**G-CLOUD SERVICES CALL-OFF TERMS**

THE SECRETARY OF STATE FOR EDUCATION

- and -

EGRESS SOFTWARE TECHNOLOGIES LTD

relating to

the provision of G-Cloud Services.

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | [28/04/2015] | **Order Reference** | [ICT2015/012] |

**FROM:**

|  |  |
| --- | --- |
| Customer | The Secretary of State for Education “Customer” |
| Customer’s Address | Sanctuary Buildings, Great Smith Street, London, SW1P3BT |
| Invoice Address | **For Electronic invoices**  [Redacted](mailto:Redacted)  **For paper invoices**  Redacted |
| Principal Contact | Name: Redacted  Address:  Redacted |

**TO:**

|  |  |
| --- | --- |
| Supplier | Egress Software Technologies Ltd “Supplier”  (company number 6393598) |
| Supplier’s Address | Unit 16, Quadrant Business Centre, 135 Salusbury Road, London NW6 6RJ |
| Account Manager | Name: Redacted  Address: Redacted  Phone:Redacted  e-mail: Redacted  Fax: Redacted |

|  |  |
| --- | --- |
| **1. TERM** | |
| **1.1 Commencement Date**  This Call-Off Agreement commences on: [12/05/2015]  **1.2** **Expiry Date**  This Call-Off Agreement shall expire on:  1.2.1 the date which is 12 months after the commencement date in 1.1 [12/05/2016]  unless otherwise extended by the Customer by a period of up to twelve months in which case the Call Off Agreement shall expire on the last day of the extended period, or  1.2.2 the call off agreement has been terminated earlier pursuant to Clause CO-9 of the Call-Off Agreement.  1.2.3 Notice of the Customer’s intention to extend the contract beyond 12/05/2016 shall be given to the Supplier in writing no later than 12/04/2016.  1.2.4 The Egress Switch Service will be activated when both parties agree that the solution implementation stages are complete and signed off but no later than 01/06/2015 (subject to both the customer and the supplier successfully completing all implementation activities and tasks as agreed and documented within the implementation plan)  **1.3 Services Requirements**  1.3.1 This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services utilized by Customer may vary from time to time during the course of this Call-Off Agreement, subject always to the terms of the Call-Off Agreement.  1.3.2 G-Cloud Services | |
| 1.3.2.1 Lot1 IaaS | N/A |
| 1.3.2.2 Lot 2 PaaS | N/A |
| 1.3.2.3 Lot 3 SaaS | Services:  Egress Switch Email & File Encryption Services;**Service ID** 5.G4.0452.201 .  Egress Switch Secure Automated File Transfer: Service ID 5307931021017088   |  | | --- | | ***Egress Switch On Premise Gateway for Data and Keys - Annual Subscription****• On Premise security• Integration with document management• Enterprise Management/Policy Engine****Including Premium Support & Maintenance***  ***Product Code ESGOPC*** |  |  | | --- | | ***Egress Switch - Secure Email & Large File Transfer - Annual Subscription****• Compresses & Encrypts using AES 256 bit• Encryption at the Desktop, Web Client & via Mobile Devices• Email Encryption• CD/DVD Encryption• Large File Transfer (FTP/STFP/HOSTED CLOUD)• File Encryption on USB/Removable Media• Policy Enforcement (automated security Or user defined)• Real-time Auditing & Access Controls (restrict date/time, copy, print, save etc)• Enforce acceptance of policy disclaimer/data sharing agreement• Revoke recipient access to data when required*  *Product Code ESSEFT* |  |  | | --- | | **Egress Switch Secure Bulk File Transfer Usage Subscription - up to 500 transactions per month***On-premise service delivering automated bulk file transfer offering document classification, secure document viewing, and real-time audit and revocation.*  *Product Code ESSBFT* |  |  | | --- | | ***Egress Switch WEBFORM USAGE - Up to 500 transactions per month****•Submitting up to a maximum of 500 transactions / submissions per month through the Egress Web Form Service*  *Product Code ESSWFHC* | |  |   Service Type: Private Cloud Service  Support Type: Premium Support  Prices for elements of the service are also included in Service ID 5.G4.0452.202 (Egress Switch Secure Web form)  Services include on-premise solution implementation (design / build/ test / training/ deployment / go live)   |  | | --- | | **Egress Professional Services - 15 Days***On-site technical services including policy configuration, set up and deployment/implementation, product testing, and documentation.*  *Product Code EPS* |   (includes training)  Premium Support and maintenance Services  All resources will be provided on-shore within the UK and no near shore and or off shore resources will be used or have access to data  The Supplier will provide a list of all open and proprietary software and development tools used throughout this engagement and as far they are aware through their own due diligence, will confirm there is no infringement of copyright in the use of the proposed proprietary tools |
| 1.3.2.4 Lot 4 Specialist Cloud Services  1.3.2.5 G-Cloud Additional Services : **Additional Training (Optional)**  **Ad-Hoc Professional Services (Optional)**  **Secure Bulk File Transfer Usage and Webfrom Usage – option to scale usage (up or down)**  **Secure Email and Large File Transfer - option to scale usage (up or down)**  **Egress Switch**  **Upgrade to Fully Hosted Cloud Service (optional)** | N/A |

|  |
| --- |
| **2. PRINCIPAL LOCATIONS** |
| **2.1 Principal locations where the services are being performed**  Where possible activity will be performed remotely by the Supplier. On-site service provision will be delivered at the following main Department for Education locations:   * London * Nottingham * Coventry * Sheffield * Darlington * Manchester * Swindon (Eduserv Data Centre) * Slough (Eduserv Data Centre) |

|  |
| --- |
| **3. STANDARDS** |
| **3.1 Quality Standards**  The Supplier warrants that it will carry out the services with reasonable care and skill and that all services supplied hereunder shall be of satisfactory quality and fit for the particular purpose for which they are supplied with reference to the Customer's requirements and in line with G-Cloud V offerings; Supplier’s response to the Customers clarifications documentation.  **3.2 Technical Standards**  Solution will be required to be accredited to enable data transfers at official – official / sensitive level  3.3 Special Clauses - Please refer to Annex C |

|  |
| --- |
| **4. ONBOARDING** |
| **4.1 On-boarding**  4.2 The Customer and Supplier shall attend a start-up meeting with representatives of the Customer within seven working days of contract commencement (date time and venue to be notified by the Customer). At this meeting the agenda will include but not be limited to: discussion and agreement on activity to implement the SFTS solution within the DfE, future contract management arrangements; project documentation and deliverables; service delivery KPIs; requirements for reporting of Management Information consistent with clause 10 the framework agreement (if any); and a forward schedule of meeting dates.  4.3 As a minimum, the Supplier’s Account Manager for the DfE shall attend and fully participate in agreed contract and service review meetings chaired by the Customer. The agenda for this meeting will be issued to participants at least three (3) working days in advance of the meeting and include a monthly Service Report produced by the Supplier. |

|  |
| --- |
| **5. CUSTOMER RESPONSIBILITIES** |
| **5.1 Customer’s Responsibilities**  The Customer is responsible for reviewing resource activities and deliverables and accepting timesheets / invoices for work against agreed tasks and deliverables.  Customer will work with the Supplier in order that any required resources and documentation can be made available in order to support the achievement of activities and production of deliverables.  Customer responsibilities for the deployment of an On premise solution are listed within the Annex A and Annex B below  **5.2 Customer’s equipment**  There is no expectation that DfE equipment will be supplied as part of this service arrangment |

|  |
| --- |
| **6. PAYMENT** |
| **6.1 Payment profile and method of payment**  Charges payable by the Customer (including any applicable discount but excluding VAT), payment profile and method of payment (e.g. Government Procurement Card (GPC) or BACS  Payment Method: BACS  **Indicate preferred payment profile(s) by selecting from:**  6.1.1 Professional Services cost is invoiced on completion of phase 1 (subject to the milestones outlined in Section 12)  6.1.2 Product Cost invoiced annually in advance (including Support & Maintenance)  The Customer may regularly benchmark the charges and performance of the Goods and Services in terms of scope, specification, volume and quality of performance, against other Suppliers providing substantially the same as the Goods and Services ordered during the Contract Period in order to provide the Customer with information for comparison purposes.  The Customer shall be entitled to use any model to determine the achievement of value for money and to carry out the benchmarking evaluation referred to in paragraph above.  The Customer shall keep confidential the results of any benchmarking of Charges and provision of the Goods and Services.  The Supplier shall use all reasonable endeavours and act in good faith to supply information required by the Customer in order to undertake the benchmarking referred to in this paragraph, such information requirements to be at the discretion of the Customer.  The Customer may offer the Supplier an opportunity to revise Charges in comparison to the findings in the benchmarking evaluation exercise.  The supplier will notify the customer of any proposed price increases for their G-Cloud services.  Egress Switch Product Quotation – Redacted  Egress Professional Services Quotation –Redacted  **6.2 Invoice format**  The Supplier shall issue electronic invoices. Invoices will be issued   * On completion of each work phase (subject to milestones outlined in section 12) for Professsional Services * Annually in advance for the Product (including Support & Maintenance)   The Customer shall pay the Supplier within [thirty (30) calendar days] of receipt of a valid invoice, submitted in accordance with this paragraph 6.2 the payment profile set out in paragraph 6.1 above and the provisions of this Call-Off Agreement.A valid invoice will be;   * Delivered in timing in accordance of the contract * Is for the correct sum * Is correct in terms of services/goods supplied * Has a unique invoice number * Quotes a valid Purchase Order number * Includes correct Supplier details, date, contact details   Invoicing will be in United Kingdom Sterling and payment will be made by BACS transfer |

|  |
| --- |
| **7. DISPUTE RESOLUTION** |
| **7.1 Level of Representative to whom disputes should be escalated to:**  Level Finance director or equivalent  **Dispute resolution covered under CO-19 of this call of agreement**  **7.2 Mediation Provider**  Centre for Effective Dispute Resolution. |

|  |
| --- |
| **8. LIABILITY** |
| **Subject to the provisions of Clause CO 11 ‘Liability’ of the Call–Off Agreement:** |
| 8.1 The annual aggregate liability of either Party for all defaults resulting in direct loss of or damage to the property of the other Party ( technical infrastructure, assets, equipment or IPR but excluding any loss or damage to the Customer Data or Customer Personal Data) under or in connection with this Call–Off Agreement shall in no event exceed £1million.  8.2 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call–Off Agreement shall in no event exceed one hundred percent (100%) of the Charges payable by the Customer to the Supplier during the Call–Off Agreement Period.  8.3 Subject to paragraphs 8.1 and 8,2 above, the annual aggregate liability under this Call–Off Agreement of either Party for all defaults shall in no event exceed the greater of one hundred and twenty five per cent (125%) per cent of the Charges payable by the Customer to the Supplier during the Call–Off Agreement Period. |

|  |
| --- |
| **9. INSURANCE** |
| **9.1 Minimum Insurance Period**  Six (6) Years following the expiration or earlier termination of this Call-Off Agreement.  **9.2 To comply with its obligations under this Call-Off Agreement and as a minimum, where requested by the Customer in writing the Supplier shall ensure that:**   * **professional indemnity insurance** is held by the Supplier and by any agent, Sub-Contractor or consultant involved in the supply of the G-Cloud Services and that such professional indemnity insurance has a minimum limit of indemnity of one million pounds sterling (£1,000,000) for each individual claim or such higher limit as the Customer may reasonably require (and as required by Law) from time to time; * **employers' liability insurance** with a minimum limit of five million pounds sterling (£5,000,000) or such higher minimum limit as required by Law from time to time. |

|  |
| --- |
| **10. TERMINATION** |
| **10.1 Undisputed Sums Time Period**  At least ninety (90) Working Days of the date of the written notice specified in Clause CO 9.4 of the Call-Off Agreement**.**  **10.2 Termination Without Cause**  At least thirty (30) Working Days in accordance with Clause CO9.2 of the Call-Off Agreement.  No refunds shall be payable by the Supplier in respect of the 12 month period during which the termination without cause occurs. |

|  |
| --- |
| **11. AUDIT AND ACCESS** |
| Twelve (12) Months after the expiry of the Call-Off Agreement Period or following termination of this Call-Off Agreement. |

|  |
| --- |
| **12. PERFORMANCE OF THE SERVICES AND DELIVERABLES** |
| **12.1 Implementation Plan and Milestones (including dates for completion)** |
|  |
| **12.2 The Implementation Plan as at the Commencement Date is set out below:**  **SFTS: Main Activity**   |  |  |  |  | | --- | --- | --- | --- | | **Activity** | **Owner** | **Start** | **Finish** | | PHASE 1  Install SFTS Infrastructure | Eduserv | 30/03/15 | 24/04/15 | | Install SFTS Software and Services:   * Manual Data Transfer * Automated Data Transfer | Egress | 11/05/15 | 05/06/15 | | Develop Web Form | Egress | 04/05/15 | 22/05/15 | | Sign off SFTS software and Services Installations | DfE / Egress | 05/06/15 | 05/06/15 | | Sign off SFTS Web form Development | DfE / Egress | 22/05/15 | 22/05/15 | | PHASE 2  Test Manual Data Transfer Services and perform any redevelopment activity.   * Manual Data Transfer initiated via Egress Switch. * Manual Data Transfer performed via the web form solution. | DfE | 08/06/15 | 12/06/15 | | Accreditation of SFTS solution | DfE | 25/05/15 | 19/06/15 | | Sign-Off Manual Data Transfer solution | DfE | 12/06/15 | 12/06/15 | | Test Automated Data Transfer Services and perform any redevelopment activity | DfE | 08/06/15 | 22/06/15 | | Sign-Off Automated Data Transfer solution | DfE | 22/06/15 | 22/06/15 | | DfE Internal Go Live Approvals | DfE | 12/06/15 | 24/06/15 | | SFTS Solution Go Live: Manual Data Transfer | DfE | 25/06/15 | 25/06/15 | | SFTS Solution Go Live: Automated Data Transfer (Dates to be reviewed with Egress). | DfE | 25/06/15 | 25/06/15 | |
| 12.1.1 If so required by the Customer, the Supplier shall produce within one (1) Month of the Commencement Date a further version of the Implementation Plan (based on the above plan) in such further detail as the Customer may reasonably require. The Supplier shall ensure that each version of the Implementation Plan is subject to Customer’s written approval. The Supplier shall ensure that the Implementation Plan is maintained and updated on a regular basis as may be necessary to reflect the then current state of the implementation transition and/or transformation of the Services. |
| 12.1.2 The Customer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the Implementation Plan. |
| 12.1.3 The Supplier shall perform its obligations so as to achieve each milestone by the milestone date. |
| 12.1.4 Changes to the milestones shall only be made in accordance with the Change Control Procedure and provided that the Supplier shall not attempt to postpone any of the milestones using the Change Control Procedure or otherwise (except in the event of a Customer default which affects the Supplier's ability to achieve a milestone by the relevant milestone date).  **Supplier Services – Annex A**  **Switch Services, Service Types, Service Dependencies,**  **The following definitions apply to Annex A and Annex B:**  **“Client Side Software”** means the software components provided by Egress for installation on systems owned and/or operated by or on behalf of the Customer to access the Services;  **“Egress Switch Client”** means Client Side Software installed on desktop or laptop workstations;  **“Egress Switch Gateway”** means Client Side Software installed on Server workstations at the network boundary designed to encrypt and decrypt data;  **“Egress Switch Server”** means Client Side Software installed on Server workstations at the network boundary to manage Encryption Keys;  **“Egress Switch Web Reader”** means the facility to access the Switch Service via a web based client;  **“Encrypted Data”** means a package of encrypted data;  **“Fault”** means that the Switch Service is not performing in according with Annex A;  **“Fault Management”** means the management and resolution of Faults in the Service in accordance with the relevant Support Type for which the Subscription Charges have been paid by the Customer;  **“Maintenance Services”** means the maintenance activities set out in Annex B which shall be provided in accordance with the Support Type;  **“Order Confirmation”** means the order form to which these Call-Off Terms are attached;  **“Recipient”** means a person to whom Encrypted Data is sent;  **“Service Dependencies”** means the technical and information requirements for the use of each Service Type as set out in Annex A;  **“Services”** means the provision of the Switch Service, and the Fault Management and Maintenance Services by Egress to the Customer in accordance with the Service Type and Support Type for which the Subscription Charges are paid by the Customer, as are more particularly set out in Annex A and B of this Agreement;  **“Service Credits”** means the service credits which shall accrue to the Customer in respect of a failure by Egress to meet the Service Levels, as set out in Annex B;  **“Service Levels”** means the service levels set out in Annex B;  **“Service Type”** means each of the Fully Managed Service, the Hybrid Cloud Service and the Private Cloud On-Premise Installation as more particularly described in Annex A;  **“Subscription Charges”** means the charges payable by the Customers, as set out in the Order Confirmation;  **“Support Hours”** means 09:00 to 18:00 GMT/BST (as applicable) Monday to Friday, excluding UK bank and public holidays;  **“Support Type ”** means the applicable level of support (being Standard, Premium or 24/7 as more particularly described in Annex B) as selected in the Order Confirmation; in the absence of any such selection, the Support Type shall be Standard;  **“Switch Module”** meanseach of Switch Secure Email, Switch Secure File Transfer, Switch Secure Workspace and Switch Secure Web Form modules and any other future modules that may be offered by Egress for use by the Customer under this Agreement;  **“Switch Platform”** means Egress’ proprietary software platform which facilitates the encryption of data for transmission to a Recipient and the un-encryption by a Recipient as required to receive the functionality of the Switch Modules, as more particularly described in Annex A;  **“Switch Service”** means provision of the Switch Platform with the Switch Modules which Customer has elected to receive, as set out in an Order Confirmation;  **“Switch Service Infrastructure”** means the hardware and software infrastructure to which access is provided to the Customer by Egress in the provision of the Switch Services, and the requirement for such access is dependent on the Service Type.   1. **Switch Services**    1. The Switch Service is an email & file encryption service that enables users to encrypt, share, and remotely manage secure information that is distributed using a variety of transfer mechanisms including email, CD/DVD, USB Flash, USB Hard Drives, FTP Servers, HTTP Servers, and hosted Cloud Servers.   1.2 The Switch Service enables small or large organisations in the Public and Private sector to share information securely by enforcing policy centrally and integrating information security into existing workflow processes. Additionally, comprehensive real-time auditing ensures that information owners know precisely who, when, and where confidential data is being accessed. This new approach to secure information sharing enables users to maintain visibility and control wherever the data resides.   * 1. Core software components in the Switch Platform include:   1.3.1 Egress Switch Gateway  1.3.2 Egress Switch Server   * + 1. Egress Switch Client     2. Egress Switch Web Access Server   Depending on the Service Type, some or all of the above components may be Client Side Software.   1. **Service Types**   2.1 There are three Service Types. The Customer’s applicable Service Type shall be as stated in the Order Confirmation.   1. Fully Hosted Cloud Service: leverages the Switch Service Infrastructure for complete delivery of encryption services, key management, and user management. 2. Hybrid Hosted Cloud Service: leverages core elements of the Switch Service Infrastructure for key management and user management while installing Client Side Software to deliver encryption services. 3. Private Cloud Service: leverages Client Side Software for complete delivery of encryption services, key management, and user management.  |  |  |  | | --- | --- | --- | | **Fully Hosted Cloud Service** | **Hybrid Hosted Cloud Service** | **Private Cloud Service** | | Egress Switch Client | Egress Switch Client | Egress Switch Client | |  | Egress Switch Gateway | Egress Switch Gateway | |  |  | Egress Switch Server | |  |  | Egress Switch Web Access Server |  1. **Service Dependencies**    1. The following Service Dependencies are specific to the Hybrid Hosted Infrastructure and the On-Premise Hosted Infrastructure:       1. Microsoft Windows operating system (Windows 2008 R2 x64 for server components, Windows 7 x32 + Outlook 2010x32 for client components)       2. Microsoft .NET framework (version 3.5 SP1 with KB2600907 and KB969166 hotfixes applied)       3. Microsoft Internet Information Server version 7.5 (part of Windows 2008 R2 x64)    2. For all new configurations of the Egress Switch Services, Egress will produce a Service Design Document which will include details of the proposed solution, policy design and architectural overview.      * 1. In order for Egress to produce the Service Design Document and to provide the Services, Customer shall provide the following information:      1. Customer site access and contact details;      2. Encryption policy requirements;      3. System integration requirements (such as integration with AV, content scanning, archiving, etc.);      4. Details of operating systems and mobile platforms used within Customer’s organisation; and      5. Details of deployment software currently used within Customer’s organisation;   2. To enable the deployment by Egress of the required Client Side Software, Customer shall provide the following information:      1. Mail-flow Topology;      2. What email servers are currently in use in Customer’s organisation;      3. What Anti-virus software is used within Customer’s organisation;      4. What gateway scanning software is used within Customer’s organisation;      5. Whether email archiving and/or journaling used within Customer’s organisation; and      6. What file size limitation is applied to email messages (if any);   3. In addition, Customer shall comply with the following obligations:      1. providing the necessary hardware/virtual infrastructure, environmental conditions, and security measures at the Customer sites in accordance with the Services system requirements;      2. giving Egress (and any third party engaged by Egress in connection with the Services) reasonable access to equipment that is covered by, or required for, the Services at reasonable times during Working Hours and in accordance with Customer’s normal security procedures;      3. ensuring that all permissions of any kind needed for the installation and operation of Client Side Software are in place at all times and can be verified by Egress upon request;      4. any other obligations reasonably notified to Customer by Egress from time to time.   **Supplier Services – Annex B**  **Maintenance Services, Fault Management, Service Levels and Service Credits**  The following definitions shall apply to this Annex B.   |  |  | | --- | --- | | “24/7 Support” | is 24/7 Premium Support. | | “Customer Service Centre” | is the Egress dedicated service for managing Faults. The contact details for the Customer Service Centre vary from Service to Service and from Customer to Customer, Egress will provide each Customer with the Customer Service Centre contact details that are relevant to its Services. | | “Emergency Changes” | is any remote configuration change to an existing Egress Switch Service that must be actioned in a reduced time-scale or in a manner that prevents thorough assessment and/or adequate planning. | | "Excluded Events" | are any of the following:  (a) a Fault in, or any other problem associated with, non-Egress supplied software, hardware or other telecommunications systems not operated or provided by us;  (b) the fault, negligence, act or omission of the Customer or that of any third-party not within Egress’s direct control;  (c) the Customer not performing or a delay in performing any of the Customer Responsibilities;  (d) Customer requesting Egress to modify a Customer Site, or test one although no Fault has been detected or reported in accordance with the terms of the Agreement;  (e) service suspension or a force majeure event in accordance with the terms of the Agreement;  (f) an Outage or Fault resulting from the actions or omissions of the Customer or a third party on the Customer’s behalf; or  (g) any other circumstances caused by events for which Egress is not liable in accordance with the terms of the Agreement. | | "Outage" | is a temporary and unavoidable interruption in service, which is necessary for us to carry out essential maintenance or network upgrades. | | “Permitted Maintenance” | is planned maintenance agreed with the Customer and documented in the Maintenance Schedule. | | “Premium Support” | means the right to contact Egress directly during the Support Hours regarding Faults. | | “Standard Support” | means the right to log Faults using Trouble Tickets (and any other methods as may be notified by Egress to the Customer). | | “Trouble Ticket” | is a record of a Fault with a unique reference allocated to it which shall be used for all subsequent updates and communications. |  1. **Fault Management**    1. Egress shall carry out Fault management during the Support Hours to endeavour to restore operation of the Services to within agreed Service Levels and minimise the adverse impact of the Fault on Customer’s business operations.      * 1. Customers shall log all Faults with Egress using the reporting methods applicable to the Support Type paid for by the Customer.   2. Egress shall:      1. provide for separate identification of Faults (by raising a Trouble Ticket, at which point the Fault will be deemed to have commenced) and the tracking of Faults by the Customer Service Centre through to closure of the Trouble Ticket;      2. categorise Faults in accordance with the Severity Levels set out in Annex B;      3. maintain and update records of Faults; and      4. investigate, carry out diagnostic activities, and resolve any Faults where such activities are included as part of the Services and subject always to any exclusions or restrictions set out herein.   3. Customer shall:      1. appoint primary and secondary central points of contact within the Customer organisation who will be responsible for reporting Faults to and progressing Faults;      2. provide adequate information when the Fault is first reported to enable Egress to diagnose and resolve suspected Faults. This information will include:         1. Customer name;         2. the name, telephone number and email address of the person reporting the Fault;         3. Customer contact name, telephone number and email address if different from above;         4. the physical location of the Fault;         5. the number of sites affected by the Fault (if relevant);         6. identification of the service or component the Fault is being reported against, such as Egress Switch Client , Switch Gateway, Egress Switch Server, or similar identifiers; and         7. any other details that may be relevant to diagnosis of the Fault (including symptoms, events or actions leading up to the Fault, any tests carried out in attempting to isolate the problem, any environmental conditions that may be causing the Fault);      3. use all reasonable endeavours to ensure that the Fault has not arisen as a result of any matter that is not Egress’s responsibility under this Agreement before reporting a suspected Fault with the Services;      4. complete all initial troubleshooting activity previously specified by Egress before reporting a Fault; and      5. procure such co-operation from the end-users and from any third party providers as is reasonably requested by Egress to assist in the management of Faults.   4. If a Fault is reported to Egress which is not Egress’s responsibility then Egress shall have the right to charge the Customer for reasonable costs that it incurs in investigating the Fault.   5. If, after due investigations, Customer has reason to suspect that there is a Fault with the Egress Switch Service, it shall report the suspected Fault to Egress via the fault reporting process applicable to the Customer’s Support Type and provide the following information:      * + 1. Copy of Egress Switch Client de-bug logs;     2. Version of Egress Switch Client software;     3. Version of affected Operating System or mobile platform; and     4. Version of Anti-Virus software installed (if applicable);     5. In the event that the Client Side Software referred to below has been installed:        1. Confirmation that restarting the Switch Gateway Service has been attempted;        2. Version of Egress Switch Gateway software;        3. Copy of Egress Switch Gateway de-bug logs        4. Version of effected Operating System; and        5. Version of Ant-Virus software installed (if applicable);   1. Suspected Faults will be logged by Egress with a Trouble Ticket.   2. Egress will initially work to resolve all Faults remotely in accordance with the Support Type. Where an engineer is required to visit the Customer Site, the target resolution time will depend on the availability of access to the Customer Site and Egress will provide Customer with regular updates regarding resolution timescales.   3. If, after investigation, Egress considers that the Fault has not been resolved or a that a solution does not seem imminent, Egress may arrange for an engineer to visit the impacted Customer Site or upgrade the software used in the Services, save in the event that the Fault is a result of a direct result of a failure at a Customer Site or from any hardware in respect of which Egress has no management or maintenance responsibility.   4. Customer agrees to reimburse Egress for its reasonable expenses if Customer reports a suspected Fault which leads to a Customer Site visit and the fault is determined by Egress as unrelated to the Egress Switch Service.   5. The Fault will be deemed to be resolved when Egress notifies the Customer of such resolution or attempt, unsuccessfully, to contact Customer for that purpose.   6. Whenever possible, Customer should give Egress a minimum of fourteen (14) calendar days’ notice of any event of which it is aware which may disrupt the Egress Switch Service.   **2. CHANGES**   * 1. Egress reserves the right to make any organisational, procedural, or target adjustments to the Fault reporting, management processes, and the Switch Service Infrastructure provided that such adjustments do not have a materially detrimental effect on the provision of the Switch Service to Customer.   2. In the event that an Emergency Change is required to address any security risks, such change shall take priority and Egress will use reasonable endeavours to process this within two hours of receiving notification and sufficient information from Customer of the Emergency Change provided that Customer acknowledges that the reduced timescales for Emergency Changes may prevent thorough assessment and/or adequate planning and Egress cannot therefore be liable for any losses or expenses incurred by Customer or any impact on the Egress Switch Service as a result of our provision of the Emergency Change.   **3. MAINTENANCE SCHEDULE**  3.1 Egress will create and maintain a rolling maintenance schedule with regard to the Egress Switch Service to be agreed with the Customer. The maintenance schedule shall be discussed in advance and updated accordingly.   * 1. When Egress wishes to carry out any maintenance to the Egress Switch Service (other than Emergency Changes), it shall ensure that;      1. the timing of the planned maintenance is in accordance with the requirements of the maintenance schedule or is an otherwise agreed in writing with the Customer at least 10 working days in advance;      2. once agreed with the Customer the planned maintenance (which shall be known as ‘Permitted Maintenance’) is entered into the maintenance schedule;   2. Egress shall book a maximum of 24 hours Outage for Permitted Maintenance in any one calendar month which shall take place between the hours and on the day specified in the maintenance schedule unless otherwise agreed in writing with the Customer. For avoidance of doubt, Permitted Maintenance shall not exceed 24 hours per calendar month;   3.4 Outages arising due to Permitted Maintenance that is carried out by Egress in accordance with 3.4 will be subtracted from the total number of hours in the relevant service period when calculating Service Availability.   1. **OUTAGES**    1. Outages to the Egress Switch Services and/or equipment may be necessary from time to time. Egress will:       1. use reasonable endeavours to give Customer as much notice as reasonably possible of any Outage, which will affect the availability of the Egress Switch Service;       2. use reasonable endeavours to minimise the number of Outages and any subsequent disruption to Customer; and       3. not be liable for any charges or costs incurred as a result of an Outage caused by Customer or Customer end users.    2. Customer shall notify its end users, Recipients, Customers or third party providers of any Outage. 2. **SEVERITY LEVELS**   Severity Levels for Faults are defined as follows:   |  |  | | --- | --- | | Severity Level | Severity Level definition | | Category 1 Faults | Means those Faults in the Egress Switch Service that cause the system to fail and seriously impact or prevent the use of the Egress Switch Service. Egress will use reasonable endeavours to investigate and resolve the Fault concerned within 4 hours of notification. | | Category 2 Faults | Means those Faults that allow the Service to be used albeit in a limited or undesirable capacity and that must be corrected within a reasonable time. Egress will use reasonable endeavours to investigate and resolve the Fault concerned within 24 hours of notification. | | Category 3 Faults | Means those Faults that are cosmetic and minor by nature and will not prevent the successful operation of the Egress Switch Service. Egress will attempt to fix such issue in the next update of the Service. |      1. **SERVICE LEVELS & MEASUREMENT**     1. The availability of the Egress Switch Service will be measured as the percentage of time the Egress Switch Service is available in a calendar month.    2. Service availability for each Customer Site will be calculated as follows:   P = A – B x 100%  A  Where:  P = percentage availability  A = number of hours in the relevant calendar month  B = number of hours in the relevant calendar month during which the Egress Switch Service is not available, excluding time where the Egress Switch Service is not available due to:   * + - * 1. Permitted Maintenance         2. Outages;         3. agreed changes of the Egress Switch Service;         4. unavailability of access to Customer sites for engineering staff;         5. an Excluded Event; and         6. Emergency Changes;   1. The target availability of the Egress Switch Service is 99% (“**Target Availability**”).  1. **SERVICE CREDITS**    1. Any Service Credits which accrue hereunder will be applied to Customer’s next Subscription Charges invoice. No other Services Credit shall be payable.    2. Where the availability of the Egress Switch Service does not meet the Target Availability set out in paragraph 6.3 above, Customer shall be entitled to a following Service Credits, provided that at least 10% of the users at a Customer Site are affected by the unavailability:  |  |  | | --- | --- | | **Service Availability in a given month** | **Service Credit (percentage of Subscription Charge paid for the affected Customer site for the relevant month (annual charges shall be pro-rated to calculated monthly charges)** | | Equal to or > than 99% | 0% | | 95% - 98.99% | 10% | | 93% - 94.99 | 15% | | 90% - 92.99% | 20% | | 80% - 89.99% | 25% | | 70% - 79.99% | 30% | | 60% - 69.99% | 35% | | 50% - 59.99% | 40% |  * 1. Service Credits will only be payable if:      1. In respect of the annual measurement period or monthly measurement period stated if the actual Service availability falls below the applicable Target Availability for that period; and   *Either*   * + 1. Egress notifies Customer that a Service Credit is payable; *or*     2. Customer notifies Egress in writing that Customer believes a Service Credit is payable within 30 calendar days of the date of the relevant Service failure which Customer believe gives rise to a Service Credit. Egress will investigate the claim for a Service Credit and confirm whether the Service Credit is payable.   1. The maximum Service Credits that can accrue in any Subscription Period is 40% of the Subscription Charges paid by the Customer for that Subscription Period. Service Credits shall be applied to the next Subscription Charges invoice in full and final settlement of all Egress liability arising as a result of the Service failure in respect of which the Service Credits are payable. |

|  |
| --- |
| **13. COLLABORATION AGREEMENT** |
| In accordance with Clause CO-21 of this Contract, the Customer does not require the Supplier to enter into a Collaboration Agreement. |

Annex C

Department for Education Special Clauses

**1. Intellectual Property Rights and Copyright**

"Intellectual Property means patents, trade marks, service marks, design rights

Rights” (whether registerable or otherwise), applications for any of the foregoing, know-how, rights protecting databases, trade or business names and other similar rights or obligations whether registerable or not in any country (including but not limited to the United Kingdom).

"the Act" means the Copyright Designs and Patents Act 1988;

"Copyright" means any and all copyright, design right (as defined by the Act) and all other rights of a like nature which may, during the course of this Contract, come into existence in or in relation to any Work (or any part thereof);

"Crown and/or Her both mean Queen Elizabeth II and any successor to

Majesty" Her Majesty;

"HMSO" means Her Majesty's Stationery Office;

"Her Majesty's means the duly elected Government for the time being

Government" during the reign of Her Majesty and/or any department, committee, office, servant or officer of such Government;

"Work" means any and all Works including but not limited to literary, dramatic, musical or artistic works, sound recordings, films, broadcasts or cable programmes, typographical arrangements and designs (as the same are defined in the Act) which are created from time to time during the course of this Contract by the Contractor or by or together with others at the Contractor's request or on its behalf and where such works directly relate to or are created in respect of the performance of this Contract or any part of it.

1 Intellectual Property Rights and Copyright

1.1 Save as granted under this Contract, neither the CUSTOMER nor the SERVICE PROVIDER shall acquire any right, title or interest in the other’s Pre-Existing Intellectual Property Rights. The SERVICE PROVIDER acknowledges that the CUSTOMER Data is the property of the CUSTOMER and the CUSTOMER hereby reserves all Intellectual Property Rights which may subsist in the CUSTOMER Data.

1.2 **Not used**

**COPYRIGHT WARRANTIES**

1.3 The Contractor now warrants to the Crown, HMSO and the Department (and to any assignees and licensees of each) that all Works will not infringe in whole or in part any copyright or like right or any other intellectual property right of any other person (wheresoever) and agrees to indemnify and hold harmless Her Majesty and/or Her Majesty's Government against any and all claims, demands, proceedings, expenses and losses, including any of a consequential nature, arising directly or indirectly out of any act of the foregoing in relation to any Work, where such act is or is alleged to be an infringement of a third party's copyright or like right or other intellectual property right (wheresoever).

1.4 The warranty and indemnity contained in Clause 1.3 above shall survive the termination of this Contract and shall exist for the life of the Copyright.

2.0 Ownership of Drawings Specifications and Other Data

2.1 Any relevant drawings, specifications or other data specific to the departments requirements that are completed or provided in connection with this Contract shall become or, as the case may be, remain the property of the Department and be delivered up to the Department on request with a reasonable period of notice or on completion or termination of the Contract.

**3. Not used**

**4. Contractors Standards**

The Contractor shall as far as practicable satisfy the Department that it operates to an acceptable standard such as BS 5750, BS EN ISO 9000 or an equivalent.

**5. Not Used**

**6. Contractors Employees and Sub-Contractors**

6.1 The Contractor shall give to the Department if so requested a list of all persons who are or may be at any time directly concerned with the performance of this Contract specifying the capacity in which they are concerned with the provision of the Services' and giving such other particulars as the Department may reasonably require.

6.2 If the Department notifies the Contractor that it considers that an employee or sub-contractor is not appropriately qualified or trained to provide the Services or otherwise is not providing the Services in accordance with this Contract, then the Contractor shall, as soon as is reasonably practicable, take all such steps as the Department considers necessary to remedy the situation or, if so required by the Department, shall remove the said employee or sub-contractor from providing the Services and shall provide a suitable replacement (at no cost to the Department).

6.3 The Contractor shall take all reasonable steps to avoid changes of employees or sub-contractors assigned to and accepted to provide the Services under the Contract except whenever changes are unavoidable or of a temporary nature. The Contractor shall give at least one month's written notice to the Contract Manager of proposals to change key employees or sub-contractors*.*

6.4 The contractor shall use all reasonable endeavours to ensure that all its employees and sub contractors who are not  EC Nationals are legally entitled to be resident in the UK and have a work permit, where applicable.'

7. Not used

8. Not used

9. Not used

10. Not used

11.  Data Protection Act

|  |  |
| --- | --- |
| **"Affiliate"** | in relation to a body corporate, any other entity which directly or indirectly Controls, is Controlled by, or is under direct or indirect common Control with, that body corporate from time to time; |
| **"Contractor Personnel"** | all employees, agents, Contractors and contractors of the Contractor and/or of any Sub-contractor; |
| **"Control"** | means that a person possesses, directly or indirectly, the power to direct or cause the direction of the management and policies of the other person (whether through the ownership of voting shares, by contract or otherwise) and **"Controls"** and **"Controlled"** shall be interpreted accordingly; |
| **“Regulatory Bodies”** | those government departments and regulatory, statutory and other entities, committees and bodies which, whether under statute, rules, regulations, codes of practice or otherwise, are entitled to regulate, investigate, or influence the matters dealt with in this Contract or any other affairs of the Department and **"Regulatory Body"** shall be construed accordingly. |
| **"Sub-contractor"** | the third party with whom the Contractor enters into a Sub-contract or its servants or agents and any third party with whom that third party enters into a Sub-contract or its servants or agents; |
| **"Working Day"** | any day other than a Saturday, Sunday or public holiday in England and Wales. |

11.1 With respect to the parties' rights and obligations under this Contract, the parties agree that the Department is the Data Controller and that the Contractor is the Data Processor. For the purposes of this Clause 11, the terms “Data Controller”, “Data Processor”, “Data Subject”, “Personal Data”, “Process” and “Processing shall have the meaning prescribed under the DPA.

11.2 The Contractor shall:

11.2.1 Process the Personal Data only in accordance with instructions from the Department (which may be specific instructions or instructions of a general nature as set out in this Contract or as otherwise notified by the Department to the Contractor during the period of the Contract);

11.2.2 Process the Personal Data only to the extent, and in such manner, as is necessary for the provision of the Services or as is required by law or any Regulatory Body;

11.2.3 Implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to the Personal Data and having regard to the nature of the Personal Data which is to be protected;

11.2.4 Take reasonable steps to ensure the reliability of any Contractor Personnel who have access to the Personal Data;

11.2.5 Obtain prior written consent from the Department in order to transfer the Personal Data to any Sub-contractors or Affiliates for the provision of the Services;

11.2.6 Ensure that all Contractor Personnel required to access the Personal Data are informed of the confidential nature of the Personal Data and comply with the obligations set out in this Clause11;

11.2.7 Ensure that none of Contractor Personnel publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Department;

11.2.8 Notify the Department within five Working Days if it receives:

11.2.8.1 a request from a Data Subject to have access to that person's Personal Data; or

11.2.8.2 a complaint or request relating to the Department's obligations under the Data Protection Legislation;

11.2.9 Provide the Department with full cooperation and assistance in relation to any complaint or request made, including by:

11.2.9.1 providing the Department with full details of the complaint or request;

11.2.9.2 complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Department's instructions;

11.2.9.3 providing the Department with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Department); and

11.2.9.4 providing the Department with any information requested by the Department;

11.2.10 Permit the Department or the Department’s Representative (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Contractor's data processing activities (and/or those of its agents, subsidiaries and Sub-contractors) and comply with all reasonable requests or directions by the Department to enable the Department to verify and/or procure that the Contractor is in full compliance with its obligations under this Contract;

11.2.11 Provide a written description of the technical and organisational methods employed by the Contractor for processing Personal Data (within the timescales required by the Department); and

11.2.12 Not Process or otherwise transfer any Personal Data outside the European

Economic Area. If, after the Commencement Date, the Contractor (or any

Sub-contractor) wishes to Process and/or transfer any Personal Data

outside the European Economic Area, the following provisions shall apply:

11.2.12.1 the Contractor shall submit a request for change to the Department which shall be dealt with in accordance with any Change Control Procedure

11.2.12.2 the Contractor shall set out in its request for change details of the following:

(a) the Personal Data which will be Processed and/or transferred outside the European Economic Area;

(b) the country or countries in which the Personal Data will be Processed and/or to which the Personal Data will be transferred outside the European Economic Area;

(c) any Sub-contractors or other third parties who will be Processing and/or transferring Personal Data outside the European Economic Area; and

(d) how the Contractor will ensure an adequate level of protection and adequate safeguards (in accordance with the Data Protection Legislation and in particular so as to ensure the Department’s compliance with the Data Protection Legislation) in respect of the Personal Data that will be Processed and/or transferred outside the European Economic Area;

11.2.12.3 in providing and evaluating the request for change, the parties shall ensure that they have regard to and comply with then-current Department, Government and Information Commissioner Office policies, procedures, guidance and codes of practice on, and any approvals processes in connection with, the Processing and/or transfers of Personal Data outside the European Economic Area and/or overseas generally; and

11.2.12.4 the Contractor shall comply with such other instructions and shall carry out such other actions as the Department may notify in writing, including:

(a) incorporating standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) in this Contract or a separate data processing agreement between the parties; and

(b) procuring that any Sub-contractor or other third party who will be Processing and/or transferring the Personal Data outside the European Economic Area enters into a direct data processing agreement with the Authority on such terms as may be required by the Department, which the Contractor acknowledges may include the incorporation of standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation).”

11.3 The Contractor shall comply at all times with the Data Protection Legislation and shall not perform its obligations under this Contract in such a way as to cause the Department to breach any of its applicable obligations under the Data Protection Legislation.

12. Not used

13. Not used

14. Not used

15. Not used

16 Not used

17. Not used

**18. Contractors co-operation with Departmental objectives**

In performing the Contract, the Contractor shall at all times co-operate with the Department to maximise value for money, sustainable delivery where it is not detrimental to the interests of either Party to do so.

* + - 1. **19. Sustainable Considerations**

The Contractor shall in all his operations, including purchase of materials goods and services, adopt a sound proactive sustainable approach, designed to minimise harm to the environment, society and economy and be able to provide proof of doing so to the Contract Manager on demand.

**20. Contractors use of sustainability impact assessment tools**

Contractors shall undertake a sustainability impact assessment and use outputs of this and other good practice examples to deliver the *services* in a manner that optimises the environmental, social and economic impact of this contract including but not limited to *energy usage, transportation, bio-diversity, water usage, pollution, re-cycling*, in order to maximise value for money, sustainable delivery.

**21 Not used**

**22 Personnel Security Standard**

“Departmental Assets” Includes but not limited to Departmental premises, IT systems and information with a classification up to confidential.

“Personnel Security Standard” A government wide requirement including checks on identity, employment history, nationality and immigration status and the declaration of unspent criminal records.

22.1 The Contractor shall ensure that any personnel provided under this Contract including those of any sub-contractors, who have unsupervised access to Departmental Assets meet the Personnel Security Standards and shall provide evidence that the checks have been performed on request.

22.2 A breach of this Clause [22] shall entitle the Department to terminate the contract immediately.

**23 Not used**

**24 Staffing Security**

|  |  |
| --- | --- |
| **"Contractor Personnel"** | all employees, agents, consultants and contractors of the Contractor and/or of any Sub-contractor; |
|  |  |
| **"Staff Vetting Procedures"** | the Department's procedures and departmental policies for the vetting of personnel whose role will involve the handling of information of a sensitive or confidential nature or the handling of information which is subject to any relevant security measures, including, but not limited to, the provisions of the Official Secrets Act 1911 to 1989; |

24.1 The Contractor shall comply with the Staff Vetting Procedures in respect of all Contractor Personnel employed or engaged in the provision of the Services. The Contractor confirms that all Contractor Personnel employed or engaged by the Contractor to work on this Contract were vetted and recruited on a basis that is equivalent to and no less strict than the Staff Vetting Procedures.

**25 Security Requirements**

|  |  |
| --- | --- |
| **"Contractor Personnel"** | all employees, agents, consultants and contractors of the Contractor and/or of any Sub-contractor; |
| **"ICT"** | information and communications technology; |
| **"ICT Environment"** | the Department’s system and the Contractor system; |
| **"Malicious Software"** | any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence; |
| **"Security Plan"** | the security plan agreed between the Department and Contractor and included as a schedule (Security Requirements) to the contract; |
|  |  |

25.1 The Contractor shall comply, and shall procure the compliance of the Contractor Personnel, with the Security Plan.

25.2 The Department shall notify the Contractor of any changes or proposed changes to the Security Plan.

25.3 If the Contractor believes that a change or proposed change to the Security Plan will have a material and unavoidable cost implication to the Services it may submit a business case for any additional costs. In doing so, the Contractor 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.

25.4 Until and/or unless a change to the charges is agreed by the Department pursuant to clause 25.3 the Contractor shall continue to perform the Services in accordance with its existing obligations.

**Malicious Software**

25.5 The Contractor shall, as an enduring obligation throughout the period of the Contract, use the latest versions of anti-virus definitions available to check for and delete Malicious Software from the ICT Environment.

25.6 Notwithstanding clause 25.5, if Malicious Software is found, the parties shall co-operate to reduce the effect of the Malicious Software and, particularly if Malicious Software causes loss of operational efficiency or loss or corruption of Department’s Data, assist each other to mitigate any losses and to restore the Services to their desired operating efficiency.

25.7 Any cost arising out of the actions of the parties taken in compliance with the provisions of clause 25.6 shall be borne by the parties as follows:

25.7.1 by the Contractor where the Malicious Software originates from the Contractor Software, the Third Party Software or the Department’s Data (whilst the Department’s Data was under the control of the Contractor); and

25.7.2 by the Department if the Malicious Software originates from the Department’s Software or the Department’s Data (whilst the Department’s Data was under the control of the Department).

26 Not used

27 Not used

28 Not used

29 Not used

30 Not used

31 Tax Compliance

Definitions and Interpretations

“Occasion of Tax Non-Compliance” means:

(a) any tax return of the Supplier submitted to a Relevant Tax Authority on or after 1 October 2012 is found on or after 1 April 2013 to be incorrect as a result of:

(i) a Relevant Tax Authority successfully challenging the Supplier under the General Anti-Abuse Rule or the Halifax Abuse Principle or under any tax rules or legislation that have an effect equivalent or similar to the General Anti-Abuse Rule or the Halifax Abuse Principle;

(ii) the failure of an avoidance scheme which the Supplier was involved in, and which was, or should have been, notified to a Relevant Tax Authority under the DOTAS or any equivalent or similar regime; and/or

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

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

“General Anti-Abuse Rule” means (a) the legislation in Part 5 of the Finance Act 2013; and

(b) any future legislation introduced into parliament to counteract tax advantages arising from abusive arrangements to avoid national insurance contributions.

“Halifax Abuse Principle” means the principle explained in the CJEU Case C-255/02 Halifax and others.

“Relevant Tax Authority” means: HM Revenue & Customs, or, if applicable, a tax authority in the jurisdiction in which the Supplier is established.

**32 Tax Compliance**

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

32.2 If at any point during the Term, an Occasion of Tax Non-Compliance occurs, the Contractor shall:

a) notify the Department in writing of such fact within 5 Working Days of its occurrence; and

b) promptly provide to the Department with:

i) details of the steps which the Contractor is taking to address the Occasion of Tax Non-Compliance and to prevent the same from recurring, together with any mitigating factors that it considers relevant; and

ii) such other information in relation to the Occasion of Tax Non-Compliance as the Department may reasonably require.

32.3 In the event that:

(a) the warranty given by the Contractor pursuant to Clause 32.1 is materially untrue; or

(b) the Contractor commits a material breach of its obligation to notify the Department of any Occasion of Tax Non-Compliance as required by Clause 32.2; or

(c) the Contractor fails to provide details of proposed mitigating factors which in the reasonable opinion of the Department, are acceptable

the Department shall be entitled to terminate this Contract with immediate effect by notice in writing.

**Departmental Security Standards for ICT Contracts**

|  |  |
| --- | --- |
| “CESG” | is the UK government’s National Technical Authority for Information Assurance. The website is http://www.cesg.gov.uk/Pages/homepage.aspx |
| “Data”, “Data Controller”, “Data Processor”, “Personal Data”, “Sensitive Personal Data”, “Data Subject”, “Process” and “Processing” | shall have the meanings given to those terms by the Data Protection Act 1998 |
| "Department’s Data" | (a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media, and which are:  (i) supplied to the Contractor by or on behalf of the Department; or  (ii) which the Contractor is required to generate, process, store or transmit pursuant to this Contract; or  (b) any Personal Data for which the Department is the Data Controller; |
| “Departmental Security Standards” | means the Department’s specification for security that the Contractor is required to deliver. |
| “Good Industry Practice” | 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. |
| “Good Industry Standard” | 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. |
| “IT Security Health Check” | means an assessment to identify vulnerabilities in IT systems and networks which may compromise the confidentiality, integrity or availability of information held on that IT system. |

1. The Contractor will assure the Department that they can comply with its Departmental Security Standards for Contractors which include but are not constrained to the following paragraphs:
2. Where the Contractor will process personal data on behalf of the Department or other data deemed sensitive by the Department or supply ICT products or services to, or on behalf of, the Department, the Contractor will be expected to have achieved, and be able to maintain, certification to the appropriate level, under the HMG Cyber Essentials Scheme. The certification must have a scope relevant to the services supplied to, or on behalf of, the Department. Alternatively, the Contractor must demonstrate, to the satisfaction of the Department, compliance with the requirements of the Cyber Essentials Scheme.

For the duration of this Agreement, Egress shall maintain security accreditation for the Switch Service software from one or more independent certification/accreditation organisations and shall provide evidence of such certification/accreditation to the Customer at the Customer’s request. This condition applies to the standard referenced above (section 2), and also Sections 3, 4, 7, 9,10,14

1. The Contractor will be expected to have achieved, and be able to maintain, independent certification to ISO/IEC 27001 (Information Security Requirements Specification). The ISO/IEC 27001 certification must have a scope relevant to the services supplied to, or on behalf of, the Department and the statement of applicability must be acceptable to the Department, including the application of an appropriate selection of controls from ISO/IEC 27002 (Code of Practice for Information Security Controls).
2. The Contractor will adopt the UK Government Security Classification Policy in respect of any Departmental Data being handled in the course of providing this service, and will handle this data in accordance with its security classification and Impact Level. (In the event where the Contractor has an existing Protective Marking Scheme then the Contractor may continue to use this but must map the HMG security classifications against it to ensure the correct controls are applied to the Departmental Data).
3. The Contractor will have in place and maintain physical (e.g. door access) and logical (e.g. identification and authentication) access controls to ensure only authorised access to Departmental Data.
4. The Contractor will have in place and maintain technical safeguards to protect Departmental Data, including but not limited to: Good Industry Standard anti-virus and firewalls; up-to-date patches for operating system, network device, and application software.
5. Any electronic transfer methods across public space or cyberspace must be protected via encryption which has been certified to FIPS140-2 or certified under a CESG (e.g. CAPS or CPA) or CESG-endorsed scheme, and the method shall be approved by the Department prior to being used for the transfer of any Departmental Data.
6. Paper documents containing Departmental Data shall be transmitted, both within and outside company premises in such a way as to make sure that no unauthorised person has access.
7. Any portable removable media (including but not constrained to pen drives, memory sticks, CDs, DVDs, PDPs, USB devices) which handle, store or process in any way Departmental Data to deliver and support the service, shall be under the configuration management of the (sub-)contractors providing the service, shall be necessary to deliver the service, and shall be full-disk encrypted using a product which has been certified to FIPS140-2 or certified under a CESG (e.g. CAPS or CPA) or CESG-endorsed scheme or uses another encryption standard that is acceptable to the Department.
8. All portable ICT devices (including but not limited to laptops, PDAs, smartphones) which handle, store or process in any way Departmental Data to deliver and support the service, shall be under the configuration management of the (sub-)contractors providing the service and shall be full-disk encrypted using a product which has been certified to FIPS140-2 or been certified under a CESG (e.g. CAPS or CPA) or CESG-endorsed scheme or uses another encryption standard that is acceptable to the Department.
9. Storage of Departmental Data on any portable devices or media shall be limited to the minimum required to deliver the business requirement.
10. Access by Contractor staff to Departmental Data shall be confined to those individuals who have a “need-to-know” and whose access is essential for the purpose of their duties. All employees with direct or indirect access to Departmental Data must be subject to pre-employment checks equivalent to or higher than the Baseline Personnel Security Standard (BPSS): Details of the standard are available at the HMG website <https://www.gov.uk/government/publications/security-policy-framework>
11. All Contractor employees who handle Departmental Data must have annual awareness training in protecting information.
12. The Contractor will deliver services that are compliant with HMG Security Policy Framework in conjunction with CESG Information Assurance Policy Portfolio. The Contractor will provide the DfE with evidence of compliance for the services to be delivered, including, but not limited to:

* Risk Management Accreditation Document Set (RMADS)
* Full Risk Assessments for the Services, including Residual Risk Statements
* Security Operating Procedures (SyOPs) for all user types
* Forensic Readiness Policy

1. The Contractor will provide details of:

* Any existing HMG accreditations including the body awarding accreditation; the scope of the accreditation; any caveats; date awarded and duration; residual risk statement. Evidence of accreditation will be required.
* Progress in achieving HMG accreditation including whether documentation has been produced and submitted. If HMG accreditation is in progress, the Contractor will state who the awarding organisation will be and date expected.

1. If no current HMG accreditation is held the Contractor will undergo appropriate assurance as determined by the Department which may involve HMG accreditation by DfE Accreditor. In this case the Contractor will support the production of the necessary documentation (e.g. RMADS). This will include obtaining the necessary professional security expertise, for example CESG Listed Advisor Scheme (CLAS) as described in <http://www.cesg.gov.uk/servicecatalogue/CLAS/Pages/CLAS.aspx>
2. The Contractor will provide details of the most recent IT Health Check conducted and submit the report to the Department. If no IT Health Check has been carried out in the last year, or, if it has not been performed by a CHECK provider then the Contractor will be required to arrange for a CHECK IT Health Check; the scoping to be agreed with the Department. In the event of significant issues being identified, a follow up remediation test will be required.
3. An IT Health Check to be performed by a CHECK provider will further be required annually for the duration of the contract. The results of which must be shared with the Department.
4. The Contractor will provide details of any proposal to store or host Departmental Data outside the UK or to perform ICT management or support from outside the UK and will not go ahead with such a proposal without prior agreement from the Department.
5. Departmental Data being handled in the course of providing this service must be segregated from other data on the Contractor’s own IT equipment to protect the Departmental Data and enable it to be securely deleted when required. In the event that it is not possible to segregate the Departmental Data then the Contractor is required to ensure that it is stored in such a way that it is possible to securely delete the data in line with Clause 21.
6. At the end of the contract or in the event of failure or obsoletion, all equipment holding Departmental Data must be securely cleansed or destroyed using a CESG approved product or method and in accordance with HMG standards. Where this is not possible e.g. for legal or regulatory reasons, or technical reasons such as where there is storage area network (SAN) or shared backup tapes, then the Contractor must protect the equipment until the time (which may be long after the end of the contract) when it can be securely cleansed or destroyed.
7. All paper holding Departmental Data must be securely protected whilst in the Contractor’s care and securely destroyed when no longer required in accordance with HMG standards.
8. The Contractor must have ISO 22301 conformant Business Continuity plans and processes including IT disaster recovery plans and procedures to ensure that the delivery of the contract is not adversely affected in the event of an incident or crisis. The Contractor must describe how this requirement will be met.
9. Any non-compliance with these Departmental Security Standards for Contractors, or any suspected or actual breach of the confidentiality or integrity of Departmental Data being handled in the course of providing this service, shall be immediately escalated to the Department by a method agreed by both parties.
10. The Contractor shall contractually enforce all these Departmental Security Standards for Contractors onto any third-party suppliers, sub-contractors or partners who could potentially access Departmental Data in the course of providing this service.
11. The Department reserves the right to audit the Contractor with 24 hours’ notice in respect to the Contractor’s compliance with the clauses contained in this Section.

Annex D

Egress Switch Product Quotation

Redacted

Annex E

Egress Professional Services Quotation

Redacted

**BY SIGNING AND RETURNING THIS ORDER FORM THE SUPPLIER AGREES** to enter a legally binding contract with the Customer to provide the G-Cloud Services. The Parties hereby acknowledge and agree that they have read the Call-Off Terms and the Order Form and by signing below agree to be bound by the terms of this Call-Off Agreement.

|  |  |
| --- | --- |
| **For and on behalf of the Supplier:** | |
| Name and Title |  |
| Position |  |
| Signature |  |
| Date |  |

|  |  |
| --- | --- |
| **For and on behalf of the Customer:** | |
| Name and Title |  |
| Position |  |
| Signature |  |
| Date |  |

Call-Off Agreement Terms and Conditions

THIS CONTRACT is made on the [28] day of [04] 2015

BETWEEN

1. The Secretary of State for Education of Sanctuary Buildings, Great Smith Street, London (the “Customer”); and
2. Egress Software Technologies Limited a company registered in England under company number 6393598 and whose registered office is at Unit 16, Quadrant Business Centre, 135 Salusbury Road, London NW6 6RJ (the “Supplier”).

IT IS AGREED AS FOLLOWS:

OVERRIDING PROVISIONS

* 1. The Supplier agrees to supply the G-Cloud Services and any G-Cloud Additional Services in accordance with the Call-Off Terms, including Supplier’s own terms and conditions as identified in Framework Schedule 1 (G-Cloud Services) and incorporated into this Call-Off Agreement.
  2. In the event of and only to the extent of any conflict or ambiguity between the Clauses of this Call-Off Agreement, the provisions of the Schedules, any document referred to in the Clauses of this Call-Off Agreement (including Supplier’s terms and conditions) and the Framework Agreement, the conflict shall be resolved in accordance with the following order of precedence:
     1. the Framework Agreement (excluding Framework Schedule 2)
     2. the Clauses of this Call-Off Agreement (excluding Supplier Terms);
     3. the completed Order Form;
     4. the Collaboration Agreement (Framework Schedule 7);
     5. the Supplier’s terms and conditions as set out in the Framework Schedule 1 (G-Cloud Services); and
     6. any other document referred to in the Clauses of this Call-Off Agreement.
  3. The Supplier acknowledges and accepts that the order of prevailing provisions as set out in Clause CO-1.2 above.

PREVENTION OF BRIBERY AND CORRUPTION

* 1. If the Supplier breaches
     1. Clauses FW-22.1 or FW-22.2 of the Framework Agreement; or,
     2. the Bribery Act 2010 in relation to the Framework Agreement

the Customer may terminate this Call-Off Agreement.

* 1. The Parties agree that the Management Charge payable in accordance with Clause FW-9 does not constitute an offence under section 1 of the Bribery Act 2010.

PROTECTION OF INFORMATION

* 1. The provisions of this Clause CO-3, shall apply during the Call-Off Agreement Period and for such time as the Supplier holds the Customer Personal Data.
  2. The Supplier shall and shall procure that Supplier’s Staff comply with any notification requirements under the DPA and both Parties undertake to duly observe all their obligations under the DPA which arise in connection with the Call-Off Agreement.
  3. To the extent that the Supplier is Processing the Order Personal Data the Supplier shall:
     1. ensure that it has in place appropriate technical and organisational measures to ensure the security of the Order Personal Data (and to guard against unauthorised or unlawful Processing of the Order Personal Data and against accidental loss or destruction of, or damage to, the Order Personal Data; and
     2. provide the Customer with such information as the Customer may reasonably request to satisfy itself that the Supplier is complying with its obligations under the DPA;
     3. promptly notify the Customer of any breach of the security measures to be put in place pursuant to this Clause; and
     4. ensure that it does not knowingly or negligently do or omit to do anything which places the Customer in breach of its obligations under the DPA.
  4. To the extent that the Supplier Processes Service Personal Data the Supplier shall:
     1. Process Service Personal Data only in accordance with written instructions from the Customer as set out in this Call-Off Agreement;
     2. Process the Service Personal Data only to the extent, and in such manner, as is necessary for the provision of the G-Cloud Services or as is required by Law or any Regulatory Body;
     3. implement appropriate technical and organisational measures to protect Service Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful Processing, accidental loss, destruction or damage to Service Personal Data and having regard to the nature of the Service Personal Data which is to be protected;
     4. take reasonable steps to ensure the reliability of any Supplier Staff who have access to Service Personal Data;
     5. ensure that all Supplier Staff required to access Service Personal Data are informed of the confidential nature of the Service Personal Data and comply with the obligations set out in this Clause;
     6. ensure that none of the Supplier Staff publish, disclose or divulge Customer’s Personal Data to any third party unless necessary for the provision of the G-Cloud Services under the Call-Off Agreement and/or directed in writing to do so by the Customer;
     7. notify the Customer within five (5) Working Days if it receives:
        1. a request from a Data Subject to have access to Service Personal Data relating to that person; or
        2. a complaint or request relating to the Customer’s obligations under the Data Protection Legislation;
     8. provide the Customer with full cooperation and assistance in relation to any complaint or request made relating to Service Personal Data, including by:
        1. providing the Customer with full details of the complaint or request;
        2. complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the Customer’s instructions;
        3. providing the Customer with any Service Personal Data it holds in relation to a Data Subject (within the timescales required by the Customer); and
        4. providing the Customer with any information requested by the Data Subject.
  5. The Supplier shall:
     1. permit the Customer or the Customer’s Representative (subject to the reasonable and appropriate confidentiality undertakings), to inspect and audit the Supplier's data Processing activities (and/or those of its agents, subsidiaries and Sub-Contractors) or provide to the Customer an independent third party inspection and audit certificate in lieu of the same (unless otherwise agreed between the Parties, the option of providing a certificate in lieu shall not be available at IL3 and above) and shall comply with all reasonable requests or directions by the Customer to enable the Customer to verify and/or procure that the Supplier is in full compliance with its obligations under this Call-Off Agreement; and/or
     2. subject to Clause CO-3.6 agree to an appointment of an independent auditor selected by the Supplier to undertake the activities in Clause CO-3.5.1 provided such selection is acceptable to the Customer or Customer Representative (subject to such independent auditor complying with the reasonable and appropriate confidentiality undertakings).
  6. The Supplier Shall:
     1. obtain prior written consent from the Customer in order to transfer Customer Personal Data to any other person (including for the avoidance of doubt any Sub-Contractors) for the provision of the G-Cloud Services;
     2. not cause or permit to be Processed, stored, accessed or otherwise transferred outside the EEA any Customer Personal Data supplied to it by the Customer without the prior written consent of the Customer. Where the Customer consents to such Processing, storing, accessing or transfer outside the European Economic Area the Supplier shall:
        1. comply with the obligations of a Data Controller under the Eighth Data Protection Principle set out in Schedule 1 of the Data Protection Act 1998 by providing an adequate level of protection to any Personal Data that is so processed, stored, accessed or transferred;
        2. comply with any reasonable instructions notified to it by the Customer and either:
        3. incorporate standard and/or model clauses (which are approved by the European Commission as offering adequate safeguards under the Data Protection Legislation) or warrant that that the obligations set out in the Supplier Terms provide Adequate protection for Personal Data.
  7. The Supplier shall not perform its obligations under this Call-Off Agreement in such a way as to cause the Customer to breach any of its applicable obligations under the Data Protection Legislation.
  8. The Supplier acknowledges that, in the event that it breaches (or attempts or threatens to breach) its obligations relating to Personal Data that the Customer may be irreparably harmed (including harm to its reputation). In such circumstances, the Customer may proceed directly to court and seek injunctive or other equitable relief to remedy or prevent any further breach (or attempted or threatened breach).

CONFIDENTIALITY

* 1. Except to the extent set out in this Clause or where disclosure is expressly permitted elsewhere in this Call-Off Agreement, each Party shall:
     1. treat the other Party’s Confidential Information as confidential and safeguard it accordingly; and
     2. not disclose any Confidential Information belonging to the other Party to any other person without the prior written consent of the other Party, except to such persons and to such extent as may be necessary for the performance of this Call-Off Agreement.
  2. The Supplier may only disclose the Customer's Confidential Information to the Supplier Staff who are directly involved in the provision of the G-Cloud Services and who need to know the information, and shall ensure that such Supplier Staff are aware of and shall comply with these obligations as to confidentiality.
  3. The Supplier shall not, and shall procure that the Supplier Staff do not, use any of the Customer's Confidential Information received otherwise than for the purposes of this Call-Off Agreement.
  4. The provisions of Clauses CO-4.1 shall not apply to the extent that:
     1. such disclosure is a requirement of Law placed upon the Party making the disclosure, including any requirements for disclosure under Clause CO-7 (Transparency) and the FOIA, the Ministry of Justice Code or the Environmental Information Regulations pursuant to Clause CO-6 (Freedom of Information);
     2. such information was in the possession of the Party making the disclosure without obligation of confidentiality prior to its disclosure by the information owner;
     3. such information was obtained from a third party without obligation of confidentiality;
     4. such information was already in the public domain at the time of disclosure otherwise than by a breach of this Call-Off Agreement; or
     5. it is independently developed without access to the other Party's Confidential Information.
  5. Nothing in this Call-Off Agreement shall prevent the Customer from disclosing the Supplier's Confidential Information (including the Management Information obtained under Clause FW-8 (Provision of Management Information) of the Framework Agreement):
     1. for the purpose of the examination and certification of the Customer’s accounts;
     2. for any examination pursuant to Section 6(1) of the National Audit Act 1983 of the economy, efficiency and effectiveness with which the Customer has used its resources;
     3. to any Crown body or any Other Contracting Body. All Crown bodies or Contracting Bodies receiving such Supplier's Confidential Information shall be entitled to further disclose the Supplier's Confidential Information to other Crown bodies or Other Contracting Bodies on the basis that the information is confidential and is not to be disclosed to a third party which is not part of any Crown body or any Contracting Body; or
     4. to any consultant, contractor or other person engaged by the Customer (on the basis that the information shall be held by such consultant, contractor or other person in confidence and is not to be disclosed to any third party) or any person conducting a Cabinet Office or ERG Gateway review or any additional assurance programme.
  6. In the event that the Supplier fails to comply with Clauses CO-4.1 to Clause CO-4.4, the Customer reserves the right to terminate this Call-Off Agreement with immediate effect by notice in writing.
  7. In order to ensure that no unauthorised person gains access to any Confidential Information or any data obtained in performance of this Call-Off Agreement, the Supplier undertakes to maintain adequate security arrangements that meet the requirements of Good Industry Practice.
  8. The Supplier will immediately notify the Customer of any breach of security in relation to Customer Confidential Information obtained in the performance of this Call-Off Agreement and will keep a record of such breaches. The Supplier will use its best endeavours to recover such Customer Confidential Information however it may be recorded. This obligation is in addition to the Supplier's obligations under Clauses CO-4.1 to Clause CO-4.4. The Supplier will co-operate with the Customer in any investigation that the Customer considers necessary to undertake as a result of any breach of security in relation to Customer Confidential Information.
  9. Subject always to Clause CO-11.4 the Supplier shall, at all times during and after the Call-Off Agreement Period, indemnify the Customer and keep the Customer fully indemnified against all losses, damages, costs or expenses and other liabilities (including legal fees) incurred by, awarded against the Customer arising from any breach of the Supplier's obligations under the DPA or this Clause CO-4 (Confidentiality) except and to the extent that such liabilities have resulted directly from the Customer's instructions.

CUSTOMER DATA

* 1. The Supplier shall not delete or remove any proprietary notices contained within or relating to the Customer Data.
  2. The Supplier shall not store, copy, disclose, or use the Customer Data except as necessary for the performance by the Supplier of its obligations under this Call-Off Agreement or as otherwise expressly approved by the Customer.
  3. The Supplier shall ensure that any system on which the Supplier holds any Customer Data, including back-up data, is a secure system that complies with the Supplier security policy.

STATUTORY OBLIGATIONS AND REGULATIONS

FREEDOM OF INFORMATION

* 1. The Supplier acknowledges that the Customer is subject to the requirements of the FOIA and the Environmental Information Regulations and shall assist and co-operate with the Customer to enable the Customer to comply with its Information disclosure obligations.
  2. The Supplier shall:
     1. transfer to the Customer all Requests for Information that it receives as soon as practicable and in any event within two (2) Working Days of receiving a Request for Information;
     2. provide the Customer with a copy of all Information, relating to a Request for Information, in its possession or control, in the form that the Customer requires within five (5) Working Days (or such other period as the Customer may specify) of the Customer's request; and
     3. provide all necessary assistance as reasonably requested by the Customer to enable the Customer to respond to the Request for Information within the time for compliance set out in section 10 of the FOIA or regulation 5 of the Environmental Information Regulations.
  3. The Customer shall be responsible for determining in its absolute discretion and notwithstanding any other provision in this Call-Off Agreement or any other agreement whether the Commercially Sensitive Information and/or any other Information (including Supplier’s Confidential Information) is exempt from disclosure in accordance with the provisions of the FOIA or the Environmental Information Regulations.
  4. In no event shall the Supplier respond directly to a Request for Information unless authorised in writing to do so by the Customer.
  5. The Supplier acknowledges that the Customer may, acting in accordance with the Ministry of Justice Code, be obliged under the FOIA, or the Environmental Information Regulations to disclose Information concerning the Supplier or the G-Cloud Services:
     1. in certain circumstances without consulting the Supplier; or
     2. following consultation with the Supplier and having taken its views into account;

provided always that where Clause CO-6.5.3 applies the Customer shall, in accordance with any recommendations of the Ministry of Justice Code, take reasonable steps, where appropriate, to give the Supplier advanced notice, or failing that, to draw the disclosure to the Supplier's attention after any such disclosure.

* + 1. The Supplier acknowledges that the description of information as Commercially Sensitive Information in Framework Schedule 6 (Interpretations and Definitions) is of an indicative nature only and that the Customer may be obliged to disclose it in accordance with this Clause CO-6.

TRANSPARENCY

* 1. The Parties acknowledge that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of this Call-Off Agreement is not Confidential Information. The Customer shall be responsible for determining in its absolute discretion whether any of the content of this Call-Off Agreement is exempt from disclosure in accordance with the provisions of the FOIA.
  2. Notwithstanding any other term of this Call-Off Agreement, the Supplier hereby gives its consent for the Customer to publish this Call-Off Agreement in its entirety (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted), including from time to time agreed changes to this Call-Off Agreement, to the general public.
  3. The Customer may consult with the Supplier to inform its decision regarding any redactions but the Customer shall have the final decision in its absolute discretion.
  4. The Supplier shall assist and cooperate with the Customer to enable the Customer to publish this Call-Off Agreement.

OFFICIAL SECRETS ACTS

* 1. The Supplier shall comply with and shall ensure that the Supplier Staff comply with, the provisions of:
     1. the Official Secrets Act 1911 to 1989; and
     2. Section 182 of the Finance Act 1989.
  2. In the event that the Supplier or the Supplier Staff fails to comply with this Clause, the Customer reserves the right to terminate this Call-Off Agreement with immediate effect by giving notice in writing to the Supplier.

TERM AND TERMINATION

* 1. This Call-Off Agreement shall take effect on the Effective Date and shall expire on:
     1. the date specified in paragraph 1.2 of the Order Form; or
     2. twenty four (24) Months after the Effective Date, whichever is the earlier, unless terminated earlier pursuant to this Clause CO-9.
  2. Termination without Cause
     1. The Customer shall have the right to terminate this Call-Off Agreement at any time by giving the length of written notice to the Supplier as set out in paragraph 10.2 of the Order Form.
  3. Termination on Change of Control
     1. The Supplier shall notify the Customer immediately if the Supplier undergoes a change of control within the meaning of Section 450 of the Corporation Tax Act 2010 ("Change of Control") and provided this does not contravene any Law shall notify the Customer immediately in writing of any circumstances suggesting that a Change of Control is planned or in contemplation. The Customer may terminate the Call-Off Agreement by notice in writing with immediate effect within six (6) Months of:
        1. being notified in writing that a Change of Control has occurred or is planned or in contemplation; or
        2. where no notification has been made, the date that the Customer becomes aware of the Change of Control,

but shall not be permitted to terminate where a written approval was granted prior to the Change of Control.

* + 1. For the purposes of Clause CO-9.3.1, any transfer of shares or of any interest in shares by its affiliate company where such transfer forms part of a bona fide reorganisation or restructuring shall be disregarded.
  1. Termination by Supplier

CO-9.4.1 If the Customer fails to pay the Supplier undisputed sums of money when due, the Supplier shall notify the Customer in writing of such failure to pay and allow the Customer five (5) calendar days to settle undisputed invoice. If the Customer fails to pay such undisputed sums within allotted additional 5 calendar days, the Supplier may terminate this Call-Off Agreement subject to giving the length of notice as specified in paragraph 10.1 of the Order Form.

* 1. Termination on Insolvency
     1. The Customer may terminate this Call-Off Agreement with immediate effect by notice in writing where the Supplier:
        1. being an individual, or where the Supplier is a firm, any partner or partners in that firm who together are able to exercise direct or indirect control, as defined by Section 416 of the Income and Corporation Taxes Act 1988, and:
        2. shall at any time become bankrupt or shall have a receiving order or administration order made against him or shall make any composition or arrangement with or for the benefit of his creditors, or shall make any conveyance or assignment for the benefit of his creditors, or shall purport so to do, or appears unable to pay or to have no reasonable prospect of being able to pay a debt within the meaning of Section 268 of the Insolvency Act 1986, or any similar event occurs under the law of any other jurisdiction; or
        3. a creditor or encumbrancer attaches or takes possession of, or a distress, execution, sequestration or other such process is levied or enforced on or sued against, the whole or any part of the Supplier's assets and such attachment or process is not discharged within fourteen (14) calendar days; or
        4. he dies or is adjudged incapable of managing his affairs within the meaning of Part VII of the Mental Health Act 1983; or
        5. the Supplier suspends or ceases, or threatens to suspend or cease, to carry on all or a substantial part of his business.
     2. being a company, passes a resolution, or the Court makes an order that the Supplier or its Parent Company be wound up otherwise than for the purpose of a bona fide reconstruction or amalgamation, or a receiver, manager or administrator on behalf of a creditor is appointed in respect of the business or any part thereof of the Supplier or its Parent Company (or an application for the appointment of an administrator is made or notice to appoint an administrator is given in relation to the Supplier or its Parent Company), or circumstances arise which entitle the Court or a creditor to appoint a receiver, manager or administrator or which entitle the Court otherwise than for the purpose of a bona fide reconstruction or amalgamation to make a winding-up order, or the Supplier or its Parent Company is unable to pay its debts within the meaning of Section 123 of the Insolvency Act 1986 (except where the claim is made under Section 123(1)(a) and is for an amount of less than ten thousand pounds (£10,000)) or any similar event occurs under the law of any other jurisdiction.
  2. Termination on Material Breach
     1. The Customer may terminate this Call-Off Agreement with immediate effect by giving written notice to the Supplier if the Supplier commits a Material Breach of any obligation under this Call-Off Agreement and if:
        1. the Supplier has not remedied the Material Breach within thirty (30) Working Days (or such other longer period as may be specified by the Customer) of written notice to the Supplier specifying the Material Breach and requiring its remedy; or
        2. the Material Breach is not, in the opinion of the Customer capable of remedy.
  3. Termination for repeated Default
     1. If there are two or more Defaults (of a similar nature) that will be deemed a breach for Material Breach. Where the Customer considers that the Supplier has committed a repeated Default in relation to this Call-Off Agreement or any part thereof (including any part of the G-Cloud Services) and believes that the Default is remediable, then the Customer shall be entitled to serve a notice on the Supplier:
        1. specifying that it is a formal warning notice;
        2. giving reasonable details of the breach; and
        3. stating that such breach is a breach which, if it recurs or continues, may result in a termination of this Call-Off Agreement or that part of the G-Cloud Services affected by such breach.
     2. If, thirty (30) Working Days after service of a formal warning notice as described in Clause CO-9.7, the Supplier has failed to demonstrate to the satisfaction of the Customer that the breach specified has not continued or recurred and that the Supplier has put in place measures to ensure that such breach does not recur, then the Customer may deem such failure to be a Material Breach not capable of remedy for the purposes of Clause CO-9.6.1.2.
  4. The termination (howsoever arising) or expiry of this Call-Off Agreement pursuant to this Clause 9 shall be without prejudice to any rights of either the Customer or the Supplier that shall have accrued before the date of such termination or expiry.
  5. Save as aforesaid, the Supplier shall not be entitled to any payment from the Customer after the termination (howsoever arising) or expiry of this Call-Off Agreement.

CONSEQUENCES OF SUSPENSION, TERMINATION AND EXPIRY

* 1. Where a Customer has the right to terminate a Call-Off Agreement, it may elect to suspend this Call-Off Agreement and its performance.
  2. Notwithstanding the service of a notice to terminate this Call-Off Agreement or any part thereof, the Supplier shall continue to provide the Ordered G-Cloud Services until the date of expiry or termination (howsoever arising) of this Call-Off Agreement (or any part thereof) or such other date as required under this Clause CO-10.
  3. Within ten (10) Working Days of the earlier of the date of expiry or termination (howsoever arising) of this Call-Off Agreement, the Supplier shall return (or make available) to the Customer:
     1. any data (including (if any) Customer Data), Customer Personal Data and Customer Confidential Information in the Supplier’s possession, power or control, either in its then current format or in a format nominated by the Customer (in which event the Customer will reimburse the Supplier’s pre-agreed and reasonable data conversion expenses), together with all training manuals, access keys and other related documentation, and any other information and all copies thereof owned by the Customer, save that it may keep one copy of any such data or information for a period of up to twelve (12) Months to comply with its obligations under the Framework Schedule FW-5, or such period as is necessary for such compliance (after which time the data must be deleted); and
     2. any sums prepaid in respect of Ordered G-Cloud Services not provided by the date of expiry or termination (howsoever arising) of this Call-Off Agreement.
  4. The Customer and the Supplier shall comply with the exit and service transfer arrangements as per the Supplier’s terms and conditions identified in Framework Schedule 1 (G-Cloud Services).
  5. Subject to Clause CO-11 (Liability), where the Customer terminates this Call-Off Agreement under Clause CO-9.2 (Termination without Cause), the Customer shall indemnify the Supplier against any reasonable and proven commitments, liabilities or expenditure which would otherwise represent an unavoidable loss by the Supplier by reason of the termination of this Call-Off Agreement, provided that the Supplier takes all reasonable steps to mitigate such loss. Where the Supplier holds insurance, the Supplier shall reduce its unavoidable costs by any insurance sums available. The Supplier shall submit a fully itemised and costed list of such loss, with supporting evidence, of losses reasonably and actually incurred by the Supplier as a result of termination under Clause CO-9.2 (Termination without Cause).

LIABILITY

* 1. Nothing in this Clause CO-11 shall affect a Party’s general duty to mitigate its loss.
  2. Nothing in this Call-Off Agreement shall be construed to limit or exclude either Party's liability for:
     1. death or personal injury caused by its negligence or that of its staff;
     2. bribery, Fraud or fraudulent misrepresentation by it or that of its staff;
     3. any breach of any obligations implied by Section 2 of the Supply of Goods and Services Act 1982; or
     4. any other matter which, by Law, may not be excluded or limited.
  3. Nothing in this Call-Off Agreement shall impose any liability on the Customer in respect of any liability incurred by the Supplier to any other person, but this shall not be taken to exclude or limit any liability of the Customer to the Supplier that may arise by virtue of either a breach of the Call-Off Agreement or by negligence on the part of the Customer, or the Customer's employees, servants or agents.
  4. Subject always to Clause CO-11.2, the aggregate liability of either Party under or in connection with each Year of this Call-Off Agreement (whether expressed as an indemnity or otherwise):
     1. for all defaults resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to the Customer Personal Data or Customer Data ) of the other Party, shall be subject to the financial limits set out in paragraph 8.1 of the Order Form;
     2. and in respect of all other defaults, claims, losses or damages, whether arising from breach of contract, misrepresentation (whether tortuous or statutory), tort (including negligence), breach of statutory duty or otherwise shall not exceed a sum equivalent to the financial limit set out in paragraph 8.3 of the Order Form .
  5. Subject always to Clause CO-11.4 the Customer shall have the right to recover as a direct loss:
     1. any additional operational and/or administrative expenses arising from the Supplier's Default;
     2. any wasted expenditure or charges rendered unnecessary and/or incurred by the Customer arising from the Supplier's Default; and
     3. any losses, costs, damages, expenses or other liabilities suffered or incurred by the Customer which arise out of or in connection with the loss of, corruption or damage to or failure to deliver Customer Data by the Supplier.
  6. The Supplier shall not be responsible for any injury, loss, damage, cost or expense if and to the extent that it is caused by the negligence or wilful misconduct of the Customer or by breach by the Customer of its obligations under the Call-Off Agreement.
  7. Subject to Clauses CO-11.2 and Clause CO-11.5, in no event shall either Party be liable to the other for any:
     1. loss of profits;
     2. loss of business;
     3. loss of revenue;
     4. loss of or damage to goodwill;
     5. loss of savings (whether anticipated or otherwise); and/or
     6. any indirect, special or consequential loss or damage.

CO-11.8 The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call–Off Agreement shall be subject to the financial limits set out in paragraph 8.2 of the Order Form.

INSURANCE

* 1. The Supplier shall effect and maintain with a reputable insurance company a policy or policies of insurance providing an adequate level of cover in respect of all risks which may be incurred by the Supplier, arising out of the Supplier's performance of its obligations under this Call-Off Agreement, including death or personal injury, loss of or damage to property or any other loss (including the insurance policies specified in the relevant paragraph of the Order Form). Such policies shall include cover in respect of any financial loss arising from any advice given or omitted to be given by the Supplier. Such insurance shall be maintained for the Call-Off Agreement Period and for the minimum insurance period as set out in paragraph 9 of the Order Form.
  2. The provisions of any insurance or the amount of cover shall not relieve the Supplier of any liabilities under this Call-Off Agreement.

PAYMENT, VAT AND CALL-OFF AGREEMENT CHARGES

* 1. In consideration of the Supplier's performance of its obligations under this Call-Off Agreement, the Customer shall pay the Charges in accordance with the Clause CO-13.2 to CO-13.8.
  2. The Customer shall pay all sums properly due and payable to the Supplier in cleared funds within the time period specified in paragraph 6 of the Order Form.
  3. The Supplier shall ensure that each invoice contains all appropriate references and a detailed breakdown of the G-Cloud Services supplied and that it is supported by any other documentation reasonably required by the Customer to substantiate the invoice.
  4. Where the Supplier enters into a Sub-Contract it shall ensure that a provision is included in such Sub-Contract which requires payment to be made of all sums due by the Supplier to the Sub-Contractor within a specified period not exceeding thirty (30) calendar days from the receipt of a validly issued invoice, in accordance with the terms of the Sub-Contract.
  5. The Supplier shall add VAT to the Charges at the prevailing rate as applicable.
  6. The Supplier shall fully indemnify the Customer on demand and keep the Customer fully indemnified on a continuing basis against any liability, including without limitation against any interest, penalties or costs, which are suffered or incurred by or levied, demanded or assessed on the Customer at any time in respect of the Supplier's failure to account for or to pay any VAT relating to payments made to the Supplier under this Call-Off Agreement. Any amounts due under this Clause CO-13 shall be paid by the Supplier to the Customer not less than five (5) Working Days before the date upon which the tax or other liability is payable by the Customer.

The Supplier shall not suspend the supply of the G-Cloud Services unless the Supplier is entitled to terminate this Call-Off Agreement under Clause CO-9.4 for Customer’s failure to pay undisputed sums of money. Interest shall be payable by the Customer on the late payment of any undisputed sums of money properly invoiced in accordance with the Late Payment of Commercial Debts (Interest) Act 1998 (as amended from time to time).

* 1. In the event of a disputed invoice, the Customer shall make payment in respect of any undisputed amount in accordance with the provisions of Clause CO-13 of this Call-Off Agreement and return the invoice to the Supplier within ten (10) Working Days of receipt with a covering statement proposing amendments to the invoice and/or the reason for any non-payment. The Supplier shall respond within ten (10) Working Days of receipt of the returned invoice stating whether or not the Supplier accepts the Customer’s proposed amendments. If it does then the Supplier shall supply with the response a replacement valid invoice.
  2. [The Supplier shall accept the Government Procurement Card as a means of payment for the G-Cloud Services where such card is agreed with the Customer to be a suitable means of payment. The Supplier shall be solely liable to pay any merchant fee levied for using the Government Procurement Card and shall not be entitled to recover this charge from the Customer.]

GUARANTEE

* 1. Where the Customer has specified in the Order Form that this Call-Off Agreement shall be conditional upon receipt of a guarantee from the Guarantor, the Supplier shall deliver to the Customer an executed guarantee from the Guarantor, on or prior to the Commencement Date; and deliver to the Customer a certified copy of the passed resolution and/or board minutes of the Guarantor approving the execution of the guarantee

FORCE MAJEURE

* 1. Neither Party shall be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Agreement to the extent that such delay or failure is a result of Force Majeure.
  2. Notwithstanding Clause CO-15.1, each Party shall use all reasonable endeavours to continue to perform its obligations under the Call-Off Agreement for the duration of such Force Majeure. However, if such Force Majeure prevents either Party from performing its material obligations under this Call-Off Agreement for a period in excess of one hundred and twenty (120) calendar days, either Party may terminate this Call-Off Agreement with immediate effect by notice in writing to the other Party.

TRANSFER AND SUB-CONTRACTING

* 1. The Supplier shall not assign, novate, sub-contract or in any other way dispose of this Call-Off Agreement or any part of it without the Customer’s prior written approval which shall not be unreasonably withheld or delayed. Sub-Contracting any part of this Call-Off Agreement shall not relieve the Supplier of any obligation or duty attributable to the Supplier under this Call-Off Agreement.
  2. The Supplier shall be responsible for the acts and omissions of its Sub-Contractors as though they are its own.
  3. The Customer may assign, novate or otherwise dispose of its rights and obligations under the Call-Off Agreement or any part thereof to:
     1. any other body established by the Crown or under statute in order substantially to perform any of the functions that had previously been performed by the Customer; or
     2. any private sector body which substantially performs the functions of the Customer

provided that any such assignment, novation or other disposal shall not increase the burden of the Supplier’s obligations under the Call-Off Agreement.

THE CONTRACTS (RIGHTS OF THIRD PARTIES) ACT 1999

* 1. A person who is not party to this Call-Off Agreement has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this Call-Off Agreement but this does not affect any right or remedy of any person which exists or is available otherwise than pursuant to that Act.

LAW & JURISDICTION

* 1. This Call-Off Agreement and/or any non-contractual obligations or matters arising out of or in connection with it, shall be governed by and construed in accordance with the Laws of England and Wales and without prejudice to the dispute resolution procedures set out in Clause FW-14 or CO-22 (Dispute Resolution) each Party agrees to submit to the exclusive jurisdiction of the courts of England and Wales and for all disputes to be conducted within England and Wales.

Additional G-Cloud Services

CO-19.1 The Customer may require the Supplier to provide the Additional G-Cloud Services. The Supplier acknowledges that the Customer is not obliged to take any Additional G-Cloud Services from the Supplier and that there is nothing preventing the Customer from receiving services that are the same as or similar to the Additional G-Cloud Services from any third party.

CO-19.2 The Supplier shall provide Additional G-Cloud Services in accordance with any relevant Implementation Plan(s) and the Supplier shall monitor the performance of such services against the Implementation Plan(s).

**COLLABORATION AGREEMENT**

CO-20.1 Where the Customer has specified in paragraph 13 of the Order Form that the Customer requires the Supplier to enter into a Collaboration Agreement, a Collaboration Agreement should be executed between the Parties, on or prior to the Commencement Date.

CO-20.2 In addition to its obligations under any Collaboration Agreement, the Supplier shall:

CO-20.2.1 work pro-actively with each of the Customer’s contractors in a spirit of trust and mutual confidence;

CO-20.2.2 in addition to its obligations under the Collaboration Agreement the Supplier shall cooperate with the Customer’s contractors of other services to enable the efficient operation of the ICT services; and

CO-20.2.3 assist in sharing information with the Customer’s contractors for the purposes of facilitating adequate provision of the G-Cloud Services and/or Additional G-Cloud Services.

**VARIATION PROCEDURE**

CO-21.1 The Customer may request in writing a variation to this Call-Off Agreement provided that such variation does not amount to a material change of the Framework Agreement and is within the meaning of the Regulations and the Law. Such a change once implemented is hereinafter called a **"Variation**".

CO-21.2 The Supplier shall notify the Customer immediately in writing of any changes proposed or in contemplation in relation to G-Cloud Services or their delivery by submitting Variation request. For the avoidance of doubt such changes would include any changes within the Supplier’s supply chain.

CO-21.3 In the event that:

* + - 1. Either Party is unable to agree (agreement shall not be unreasonably withheld or delayed) to or provide the Variation;
      2. the Customer may:
         1. agree to continue to perform its obligations under this Call-Off Agreement without the Variation; or
         2. terminate this Call-Off Agreement by mutual agreement within 30 days with immediate effect.

DISPUTE RESOLUTION

* 1. The Customer and the Supplier shall attempt in good faith to negotiate a settlement of any dispute between them arising out of or in connection with this Call-Off Agreement within twenty (20) Working Days of either Party notifying the other of the dispute and such efforts shall involve the escalation of the dispute to the Customer Representative and the Supplier Representative.
  2. If the dispute cannot be resolved by the Parties pursuant to this Clause, the Parties shall refer it to mediation unless the Customer considers that the dispute is not suitable for resolution by mediation.
  3. If the dispute cannot be resolved by mediation the Parties may refer it to arbitration.
  4. The obligations of the Parties under this Call-Off Agreement shall not be suspended, cease or be delayed by the reference of a dispute to mediation or arbitration pursuant to this Clause and the Supplier and Supplier’s Staff shall continue to comply fully with the requirements of this Call-Off Agreement at all times.