



Department
for Education

**The Secretary of State for
The Department for Education
And
Total Enterprise Solutions for**

Microsoft Dynamics License Enhancement Charges

Order Form

Supplier ID number:	773663587596097
Department for Education Contract reference:	PROJ_4856
Contract title:	Microsoft Dynamics Business Central Licence Enhancement
Contract description:	The services to be delivered under this Contract are payment of enhancement charges linked to DfE Microsoft Dynamics Business Central “On Premise” Essential “Full” licenses, Microsoft Dynamics Business Central “Team” licenses.
Start date:	14 th September 2020
Expiry date:	13 th September 2021
Contract value:	£103,657.88. + VAT
Charging method:	Fixed Price
Purchase order number:	TBC

From: the Buyer	The Secretary of State for the Department for Education Sanctuary Buildings Great Smith Street London SW1P 3BT
To: the Supplier	Total Enterprise Solutions Croft Farm Main Street Monk Fryston Leeds LS25 5DU Company number: 05403319

Together: the 'Parties'

Principle contact details

For the Buyer:	Title: <REDACTED> Name: <REDACTED> Email: <REDACTED> Phone: <REDACTED>
For the Supplier:	Title: <REDACTED> Name: <REDACTED> Email: <REDACTED> Phone: <REDACTED>

Contract term

Start date:	This Contract Starts on 14 th September 2020 and is valid for 12 months.
Ending (termination):	The notice period needed for Ending the Contract is 90 Working Days from the date of written notice for disputed sums or 30 days from the date of written notice for Ending without cause.
Extension period:	N/A

Buyer contractual details

Services required:	<p>The Services to be provided by the Supplier under this Contract are outlined below and in Schedule 1 (Services):</p> <ul style="list-style-type: none">• Microsoft Support & Maintenance – Enhancement Cost (calculated @ <REDACTED> of total license costs) <p>DfE Microsoft Dynamics Business Central licences purchased are perpetual. DfE retains ownership of these Capital Assets and the associated enhancements.</p>
Additional services:	N/A
Location:	Unless otherwise agreed, the Services shall be provided at the Buyer's offices in either London, Coventry, Sheffield, Manchester or other offices in the UK

	including the Supplier's offices.
Quality standards:	The quality standards required in this Contract are as described in Microsoft License T&Cs
Technical standards:	The technical standards required in this Contract are as described in Microsoft License T&Cs
Service level agreement:	The service level and availability criteria required for this Contract are as described in Microsoft License T&Cs
Onboarding:	The Supplier will deliver the licenses to the Buyer as specified in Schedule 1 of this Contract.
Off-boarding:	The offboarding & Exit plan for this Call-Off Contract will be agreed jointly.
Collaboration agreement:	Not applicable
Limit on Parties' liability:	<p>The annual total liability of either Party for all Property defaults will not exceed the sum of £1,000,000 in each Contract year in which the Default occurs.</p> <p>The annual total liability for Buyer Data defaults will not exceed £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Contract Term (whichever is the greater).</p> <p>The annual total liability for all other defaults will not exceed the greater of £1,000,000 or 125% of the Charges payable by the Buyer to the Supplier during the Contract Term (whichever is the greater).</p>
Insurance:	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> • a minimum insurance period of six 6 years following the expiration or Ending of this Contract • Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply these Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law) • employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law
Force majeure:	A Party may End this if the Other Party is affected by a Force Majeure Event that lasts for more than 10 consecutive days.
Audit:	Not Applicable
Buyer's responsibilities:	None
Buyer's equipment:	Not Applicable

Supplier's information


Subcontractors or partners:	N/A
------------------------------------	-----

Contract charges and payment

The Contract charges and payment details are in the table below.

Payment method:	The payment method for this Contract is by BACS.
Payment profile:	The payment profile for this Contract is Fixed Price.
Invoice details:	The Supplier will issue electronic invoices in arrears. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.
Who and where to send invoices to:	Electronic invoices will be sent to: <REDACTED>
Invoice information required – for example purchase order, project reference:	All invoices must include: <ul style="list-style-type: none">• be dated and have a unique invoice number;• quote a valid purchase order number and Contract reference number;• include correct Supplier details;• specify the services supplied;• be for the correct sum – in accordance to costs agreed with the Customer and not future dated;• provide contact details for queries.• Is in an un-editable format such as pdf or jpeg
Invoice frequency:	Invoices will be sent to the Buyer in arrears.
Contract value:	£103,657.88 + VAT
Contract charges:	£103,657.88.+ VAT

Additional buyer terms

Performance of the service and deliverables:	One off payment of enhancement charges <REDACTED> associated with DFE Microsoft Dynamics Business Central Licences
Guarantee:	Not Applicable
Warranties, representations:	Not Applicable
Supplemental requirements in addition to the Contract terms:	As described below in Schedule 1.
Alternative clauses:	As described in the attached Microsoft license T&Cs  Licence Agreement - Dynamics 365 Busine:
Buyer specific	As described below in Schedule 3

amendments to/refinements of the Contract terms:	
Public Services Network (PSN):	Not Applicable
Personal Data and Data Subjects:	Not Applicable

1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Contract terms and by signing below agree to be bound by this Contract.
- 1.3 This Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict the terms and conditions of the Contract and Order Form will supersede those of the Supplier Terms and Conditions.

Signed:	Supplier	Buyer
Name:	<REDACTED>	<REDACTED>
Title:	<REDACTED>	<REDACTED>
Signature:	<REDACTED>	<REDACTED>
Date:	22/10/2020	22/10/2020

Schedule 1 – Services

1. The Supplier shall facilitate the payment of Support and Maintenance (Enhancement) charges to be paid with effect From 14th September 2020, <REDACTED> on the following licences:

<REDACTED>

Schedule 2 - Contract charges

The applicable Contract Charges are as follows:

£103,657.88.

Schedule 3 – Additional Buyers Terms and Conditions

The following additional Terms and Conditions clauses shall apply. They will be included within the Order Form.

1. Departmental Security Standards

“BPSS” “Baseline Personnel Security Standard”	a level of security clearance described as pre-employment checks in the National Vetting Policy. Further information can be found at: https://www.gov.uk/government/publications/government-baseline-personnel-security-standard
“CCSC” “Certified Cyber Security Consultancy”	is NCSC's approach to assessing the services provided by consultancies and confirming that they meet NCSC's standards. This approach builds on the strength of CLAS and certifies the competence of suppliers to deliver a wide and complex range of cyber security consultancy services to both the public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-cyber-consultancy
“CCP” “Certified Professional”	is a NCSC scheme in consultation with government, industry and academia to address the growing need for specialists in the cyber security profession and are building a community of recognised professionals in both the UK public and private sectors. See website: https://www.ncsc.gov.uk/scheme/certified-professional
“CC” “Common Criteria”	the Common Criteria scheme provides assurance that a developer's claims about the security features of their product are valid and have been independently tested against recognised criteria.
“CPA” “Commercial Product Assurance” [formerly called “CESG Product Assurance”]	is an ‘information assurance scheme’ which evaluates commercial off the shelf (COTS) products and their developers against published security and development standards. These CPA certified products can be used by government, the wider public sector and industry. See website: https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

<p>“Cyber Essentials”</p> <p>“Cyber Essentials Plus”</p>	<p>Cyber Essentials is the government backed, industry supported scheme to help organisations protect themselves against common cyber-attacks. Cyber Essentials and Cyber Essentials Plus are levels within the scheme.</p> <p>There are a number of certification bodies that can be approached for further advice on the scheme; the link below points to one of these providers: https://www.iasme.co.uk/apply-for-self-assessment/</p>
<p>“Data”</p> <p>“Data Controller”</p> <p>“Data Processor”</p> <p>“Personal Data”</p> <p>“Sensitive Personal Data”</p> <p>“Data Subject”,</p> <p>“Process” and</p> <p>“Processing”</p>	<p>shall have the meanings given to those terms by the Data Protection Act 2018</p>
<p>"Department's Data"</p> <p>"Department's Information"</p>	<p>is any data or information owned or retained in order to meet departmental business objectives and tasks, including:</p> <p>(a) any data, text, drawings, diagrams, images or sounds (together with any repository or database made up of any of these components) which are embodied in any electronic, magnetic, optical or tangible media, and which are:</p> <p>(i) supplied to the Contractor by or on behalf of the Department; or</p> <p>(ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or</p> <p>(b) any Personal Data for which the Department is the Data Controller;</p>
<p>“DfE”</p> <p>“Department”</p>	<p>means the Department for Education</p>
<p>“Departmental Security Standards”</p>	<p>means the Department’s security policy or any standards, procedures, process or specification for security that the Contractor is required to deliver.</p>
<p>“Digital Marketplace / GCloud”</p>	<p>the Digital Marketplace is the online framework for identifying and procuring cloud technology and people for digital projects. Cloud services (e.g. web hosting or IT health checks) are on the G-Cloud framework.</p>
<p>“FIPS 140-2”</p>	<p>this is the Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), entitled ‘Security Requirements for Cryptographic Modules’. This document is the de facto security standard used for the accreditation of cryptographic modules.</p>

<p>“Good Industry Practice”</p> <p>“Industry Good Practice”</p>	means the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
<p>“Good Industry Standard”</p> <p>“Industry Good Standard”</p>	means the implementation of products and solutions, and the exercise of that degree of skill, care, prudence, efficiency, foresight and timeliness as would be expected from a leading company within the relevant industry or business sector.
<p>“GSC”</p> <p>“GSCP”</p>	means the Government Security Classification Policy which establishes the rules for classifying HMG information. The policy is available at: https://www.gov.uk/government/publications/government-security-classifications
<p>“HMG”</p>	means Her Majesty’s Government
<p>“ICT”</p>	means Information and Communications Technology (ICT) is used as an extended synonym for information technology (IT), used to describe the bringing together of enabling technologies used to deliver the end-to-end solution
<p>“ISO/IEC 27001”</p> <p>“ISO 27001”</p>	is the International Standard for Information Security Management Systems Requirements
<p>“ISO/IEC 27002”</p> <p>“ISO 27002”</p>	is the International Standard describing the Code of Practice for Information Security Controls.
<p>“ISO 22301”</p>	is the International Standard describing for Business Continuity
<p>“IT Security Health Check (ITSHC)”</p> <p>“IT Health Check (ITHC)”</p> <p>“Penetration Testing”</p>	means an assessment to identify risks and vulnerabilities in systems, applications and networks which may compromise the confidentiality, integrity or availability of information held on that IT system.
<p>“Need-to-Know”</p>	the Need-to-Know principle is employed within HMG to limit the distribution of classified information to those people with a clear ‘need to know’ in order to carry out their duties.
<p>“NCSC”</p>	The National Cyber Security Centre (NCSC) formerly CESG is the UK government’s National Technical Authority for Information Assurance. The NCSC website is https://www.ncsc.gov.uk

<p>“OFFICIAL”</p> <p>“OFFICIAL-SENSITIVE”</p>	<p>the term ‘OFFICIAL’ is used to describe the baseline level of ‘security classification’ described within the Government Security Classification Policy (GSCP) which details the level of protection to be afforded to information by HMG, for all routine public sector business, operations and services.</p> <p>the ‘OFFICIAL–SENSITIVE’ caveat is used to identify a limited subset of OFFICIAL information that could have more damaging consequences (for individuals, an organisation or government generally) if it were lost, stolen or published in the media, as described in the Government Security Classification Policy.</p>
<p>“Secure Sanitisation”</p>	<p>Secure sanitisation is the process of treating data held on storage media to reduce the likelihood of retrieval and reconstruction to an acceptable level. Some forms of sanitisation will allow you to re-use the media, while others are destructive in nature and render the media unusable. Secure sanitisation was previously covered by “Information Assurance Standard No. 5 - Secure Sanitisation” (“IS5”) issued by the former CESG. Guidance can now be found at: https://www.ncsc.gov.uk/guidance/secure-sanitisation-storage-media</p> <p>The disposal of physical documents and hardcopy materials advice can be found at: https://www.cpni.gov.uk/secure-destruction</p>
<p>“Security and Information Risk Advisor”</p> <p>“CCP SIRA”</p> <p>“SIRA”</p>	<p>the Security and Information Risk Advisor (SIRA) is a role defined under the NCSC Certified Professional (CCP) Scheme. See also: https://www.ncsc.gov.uk/articles/about-certified-professional-scheme</p>
<p>“SPF”</p> <p>“HMG Security Policy Framework”</p>	<p>This is the definitive HMG Security Policy which describes the expectations of the Cabinet Secretary and Government’s Official Committee on Security on how HMG organisations and third parties handling HMG information and other assets will apply protective security to ensure HMG can function effectively, efficiently and securely. https://www.gov.uk/government/publications/security-policy-framework</p>
<p>“Tailored Assurance”</p> <p>[formerly called “CTAS”, or, “CESG Tailored Assurance”]</p>	<p>is an ‘information assurance scheme’ which provides assurance for a wide range of HMG, MOD, Critical National Infrastructure (CNI) and public sector customers procuring IT systems, products and services, ranging from simple software components to national infrastructure networks. https://www.ncsc.gov.uk/documents/ctas-principles-and-methodology</p>

The Supplier shall comply with Buyer's Security Standards for Contractors which include but are not constrained to the following clauses.

- 1.1. Where the Supplier will provide ICT products or services or otherwise handle information at OFFICIAL on behalf of the Buyer, the requirements under Cabinet Office Procurement Policy Note – Use of Cyber Essentials Scheme certification - [Action Note 09/14](#) 25 May 2016, or any subsequent updated document, are mandated; that “contractors supplying products or services to HMG shall have achieved, and retain certification at the appropriate level, under the HMG Cyber Essentials Scheme”. The certification scope must be relevant to the services supplied to, or on behalf of, the Buyer.
- 1.2 The Supplier shall be able to demonstrate conformance to, and show evidence of such conformance to the ISO/IEC 27001 (Information Security Management Systems Requirements) standard, including the application of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).
- 1.3 The Supplier shall follow the UK Government Security Classification Policy (GSCP) in respect of any Buyer's Data being handled in the course of providing this service, and will handle this data in accordance with its security classification. (In the event where the Supplier has an existing Protective Marking Scheme then the Supplier may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Buyer's Data).
- 1.4 Buyer's Data being handled in the course of providing an ICT solution or service must be segregated from all other data on the Supplier's or sub-contractor's own IT equipment to protect the Buyer's Data and enable the data to be identified and securely deleted when required. In the event that it is not possible to segregate any Buyer's Data then the Supplier and any sub-contractor shall be required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 1.14.
- 1.5 The Supplier shall have in place and maintain physical security, in line with those outlined in ISO/IEC 27002 including, but not limited to, entry control mechanisms (e.g. door access) to premises and sensitive areas
- 1.6 The Supplier shall have in place and maintain an access control policy and process for the logical access (e.g. identification and authentication) to ICT systems to ensure only authorised personnel have access to Buyer's Data.
- 1.7 The Supplier shall have in place and shall maintain procedural, personnel, physical and technical safeguards to protect Buyer's Data, including but not limited to: physical security controls; good industry standard policies and process; anti-virus and firewalls; security updates and up-to-date patching regimes for anti-virus solutions; operating systems, network devices, and application software, user access controls and the creation and retention of audit logs of system use.
- 1.8 Any data in transit using either physical or electronic transfer methods across public space or cyberspace, including mail and couriers systems, or third party provider networks must be protected via encryption which has been certified to

FIPS 140-2 standard or a similar method approved by the Buyer prior to being used for the transfer of any Buyer's Data.

- 1.9 Storage of Buyer's Data on any portable devices or media shall be limited to the absolute minimum required to deliver the stated business requirement and shall be subject to Clause 1.11 and 1.12 below.
- 1.10 Any portable removable media (including but not constrained to pen drives, flash drives, memory sticks, CDs, DVDs, or other devices) which handle, store or process Buyer's Data to deliver and support the service, shall be under the control and configuration management of the Supplier or (sub-)contractors providing the service, shall be both necessary to deliver the service and shall be encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Buyer.
- 1.11 All portable ICT devices, including but not limited to laptops, tablets, smartphones or other devices, such as smart watches, which handle, store or process Buyer's Data to deliver and support the service, shall be under the control and configuration management of the Supplier or sub-contractors providing the service, and shall be necessary to deliver the service. These devices shall be full-disk encrypted using a product which has been certified to FIPS140-2 standard or another encryption standard that is acceptable to the Buyer.
- 1.12 Whilst in the Supplier's care all removable media and hardcopy paper documents containing Buyer Data must be handled securely and secured under lock and key when not in use and shall be securely destroyed when no longer required, using either a cross-cut shredder or a professional secure disposal organisation.
- 1.13 When necessary to hand carry removable media and/or hardcopy paper documents containing Buyer Data, the media or documents being carried shall be kept under cover and transported in such a way as to ensure that no unauthorised person has either visual or physical access to the material being carried. This clause shall apply equally regardless of whether the material is being carried inside or outside of company premises.
- 1.14 At the end of the contract or in the event of equipment failure or obsolescence, all Buyer information and data, in either hardcopy or electronic format, that is physically held or logically stored on the Supplier's ICT infrastructure must be securely sanitised or destroyed and accounted for in accordance with the current HMG policy using a NCSC approved product or method. Where sanitisation or destruction is not possible for legal, regulatory or technical reasons, such as a Storage Area Network (SAN) or shared backup tapes, then the Supplier or sub-contractor shall protect the Buyer's information and data until the time, which may be long after the end of the contract, when it can be securely cleansed or destroyed.
- 1.15 Access by Supplier or sub-contractor staff to Buyer's Data shall be confined to those individuals who have a "need-to-know" in order to carry out their role; and have undergone mandatory pre-employment screening, to a minimum of HMG Baseline Personnel Security Standard (BPSS); or hold an appropriate National Security Vetting clearance as required by the Department. All Supplier's or sub-contractor staff must complete this process before access to Buyer Data is permitted.
- 1.16 All Supplier or sub-contractor employees who handle Buyer Data must have annual awareness training in protecting information.

- 1.17 The Supplier shall, as a minimum, have in place robust Business Continuity arrangements and processes including IT disaster recovery plans and procedures that conform to ISO 22301 to ensure that the delivery of the contract is not adversely affected in the event of an incident. An incident shall be defined as any situation that might, or could lead to, a disruption, loss, emergency or crisis to the services delivered. If a ISO 22301 certificate is not available the Supplier will provide evidence of the effectiveness of their ISO 22301 conformant Business Continuity arrangements and processes including IT disaster recovery plans and procedures. This should include evidence that the Supplier has tested or exercised these plans within the last 12 months and produced a written report of the outcome, including required actions.
- 1.18 Any suspected or actual breach of the confidentiality, integrity or availability of Buyer Data being handled in the course of providing this service, or any non-compliance with these Buyer Security Standards for Suppliers, or other Security Standards pertaining to the solution, shall be investigated immediately and escalated to the Buyer by a method agreed by both parties.
- 1.19 The Supplier shall ensure that any IT systems and hosting environments that are used to handle, store or process Buyer Data shall be subject to independent IT Health Checks (ITHC) using a NCSC approved ITHC provider before go-live and periodically (at least annually) thereafter. The findings of the ITHC relevant to the service being provided are to be shared with the Buyer and all necessary remedial work carried out. In the event of significant security issues being identified, a follow up remediation test may be required.
- 1.20 The Supplier or sub-contractors providing the service will provide the Buyer with full details of any storage of Buyer Data outside of the UK or any future intention to host Buyer Data outside the UK or to perform any form of ICT management, support or development function from outside the UK. The Supplier or sub-contractor will not go ahead with any such proposal without the prior written agreement from the Buyer.
- 1.21 The Buyer reserves the right to audit the Supplier or sub-contractors providing the service within a mutually agreed timeframe but always within seven days of notice of a request to audit being given. The audit shall cover the overall scope of the service being supplied and the Supplier's, and any sub-contractors, compliance with the clauses contained in this Section.
- 1.22 The Supplier shall contractually enforce all these Buyer Security Standards for Suppliers onto any third-party suppliers, sub-contractors or partners who could potentially access Buyer Data in the course of providing this service.
- 1.23 The Supplier and sub-contractors shall undergo appropriate security assurance activities as determined by the Buyer. Supplier and sub-contractors shall support the provision of appropriate evidence of assurance and the production of the necessary security documentation such as completing the DfE Security Assurance Model (DSAM) process or the Business Service Assurance Model (BSAM). This will include obtaining any necessary professional security resources required to support the Supplier's and sub-contractor's security assurance activities such as: a NCSC Certified Cyber Security Consultancy (CCSC) or NCSC Certified Professional (CCP) Security and Information Risk Advisor (SIRA)

End of Security clauses

2. Issued Property

- 2.1 In this clause "Issued Property" means all items of property belonging to the Buyer issued to the Supplier for the purposes of the provision of the Services
- 2.2 Issued Property shall remain the property of the Buyer and shall be used in the execution of the Contract and for no other purpose whatsoever, save with the prior written approval of the Buyer. Within a reasonable period the Buyer shall re-issue Issued Property agreed to be defective or requiring replacement.
- 2.3 The Supplier shall be liable for any damage to Issued Property caused by misuse or negligence by the Supplier but shall not be liable for deterioration in Issued Property resulting from its normal and proper use in the performance of this Contract. The Supplier shall also be responsible for loss, including theft, of the Issued Property.
- 2.4 The Buyer will be responsible for the maintenance of the Issued Property. The Supplier shall be responsible for the safe custody of Issued Property and its prompt return upon expiry or termination of the Contract. Neither the Supplier nor its sub-contractors or other person shall have a lien on Issued Property for any sum due to the Supplier, sub-contractor or other person and the Supplier shall take all such steps as may be reasonably necessary to ensure that the title of the Buyer, and the exclusion of any such lien, are brought to the notice of all sub-contractors and other persons dealing with any Issued Property.

3. Use of Premises

- 3.1 Unless otherwise agreed, any land or premises made available to the Supplier by the Buyer in connection with the provision of the Services shall be made available to the Supplier free of charge and without exclusive possession and shall be used by the Supplier solely for the purpose of providing the Services. The Supplier shall have the use of such land or premises as licensee and shall vacate the same on the expiry or other termination of this Contract.
- 3.2 The Supplier shall ensure that in providing the Services its employees and sub-contractors co-operate as far as may be reasonably necessary with the Buyer's employees. The Supplier shall further ensure that its employees and sub-contractors carry out their duties and behave while on the Buyer's premises in such a way as to cause no unreasonable or unnecessary disruption to the routine and procedures of the Department, its employees, visitor or other contractors.
- 3.3 The Supplier shall ensure that its employees and sub-contractors comply with all rules and regulations from time to time issued by the Buyer relating to the use and/or security of the Buyer's premises.

