for the Supplier COTS Software and/or Third Party COTS Software shall be categorised by the Supplier as 'Critical', 'Important' and 'Other' by aligning these categories to the vulnerability scoring according to the agreed method in the ISMS and using the appropriate vulnerability scoring systems including:

9.2.1 the 'National Vulnerability Database' 'Vulnerability Severity Ratings': 'High', 'Medium' and 'Low' respectively (these in turn are aligned to CVSS scores as set out by NIST http://nvd.nist.gov/cvss.cfm); and

9.2.2 Microsoft's 'Security Bulletin Severity Rating System' ratings 'Critical', 'Important', and the two remaining levels ('Moderate' and 'Low') respectively.

9.3 The Supplier shall procure the application of security patches to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorised as 'Critical' within 14 days of release, 'Important' within 30 days of release and all 'Other' within 60 Working Days of release, except where:

9.3.1 the Supplier can demonstrate that a vulnerability is not exploitable within the context of any Service (e.g. because it resides in a software component which is not running in the service) provided vulnerabilities which the Supplier asserts cannot be exploited within the context of a Service must be remedied by the Supplier within the above timescales if the vulnerability becomes exploitable within the context of the Service;

9.3.2 the application of a 'Critical' or 'Important' security patch adversely affects the Supplier's ability to deliver the Services in which case the Supplier shall be granted an extension to such timescales of 5 days, provided the Supplier had followed and continues to follow the security patch test plan agreed with the Buyer; or

9.3.3 the Buyer agrees a different maximum period after a case-by-case consultation with the Supplier under the processes defined in the ISMS.

9.4 The Specification and Mobilisation Plan (if applicable) shall include provisions for major version upgrades of all Supplier COTS Software and/or Third Party COTS Software to be upgraded within 6 Months of the release of the latest version, such that it is no more than one major version level below the latest release (normally codified as running software no older than the 'n-1 version') throughout the Term unless:

9.4.1 where upgrading such Supplier COTS Software and/or Third Party COTS Software reduces the level of mitigations for known threats, vulnerabilities or exploitation techniques, provided always that such upgrade is made within 12 Months of release of the latest version; or

9.4.2 is agreed with the Buyer in writing.

9.5 The Supplier shall:

9.5.1 implement a mechanism for receiving, analysing and acting upon threat information supplied by GovCertUK, or any other competent Central Government Body;

9.5.2 ensure that the IT Environment (to the extent that the IT Environment is within the control of the Supplier) is monitored to facilitate the detection of anomalous behaviour that would be indicative of system compromise;

9.5.3 ensure it is knowledgeable about the latest trends in threat, vulnerability and exploitation that are relevant to the IT Environment by actively monitoring the threat landscape during the Contract Period;

9.5.4 pro-actively scan the IT Environment (to the extent that the IT Environment is within the control of the Supplier) for vulnerable components and address discovered vulnerabilities through the processes described in the ISMS as developed under Paragraph 3.5.12;

9.5.5 from the date specified in the Security Management Plan provide a report to the Buyer within five (5) Working Days of the end of each month detailing both patched and outstanding vulnerabilities in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and any elapsed time between the public release date of patches and either time of application or for outstanding vulnerabilities the time of issue of such report;

9.5.6 propose interim mitigation measures to vulnerabilities in the IT Environment known to be exploitable where a security patch is not immediately available;

9.5.7 remove or disable any extraneous interfaces, services or capabilities that are not needed for the provision of the Services (in order to reduce the attack surface of the IT Environment); and

9.5.8 inform the Buyer when it becomes aware of any new threat, vulnerability or exploitation technique that has the potential to affect the security of the IT Environment and provide initial indications of possible mitigations.

9.6 If the Supplier is unlikely to be able to mitigate the vulnerability within the timescales under this Paragraph 9, the Supplier shall immediately notify the Buyer.

9.7 A failure to comply with Paragraph 9.3 shall constitute a Default, and the Supplier shall comply with the Rectification Plan Process.

9.8

ANNEX 1 – BASELINE SECURITY REQUIREMENTS

1. HANDLING CLASSIFIED INFORMATION

1.1 The Supplier shall not handle Buyer information classified SECRET or TOP SECRET except if there is a specific requirement and in this case prior to receipt of such information the Supplier shall seek additional specific guidance from the Buyer.

2. END USER DEVICES

2.1 When Buyer Data resides on a mobile, removable or physically uncontrolled device it must be stored encrypted using a product or system component which has been formally assured through a recognised certification process of the National Cyber Security Centre ("NCSC") to at least Foundation Grade, for example, under the NCSC Commercial Product Assurance scheme ("CPA").

2.2 Devices used to access or manage Buyer Data and services must be under the management authority of Buyer or Supplier and have a minimum set of security policy configuration enforced. These devices must be placed into a 'known good' state prior to being provisioned into the management authority of the Buyer. Unless otherwise agreed with the Buyer in writing, all Supplier devices are expected to meet the set of security requirements set out in the End User Devices Security Guidance (https://www.ncsc.gov.uk/guidance/end-user-device-security). Where the guidance highlights shortcomings in a particular platform the Supplier may wish to use, then these should be discussed with the Buyer and a joint decision shall be taken on whether the residual risks are acceptable. Where the Supplier wishes to deviate from the NCSC guidance, then this should be agreed in writing on a case by case basis with the Buyer.

3. DATA PROCESSING, STORAGE, MANAGEMENT AND DESTRUCTION

3.1 The Supplier and Buyer recognise the need for the Buyer's information to be safeguarded under the UK Data Protection regime or a similar regime. To that end, the Supplier must be able to state to the Buyer the physical locations in which data may be stored, processed and managed from, and what legal and regulatory frameworks Buyer Data will be subject to at all times.

3.2 The Supplier shall agree any change in location of data storage, processing and administration with the Buyer in accordance with the Change Control Procedure.

3.3 The Supplier shall:

3.3.1 provide the Buyer with all Buyer Data on demand in an agreed open format;

3.3.2 have documented processes to guarantee availability of Buyer Data in the event of the Supplier ceasing to trade;

3.3.3 securely destroy all media that has held Buyer Data at the end of life of that media in line with Good Industry Practice; and

3.3.4 securely erase any or all Buyer Data held by the Supplier when requested to do so by the Buyer.

4. ENSURING SECURE COMMUNICATIONS

4.1 The Buyer requires that any Buyer Data transmitted over any public network (including the Internet, mobile networks or un-protected enterprise network) or to a mobile device must be encrypted using

a product or system component which has been formally assured through a certification process recognised by NCSC, to at least Foundation Grade, for example, under CPA.

4.2 The Buyer requires that the configuration and use of all networking equipment to provide the Services, including those that are located in secure physical locations, are at least compliant with Good Industry Practice.

5. SECURITY BY DESIGN

5.1 The Supplier shall apply the 'principle of least privilege' (the practice of limiting systems, processes and user access to the minimum possible level) to the design and configuration of IT systems which will process or store Buyer Data.

5.2 When designing and configuring the IT Environment (to the extent that the IT Environment is within the control of the Supplier) the Supplier shall follow Good Industry Practice and seek guidance from recognised security professionals with the appropriate skills and/or a NCSC certification (https://www.ncsc.gov.uk/section/products-services/ncsc-certification) for all bespoke or complex components of the IT Environment (to the extent that the IT Environment is within the control of the Supplier).

6. SECURITY OF SUPPLIER PERSONNEL

6.1 Supplier Personnel shall be subject to pre-employment checks that include, as a minimum: identity, unspent criminal convictions and right to work.

6.2 The Supplier shall agree on a case by case basis Supplier Personnel roles which require specific government clearances (such as 'SC') including system administrators with privileged access to IT systems which store or process Buyer Data.

6.3 The Supplier shall prevent Supplier Personnel who are unable to obtain the required security clearances from accessing systems which store, process, or are used to manage Buyer Data except where agreed with the Buyer in writing.

6.4 All Supplier Personnel that have the ability to access Buyer Data or systems holding Buyer Data shall undergo regular training on secure information management principles. Unless otherwise agreed with the Buyer in writing, this training must be undertaken annually.

6.5 Where the Supplier or Sub-Contractors grants increased IT privileges or access rights to Supplier Personnel, those Supplier Personnel shall be granted only those permissions necessary for them to carry out their duties. When Supplier Personnel no longer need elevated privileges or leave the organisation, their access rights shall be revoked within one (1) Working Day.

7. RESTRICTING AND MONITORING ACCESS

7.1 The Supplier shall operate an access control regime to ensure all users and administrators of the IT Environment (to the extent that the IT Environment is within the control of the Supplier) are uniquely identified and authenticated when accessing or administering the Services. Applying the 'principle of least privilege', users and administrators shall be allowed access only to those parts of the IT Environment that they require. The Supplier shall retain an audit record of accesses.

8. AUDIT

8.1 The Supplier shall collect audit records which relate to security events in the systems or that would support the analysis of potential and actual compromises. In order to facilitate effective monitoring and forensic readiness such Supplier audit records should (as a minimum) include:

8.1.1 Logs to facilitate the identification of the specific asset which makes every outbound request external to the IT Environment (to the extent that the IT Environment is within the control of the Supplier). To the extent the design of the Services allows such logs shall include those from DHCP servers, HTTP/HTTPS proxy servers, firewalls and routers.

8.1.2 Security events generated in the IT Environment (to the extent that the IT Environment is within the control of the Supplier) and shall include: privileged account log-on and log-off events, the start and termination of remote access sessions, security alerts from desktops and server operating systems and security alerts from third party security software.

8.2 The Supplier and the Buyer shall work together to establish any additional audit and monitoring requirements for the IT Environment.

8.3 The Supplier shall retain audit records collected in compliance with this Paragraph 8 for a period of at least 6 months.

ADDITIONAL CLAUSES AND SCHEDULES – CLAUSES

C1

1. RELEVANT CONVICTIONS

1.1 For the purpose of this Clause, the following definitions shall apply:

"Conviction"	1 means other than for minor road traffic offences, any previous or pending prosecutions, convictions, cautions and binding over orders (including any spent convictions as contemplated by section 1(1) of the Rehabilitation of Offenders Act 1974 by virtue of the exemptions specified in Part II of Schedule 1 of the Rehabilitation of Offenders Act 1974 (Exemptions) Order 1975 (SI 1975/1023) or any replacement or amendment to that Order, or being placed on a list kept pursuant to section 1 of the Protection of Children Act 1999 or being placed on a list kept pursuant to the Safeguarding Vulnerable Groups Act 2006; and
"Relevant Conviction"	2 means a Conviction that is relevant to the nature of the Services to be provided or as specified by the Buyer in the Order Form.

1.2 The Supplier shall ensure that no person who discloses that he has a Relevant Conviction, or who is found to have any Relevant Convictions (whether as a result of a police check or through the procedure of the Disclosure and Barring Service (DBS) or otherwise), is employed or engaged in any part of the provision of the Services without the approval of the Buyer.

1.3 Notwithstanding Clause 1.3.1, for each member of Supplier Personnel who, in providing the Services, has, will have or is likely to have access to children, vulnerable persons or other members of the public to whom the Buyer owes a special duty of care, the Supplier shall (and shall procure that the relevant Sub-Contractor shall):

1.3.1 carry out a check with the records held by the Department for Education (DfE);

1.3.2 conduct thorough questioning regarding any Relevant Convictions; and

1.3.3 ensure a police check is completed and such other checks as may be carried out through the Disclosure and Barring Service (DBS),

1.3 and the Supplier shall not (and shall ensure that any Sub-Contractor shall not) engage or continue to employ in the provision of the Services any person who has a Relevant Conviction or an inappropriate record.

C2

1. SECURITY MEASURES

1.1 For the purpose of this Clause, the following definitions shall apply:

"Document"	3 includes specifications, plans, drawings, photographs and books;
"Secret Matter"	4 means any matter connected with or arising out of the performance of this Contract which has been, or may hereafter

be, by a notice in writing given by the Buyer to the Supplier be designated 'top secret' or 'secret'; and

"Servant" 5 where the Supplier is a body corporate shall include a director of that body and any person occupying in relation to that body the position of director by whatever name called.

1.2 The Supplier shall not, either before or after the completion or termination of this Contract, do or permit to be done anything which it knows or ought reasonably to know may result in information about a Secret Matter being:

1.2.1 without the prior consent in writing of the Buyer, disclosed to or acquired by a person who is an alien or who is a British subject by virtue only of a certificate of naturalisation in which his name was included;

1.2.2 disclosed to or acquired by a person as respects whom the Buyer has given to the Supplier a notice in writing which has not been cancelled stating that the Buyer requires that Secret Matters shall not be disclosed to that person;

1.2.3 without the prior consent in writing of the Buyer, disclosed to or acquired by any person who is not a servant of the Supplier; or

1.2.4 disclosed to or acquired by a person who is an employee of the Supplier except in a case where it is necessary for the proper performance of this Contract that such person shall have the information.

1.3 Without prejudice to the provisions of Clause 1.2, the Supplier shall, both before and after the completion or termination of this Contract, take all reasonable steps to ensure:

1.3.1 no such person as is mentioned in Clause 1.2 hereof shall have access to any item or document under the control of the Supplier containing information about a Secret Matter except with the prior consent in writing of the Buyer;

1.3.2 that no visitor to any premises in which there is any item to be supplied under this Contract or where Services are being supplied shall see or discuss with the Supplier or any person employed by him any Secret Matter unless the visitor is authorised in writing by the Buyer so to do;

1.3.3 that no photograph of any item to be supplied under this Contract or any portions of the Services shall be taken except insofar as may be necessary for the proper performance of this Contract or with the prior consent in writing of the Buyer, and that no such photograph shall, without such consent, be published or otherwise circulated;

1.3.4 that all information about any Secret Matter and every document model or other item which contains or may reveal any such information is at all times strictly safeguarded, and that, except insofar as may be necessary for the proper performance of this Contract or with the prior consent in writing of the Buyer, no copies of or extracts from any such document, model or item shall be made or used and no designation of description which may reveal information about the nature or contents of any such document, model or item shall be placed thereon; and

1.3.5 that if the Buyer gives notice in writing to the Supplier at any time requiring the delivery to the Buyer of any such document, model or item as is mentioned in Clause 1.3.3, that document, model or item (including all copies of or extracts therefrom)

shall forthwith be delivered to the Buyer who shall be deemed to be the owner thereof and accordingly entitled to retain the same.

1.4 The decision of the Buyer on the question whether the Supplier has taken or is taking all reasonable steps as required by the foregoing provisions of this Clause 1.2 shall be final and conclusive.

1.5 If and when directed by the Buyer, the Supplier shall furnish full particulars of all people who are at any time concerned with any Secret Matter.

1.6 If and when directed by the Buyer, the Supplier shall secure that any person employed by it who is specified in the direction, or is one of a class of people who may be so specified, shall sign a statement that he understands that the Official Secrets Act, 1911 to 1989 and, where applicable, the Atomic Energy Act 1946, apply to the person signing the statement both during the carrying out and after expiry or termination of this Contract.

1.7 If, at any time either before or after the expiry or termination of this Contract, it comes to the notice of the Supplier that any person acting without lawful authority is seeking or has sought to obtain information concerning this Contract or anything done or to be done in pursuance thereof, the matter shall be forthwith reported by the Supplier to the Buyer and the report shall, in each case, be accompanied by a statement of the facts, including, if possible, the name, address and occupation of that person, and the Supplier shall be responsible for making all such arrangements as it may consider appropriate to ensure that if any such occurrence comes to the knowledge of any person employed by it, that person shall forthwith report the matter to the Supplier with a statement of the facts as aforesaid.

1.8 The Supplier shall place every person employed by it, other than a Sub-Contractor, who in its opinion has or will have such knowledge of any Secret Matter as to appreciate its significance, under a duty to the Supplier to observe the same obligations in relation to that matter as are imposed on the Supplier by Clauses 1.2 and 1.3 and shall, if directed by the Buyer, place every person who is specified in the direction or is one of a class of people so specified, under the like duty in relation to any Secret Matter which may be specified in the direction, and shall at all times use its best endeavours to ensure that every person upon whom obligations are imposed by virtue of this Clause C2 observes the said obligations, and the Supplier shall give such instructions and information to every such person as may be necessary for that purpose, and shall, immediately upon becoming aware of any act or omission which is or would be a breach of the said obligations, report the facts to the Supplier with all necessary particulars.

1.9 The Supplier shall, if directed by the Buyer, include in the Sub-Contract provisions in such terms as the Buyer may consider appropriate for placing the Sub-Contractor under obligations in relation to secrecy and security corresponding to those placed on the Supplier by this Clause C2, but with such variations (if any) as the Buyer may consider necessary. Further the Supplier shall:

1.9.1 give such notices, directions, requirements and decisions to its Sub-Contractors as may be necessary to bring the provisions relating to secrecy and security which are included in Sub-Contracts under this Clause C2 into operation in such cases and to such extent as the Buyer may direct;

1.9.2 if there comes to its notice any breach by the Sub-Contractor of the obligations of secrecy and security included in their Sub-Contracts in pursuance of this Clause C2, notify such breach forthwith to the Buyer; and

1.9.3 if and when so required by the Buyer, exercise its power to determine the Sub-Contract under the provision in that Sub-Contract which corresponds to Clause 1.12.

1.10 The Supplier shall give the Buyer such information and particulars as the Buyer may from time to time require for the purposes of satisfying the Buyer that the obligations imposed by or under the foregoing provisions of this Clause C2 have been and are being observed and as to what the Supplier has done or is doing or proposes to do to secure the observance of those obligations and to prevent any breach thereof, and the Supplier shall secure that a representative of the Buyer duly authorised in writing shall be entitled at reasonable times to enter and inspect any premises in which anything is being done or is to be done under this Contract or in which there is or will be any item to be supplied under this Contract, and also to inspect any document or item in any such premises or which is being made or used for the purposes of this Contract and that any such representative shall be given all such information as he may require on the occasion of, or arising out of, any such inspection.

1.11 Nothing in this Clause C2 shall prevent any person from giving any information or doing anything on any occasion when it is, by virtue of any enactment, the duty of that person to give that information or do that thing.

1.12 If the Buyer shall consider that any of the following events has occurred:

1.12.1 that the Supplier has committed a breach of, or failed to comply with any of, the foregoing provisions of this Clause C2; or

1.12.2 that the Supplier has committed a breach of any obligations in relation to secrecy or security imposed upon it by any other contract with the Buyer, or with any department or person acting on behalf of the Crown; or

1.12.3 that by reason of an act or omission on the part of the Supplier, or of a person employed by the Supplier, which does not constitute such a breach or failure as is mentioned in Clause 1.12.2, information about a Secret Matter has been or is likely to be acquired by a person who, in the opinion of the Buyer, ought not to have such information;

and shall also decide that the interests of the State require the termination of this Contract, the Buyer may by notice in writing terminate this Contract forthwith.

1.13 A decision of the Buyer to terminate this Contract in accordance with the provisions of Clause 1.12 shall be final and conclusive and it shall not be necessary for any notice of such termination to specify or refer in any way to the event or considerations upon which the Buyer's decision is based.

1.14 **Supplier's notice**

1.14.1 The Supplier may within five (5) Working Days of the termination of this Contract in accordance with the provisions of Clause 1.12, give the Buyer notice in writing requesting the Buyer to state whether the event upon which the Buyer's decision to terminate was based is an event mentioned in Clause 1.12 and to give particulars of that event; and

1.14.2 the Buyer shall within ten (10) Working Days of the receipt of such a request give notice in writing to the Supplier containing such a statement and particulars as are required by the request.

1.15 **Matters pursuant to termination**

1.15.1 The termination of this Contract pursuant to Clause 1.12 shall be without prejudice to any rights of either party which shall have accrued before the date of such termination;

1.15.2 The Supplier shall be entitled to be paid for any work or thing done under this Contract and accepted but not paid for by the Buyer at the date of such termination either at the price which would have been payable under this Contract if this Contract had not been terminated, or at a reasonable price;

1.15.3 The Buyer may take over any work or thing done or made under this Contract (whether completed or not) and not accepted at the date of such termination which the Buyer may by notice in writing to the Supplier given within thirty (30) Working Days from the time when the provisions of this Clause C2 shall have effect, elect to take over, and the Supplier shall be entitled to be paid for any work or thing so taken over a price which, having regard to the stage which that work or thing has reached and its condition at the time it is taken over, is reasonable. The Supplier shall in accordance with directions given by the Buyer, deliver any work or thing taken over under this Clause, and take all such other steps as may be reasonably necessary to enable the Buyer to have the full benefit of any work or thing taken over under this Clause; and

1.15.4 Save as aforesaid, the Supplier shall not be entitled to any payment from the Buyer after the termination of this Contract

1.15.5 If, after notice of termination of this Contract pursuant to the provisions of Clause 1.12:

(a) the Buyer shall not within ten (10) Working Days of the receipt of a request from the Supplier, furnish such a statement and particulars as are detailed in Clause 1.14; or

(b) the Buyer shall state in the statement and particulars detailed in Clause 1.14 that the event upon which the Buyer's decision to terminate this Contract was based on an event mentioned in Clause 1.12.3,

2 the respective rights and obligations of the Supplier and the Buyer shall be terminated in accordance with the following provisions:

(a) the Buyer shall take over from the Supplier at a fair and reasonable price all unused and undamaged materials, bought-out parts and components and articles in course of manufacture in the possession of the Supplier upon the termination of this Contract under the provisions of Clause 1.12 and properly provided by or supplied to the Supplier for the performance of this Contract, except such materials, bought-out parts and components and articles in course of manufacture as the Supplier shall, with the concurrence of the Buyer, elect to retain;

(b) the Supplier shall prepare and deliver to the Buyer within an agreed period or in default of agreement within such period as the Buyer may specify, a list of all such unused and undamaged materials, bought-out parts and components and articles in course of manufacture liable to be taken over by or previously belonging to the Buyer and shall deliver such materials and items in accordance with the directions of the Buyer who shall pay to the Supplier fair and reasonable handling and delivery charges incurred in complying with such directions;

(c) the Buyer shall indemnify the Supplier against any commitments, liabilities or expenditure which are reasonably and properly chargeable by the Supplier in connection with this Contract to the extent to which the said commitments, liabilities

or expenditure would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Contract;

(d) if hardship to the Supplier should arise from the operation of this Clause 1.15 it shall be open to the Supplier to refer the circumstances to the Buyer who, on being satisfied that such hardship exists shall make such allowance, if any, as in its opinion is reasonable and the decision of the Buyer on any matter arising out of this Clause shall be final and conclusive; and

(e) subject to the operation of Clauses 1.15.3, 1.15.4 and 1.15.5, termination of this Contract shall be without prejudice to any rights of either party that may have accrued before the date of such termination.